Citrix Virtual Apps and Desktops 7 2303

Contents

Citrix Virtual Apps and Desktops 7 2303

June 28, 2023

Citrix Virtual Apps and Desktops 7 2303

September 13, 2023

Sobre este lançamento de versão

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

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

  Depois de atualizar seus VDAs para essa versão (da versão 7.9 ou posterior), você não precisa atualizar o nível funcional do catálogo de máquinas. The 7.9 (or later) value remains the default functional level, and is valid for this release. Para obter mais informações, consulte Versões do VDA e níveis funcionais.

Para obter instruções de instalação e atualização:

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

Virtual Delivery Agents (VDAs) 2303

Suporte a TLS 1.3

O Citrix Virtual Apps and Desktops agora suporta o protocolo TLS 1.3 para conexões baseadas em TCP entre componentes. Para obter mais informações, consulte Transport Layer Security (TLS).

Controle de congestionamento de EDT aprimorado (Preview)

Um novo algoritmo de controle de congestionamento foi introduzido para otimizar o protocolo. Essa implementação permite que o EDT alcance maior taxa de transferência e reduza a latência para uma melhor experiência do usuário.

HDX Direct (Preview)

Com esse recurso, você pode estabelecer automaticamente uma conexão direta segura com o VDA quando a comunicação direta estiver disponível enquanto você acessa seus recursos por meio do Workspace e do Gateway Service. Consulte HDX Direct para obter mais detalhes.

Redirecionamento de geolocalização

O serviço de canal virtual de localização e sensor oferece suporte às APIs de localização do Windows atualizadas e, agora, é compatível com todos os aplicativos.

Web Studio

Suporte para configurar o roaming de sessões

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

Algumas ações renomeadas para melhor alinhá-las a seus significados reais

Renomeamos as seguintes ações em **Machine Catalogs** e **Delivery Groups**. Os fluxos de trabalho para realizar essas ações permanecem inalterados.

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

Usar um perfil de máquina ativado por padrão para a criação do catálogo do Azure

Ao criar catálogos de máquinas do Azure usando o Web Studio, a opção **Use a machine profile** agora está selecionada por padrão. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.

Anotar uma imagem ao atualizar máquinas

No Web Studio, agora você pode fazer anotações em uma imagem adicionando uma nota sobre ela ao atualizar um catálogo criado pelo MCS. Cada vez que você atualiza o catálogo, é criada uma entrada relacionada à nota se você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como null (-). Para exibir o histórico de notas da imagem, selecione o catálogo, clique em **Template Properties** no painel inferior e, em seguida, clique em **View note history**. Para obter mais informações, consulte Alterar a imagem mestre de um catálogo.

Melhorar o desempenho preservando uma VM provisionada durante o ciclo de energia

Adicionamos a configuração **Retain VMs across power cycles** à página **Machine Catalog Setup > Disk Settings**. A configuração permite preservar uma máquina virtual provisionada durante o ciclo de energia em ambientes do Azure. Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.

Modo proxy para o Web Studio

Anteriormente, o console do Web Studio precisava se comunicar com o servidor do Web Studio e com os Delivery Controllers ao gerenciar sites. Com o modo proxy, o servidor Web Studio agora pode atuar como um proxy para Delivery Controllers, tornando-se assim o único ponto de acesso ao console do Web Studio. Para obter mais informações, consulte Configurar o Web Studio como um proxy para Delivery Controllers.

> **Nota:**
>
> Algumas das fontes de informações anteriores levam você para a documentação do Citrix DaaS. No Citrix DaaS, o Web Studio é conhecido como Full Configuration. Estamos atualizando a documentação atual para cobrir o Web Studio. A implementação das atualizações é um processo contínuo. Agradecemos a sua paciência durante esta transição.

Citrix Studio

Procurar aplicativos para adicionar manualmente

Um botão **Browse** agora está disponível na página **Add Applications Manually**. Com ele, você pode facilmente procurar e selecionar um aplicativo a partir de um VDA no grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega e Aplicativos.

Citrix Director

Alerta de máquinas com falha

O recurso de notificação e alertas proativos do Director foi aprimorado para incluir um novo alerta, **Failed Machines (in %)**, que se baseia na porcentagem de máquinas com falha em um grupo de entrega. A nova condição de alerta permite que você configure limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega. Para obter mais informações, consulte a seção Máquinas com falha no artigo Alertas.

Machine Creation Services (MCS)

Suporte para personalizar o comportamento de ativação em caso de falha na alteração do tipo de armazenamento

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

Suporte para criptografia de disco do Azure no host

Com esse recurso, agora você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma especificação de modelo ou uma VM como entrada para um perfil de máquina. Para obter mais informações, consulte Criptografia de disco do Azure no host.

Nesse tipo de criptografia, o servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta. Para obter mais informações, consulte Encryption at host - End-to-end encryption for your VM data.

Suporte ao modelo de instância do GCP como uma entrada para o perfil da máquina

Com esse recurso, agora você pode selecionar um modelo de instância do GCP como uma entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP, portanto, são muito econômicos. Para fazer isso, use os comandos do PowerShell. Para obter mais informações sobre como usar comandos do PowerShell para criar e atualizar catálogos de máquinas selecionando um modelo de instância do GCP, consulte Criar um catálogo de máquinas com perfil de máquina como modelo de instância.

Suporte para ativação da MAK

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

Suporte para permitir identificadores de segurança ao criar máquinas virtuais

Anteriormente, ao criar novas máquinas virtuais com a configuração especificada por um esquema de provisionamento, você não podia adicionar um identificador de segurança (`ADAccountSid`) ao comando *NewProvVM*. Com esse recurso, agora você pode adicionar o parâmetro ADAccountSid para identificar de forma exclusiva as máquinas ao criar novas máquinas virtuais. Para obter mais informações, consulte Adicionar SIDs ao criar máquinas virtuais.

Capacidade de receber avisos associados aos catálogos MCS

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

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

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

Suporte para usar uma imagem da Galeria de Computação do Azure para criar e atualizar um catálogo MCS

Você pode criar e atualizar um catálogo de máquinas MCS usando uma imagem da Galeria de Computação do Azure. Você pode usar os comandos do Citrix Studio ou do PowerShell para criar ou atu-

alizar catálogos de máquinas. Para obter mais informações, consulte Criar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure.

Adicionar uma descrição informativa sobre atualizações de imagens

Anteriormente, não havia a opção de adicionar uma descrição a uma atualização de imagem. Com esse recurso, agora você pode adicionar notas para descrever imagens usadas para criar ou atualizar um catálogo de máquinas. Você também pode recuperar essas notas. Essa funcionalidade é útil quando você deseja manter registros das atualizações de imagem. Esses registros são úteis para auditorias. Usando comandos do PowerShell, você pode criar e visualizar a descrição. Para obter detalhes, consulte Adicionar descrições a uma imagem.

Suporte para alterar o tipo de armazenamento das VMs existentes para um nível inferior no desligamento em ambientes Azure

Em ambientes Azure, agora você pode economizar custos de armazenamento alterando o tipo de armazenamento das VMs existentes para um nível inferior quando as VMs são desligadas. Para fazer isso, use a propriedade personalizada *StorageTypeAtShutdown*. Para obter mais informações, consulte Alterar o tipo de armazenamento das VMs existentes para um nível inferior no desligamento.

Otimização do Microsoft Teams

A qualidade de áudio dos codecs antigos aumentou

Temos três opções de redirecionamento de áudio: qualidade média, qualidade alta e áudio adaptativo. Mais largura de banda foi alocada para codecs de áudio médio e alto. A largura de banda média aumentou para 24 kbps e a largura de banda alta aumentou para 224 kbps.

Problemas resolvidos

June 28, 2023

Não houve correção de problemas desde o Citrix Virtual Apps and Desktops 7 2212.

Citrix Provisioning

- A documentação do Citrix Provisioning 2303 fornece informações específicas sobre as atualizações nesta versão.

Linux VDA

- A documentação do Linux VDA 2303 fornece informações específicas sobre as atualizações nesta versão.

Profile Management

- A documentação do Profile Management 2303 fornece informações específicas sobre as atualizações nesta versão.

Session Recording

- A documentação do Session Recording 2303 fornece informações específicas sobre as atualizações nesta versão.

VDA para SO de sessão única

Exceções do sistema

No VDA versão 2203, o funcionamento do Citrix Audio Redirection falha intermitentemente. [HDX-42679]

Problemas conhecidos

April 3, 2024

Observações

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

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por

> sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Geral

- A solicitação de preparação da sessão para o VDA falha com uma mensagem de exceção. [CVADHELP-20832]
- Você não consegue instalar o VDA em uma área de trabalho do Windows 11. Você recebe o seguinte erro: **Installation of the Citrix Authentication Identity Assertion VDA Plug-in failed with error code 1603.** Como solução alternativa, recomendamos que você reinicie a instalação. [AUTH-1858]
- Após mudanças na arquitetura do Citrix Virtual Apps and Desktops na versão 2209, os ícones padrão para áreas de trabalho Windows e para aplicativos implantados antes dessa versão foram alterados para ícones genéricos de área de trabalho de PC. Essa alteração só se aplica a áreas de trabalho e aplicativos que estão apontando para o ícone padrão. Se você quiser alterar os ícones de volta para o ícone padrão do aplicativo Windows, execute o seguinte script usando o SDK remoto do PowerShell: `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- Se você iniciar a barra de aplicativos e abrir o menu Connection Center no aplicativo Citrix Workspace para Windows, a barra de aplicativos não aparece no servidor que o hospeda. [HDX-27504]
- Se você usar o aplicativo Citrix Workspace para Windows e iniciar a barra de aplicativos na posição vertical, a barra cobre o menu Iniciar ou a bandeja do relógio do sistema. [HDX-27505]
- Depois de instalar o plug-in do aplicativo Web Skype for Business, as webcams podem não ser enumeradas e as páginas de reuniões no Firefox podem não ser atualizadas automaticamente. [HDX-13288]
- Quando você inicia um aplicativo no StoreFront, o aplicativo pode não iniciar em primeiro plano ou o aplicativo aparece 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 clique na tela do aplicativo para colocá-lo no foco. [HDX-10126]
- Ao usar o Windows 10 1809 LTSC, as dependências `VCLibs` não são instaladas. [HDX-16754]
- A caixa de combinação pode não ser exibida corretamente quando um usuário seleciona uma caixa de combinação que já está com foco no host. Como solução alternativa, selecione outro elemento da interface do usuário e, em seguida, selecione a caixa de combinação. [HDX-21671]
- Você ativou o acesso ao aplicativo local. Se você iniciar uma sessão de VDA do Windows 2012 R2, desconectar-se e se reconectar à sessão e, em seguida, iniciar um aplicativo local e maximizá-lo, a barra de tarefas do VDA pode truncar o aplicativo. [HDX-21913]

- 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 "O VDI está em uso no momento"é exibido. [XSI-802]
- O Citrix Hypervisor não oferece suporte a VMs com clone completo do MCS com SRs GFS2. [XSI-832]
- Quando aplicativos do Microsoft Office 365 build 16.0.7967 e posteriores são publicados como aplicativos a partir 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 com Windows Server 2016 que não tenham o componente Web Authentication Manager que está funcionando incorretamente. [LCM-7637]
- As configurações de **Limites de sessão** para VDAs de várias sessões são recusadas em hosts de sessão que executam o Windows Server 2022, o Windows 10 Enterprise multissessão e o Windows 11 Enterprise multissessão.
  Como solução alternativa, você pode configurar os **Limites de tempo de sessão do RDS** por meio do GPO. [HDX-47001]
- Em alguns cenários, quando você usa o filtro de política IP do cliente, o endereço IP usado para avaliar a política está incorreto. [HDX-62375]

Studio

- Quando você instala o Web Studio usando o WebStudio_x64.msi, o assistente de instalação exibe uma amostra do texto do contrato de licença em vez das seguintes informações que você precisa aceitar para instalar o software. **Nota:** Recomendamos usar o instalador ISO em seu lugar. [STUD-22584]

```
CITRIX LICENSE AGREEMENT

Use of this component is subject to the Citrix license or terms
   of service covering the Citrix product(s) and/or service(s)
   with which you will be using this component. This component is
    licensed for use only with such Citrix product(s) and/or
   service(s).

CTX_code EP_T_A10352779
<!--NeedCopy-->
```

- Em **Web Studio > Logging > Events**, as operações de provisionamento do MCS disparadas através do PowerShell podem não exibir o status correto. Exemplo: mesmo quando uma operação executada através do PowerShell é concluída, ela pode continuar aparecendo como "In progress". Esse problema não afeta a funcionalidade do Citrix DaaS. Esse problema ocorre com

os seguintes cmdlets do PowerShell:

- New-ProvSchme
- New-ProvVM
- Remove-ProvVM
- Publish-ProvMasterVMImage
- Reset-ProvVMDisk
- New-ProvImageVersion
- Set-ProvSchemeImage [STUD-23361, PMCS-36679, CCVADHELP-2743]

Director

- O link **Console** em **Citrix Director > Detalhes do computador** não inicia o console da máquina nos navegadores Microsoft Edge 44 e Firefox 68 ESR. [DIR-8160]

Gráficos

- Ao compartilhar um aplicativo minimizado, a barra de título do aplicativo também pode ser compartilhada. [HDX-33898]
- Configurar a política **View window contents while dragging** como **Prohibited** não funciona no ESXi e no Hyper-V. [HDX-22002]
- Se você iniciar uma visualização de vídeo usando um aplicativo de webcam de 64 bits com compressão Theora, a sessão poderá falhar. [HDX-21443]
- No Windows 11 versão 22H2, ao mover uma janela do Windows Media Player em uma sessão, somente a metade inferior do vídeo é exibida. Como solução alternativa, selecione: **Settings > System > Multitasking > Snap windows > Show snap layouts when I drag a window to the top of my screen** [HDX-42092]
- Quando você tenta se conectar a uma sessão de VDA desconectada no Citrix Virtual Apps and Desktops versão 2303, a tela trava na tela de **boas-vindas**. Para obter mais informações, consulte o artigo de suporte CTX547782. [HDX-49992]

Impressão

- As impressoras Universal Print Server selecionadas na área de trabalho virtual não aparecem na janela **Dispositivos e impressoras** no painel de controle. No entanto, quando os usuários estão trabalhando em aplicativos, eles podem usar essas impressoras. Esse problema ocorre somente no Windows Server 2012, Windows 10 e Windows 8. Para obter mais informações, consulte CTX213540. [HDX-5043, 335153]

- A impressora padrão pode não ser marcada corretamente na janela da caixa de diálogo de impressão. Esse problema não afeta os trabalhos de impressão enviados para a impressora padrão. [HDX-12755]

Machine Creation Services

- O comando PowerShell `Remove-ProvVM` com o parâmetro `ForgetVM` pode não funcionar corretamente se as versões do Delivery Controller e do PowerShell remoto não forem compatíveis. Isso implica que as versões do Delivery Controller e do PowerShell remoto devem ser anteriores a 2212, 2212 ou posteriores. Por exemplo, se a versão do Delivery Controller for posterior à 2212 e a versão do PowerShell remoto for anterior à 2212, o comando `Remove-ProvVM` com o parâmetro `ForgetVM` não funcionará conforme o esperado. Como solução alternativa, baixe a versão mais recente do PowerShell para trabalhar com a versão mais recente do Delivery Controller. [PMCS-40278]
- Ao criar um catálogo MCS com a conexão de host Nutanix (especificamente, o plug-in Nutanix AHV 2.7.1), o tamanho do disco rígido das VMs provisionadas é exibido incorretamente na interface Full Configuration. O tamanho exibido é muito menor (1 GB) do que o tamanho real do armazenamento (50 GB). O tamanho do disco rígido é exibido corretamente no console do Nutanix. [PMCS-30639 e PMCS-32206]

Problemas de terceiros

- O Chrome é compatível com a Automação de IU somente em barras de ferramentas, guias, menus e botões em torno de uma página da Web. Devido a esse problema do Chrome, o recurso de exibição automática do teclado pode não funcionar no navegador Chrome em dispositivos de toque. Como solução alternativa, execute `chrome --force-renderer-accessibility`, ou você pode abrir uma nova guia no navegador, digitar `chrome://accessibility` e ativar o suporte à **API de acessibilidade nativa** para páginas específicas ou para todas as páginas. Além disso, ao publicar um aplicativo contínuo, você pode publicar o Chrome com o comutador `--force-renderer-accessibility`. [HDX-20858]
- No redirecionamento de conteúdo do navegador, depois de iniciar um vídeo do YouTube usando o player 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 é redimensionado, deixando um fundo preto na área completa da página. Como solução alternativa, clique no botão de tela cheia e selecione o modo de teatro. [HDX-11294]

Substituição

October 19, 2023

Os anúncios neste artigo destinam-se a fornecer um aviso prévio sobre plataformas, produtos Citrix e recursos que estão sendo eliminados gradualmente para que você possa tomar decisões de negócio oportunas. A Citrix monitora o uso e os comentários dos clientes para determinar quando serão eliminados. Os anúncios podem ser alterados em versões subsequentes e nem sempre incluirão todos os recursos ou funcionalidades preteridos. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo da Política de suporte ao ciclo de vida do produto. Para obter informações sobre a opção de serviço LTSR (Long Term Service Release), consulte https://support.citrix.com/article/CTX205549.

Substituições e remoções

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

Substituições

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

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Parâmetro `DedicatedTenancy` usado no comando `New-ProvScheme`	2303		Use o parâmetro `TenancyType`
License Server VPX	2206	11.17.2 compilação 35000	—
Disco não gerenciado para provisionar VMs em ambientes do Azure	2206		Use discos gerenciados
Redirecionamento de host para cliente (URL)	2203	—	Redirecionamento de conteúdo bidirecional

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress` usados em ambientes locais e na nuvem.	2203	—	—
Citrix Files para Windows e Citrix Files para Outlook do metainstalador de VDA.	2203	—	Use os instaladores autônomos.
Componente WEM Agent do metainstalador de VDA.	2203	—	—
Opção Wake on LAN integrada ao SCCM para Remote PC Access.	2012	—	Use o recurso Wake on LAN autônomo.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Citrix SCOM Management Packs para XenApp and XenDesktop, Provisioning Services e StoreFront. Para ver as versões do produto que podem ser monitoradas, consulte a documentação do Citrix SCOM Management Packs.	1912	—	Use o Director para monitorar e gerenciar sua implantação. Para obter mais informações sobre SCOM EOL e alternativas, consulte https://support.citrix.com/article/CTX266943.
Mobility SDK / Mobile SDK (do antigo Citrix Labs)	7.16	—	Substituído por configurações da política de experiência móvel e experiências nativas para áreas de trabalho e aplicativos hospedados.
Suporte do VDA para configuração da política "Automatic installation of in-box printer drivers".	7.16	—	Nenhuma. Configuração de política suportada com VDAs somente em sistemas operacionais anteriores (Windows 7, Windows Server 2012 R2 e versões anteriores).

Remoções

Os itens removidos foram removidos do Citrix Virtual Apps and Desktops ou não são mais suportados por ele.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Ferramentas de suporte Citrix (SupportabilityTool_x64 .msi) do VDA Meta-Installer.	—	2212	—
Citrix License Administration Console (incluído pela última vez no Windows License Server 11.16.3 build 30000 e removido no Windows License Server v11.16.6 build 31000).	2003	2006	Use o Citrix Licensing Manager.
Suporte ao adaptador gráfico Citrix Indirect Display Driver (IDD) no Windows 10 versão 1709 e versões anteriores.	2003	2003	Use VDAs do Citrix Virtual Apps and Desktops 7 1912 LTSR.
Codificação de hardware com GPUs Nvidia (NVENC) usando drivers de exibição GRID 9 ou anteriores.	2003	2003	Use drivers de exibição 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 SSPR (Redefinição de Senha de Autoatendimento).	2003	2006	—

Item	Substituição anunciada na versão	Removido na versão	Alternativa
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 .NET Framework versão 4.8.
VDAs no Windows Server 2012 R2.	1912	2003	Instale VDAs em um sistema operacional compatível.
Componente de migração de aplicativo AppDNA da edição Premium do Citrix Virtual Apps and Desktops.	1909	2003	—
Instalação do Studio em máquinas de 32 bits (x86).	1909	2003	Instale em um sistema operacional x64 compatível.
Suporte para gancho do Excel em aplicativos integrados. Isso foi usado para criar ícones separados da barra de tarefas para cada pasta de trabalho do Microsoft Excel 2010.	1909	1909	—
Componentes principais do servidor no Windows Server 2012 R2 (incluindo Service Packs). Inclui: Delivery Controller, Studio e Director.	1906	2003	Instale em um sistema operacional compatível mais recente.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para bancos de dados de monitoramento, log de configuração e configuração do site nas versões 2008 R2, 2012 e 2014 do Microsoft SQL Server (incluindo todos os Service Packs e edições).	1906	2003	Instale bancos de dados em uma versão compatível do Microsoft SQL Server.
Suporte para VDAs no Windows 10 em plataformas x86.	1906	1909*	Instale VDAs em um sistema operacional x64 compatível. *Este recurso ainda é suportado no Citrix Virtual Apps and Desktops 7 1912 LTSR.
Remoção do Citrix Smart Tools Agent da mídia de instalação do Citrix Virtual Apps and Desktops.	1903	1906	—
Remoção das opções do Delivery Controller para os seguintes produtos no fim da vida útil 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.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte do StoreFront aos protocolos TLS 1.0 e TLS 1.1 entre Citrix Virtual Apps and Desktops (anteriormente XenApp e XenDesktop) e Citrix Receiver, e Workspace Hub.	7.17	2203	Atualize Citrix Receivers para um aplicativo Citrix Workspace compatível com o protocolo TLS 1.2. Para obter mais informações sobre o aplicativo Citrix Workspace, consulte https://docs.citrix.com/en-us/citrix-workspace-app.
Suporte do StoreFront para usuários acessarem áreas de trabalho em sites do Desktop Appliance	1811	1912	Use o Desktop Lock para casos de uso não associados ao domínio.
Suporte para a tecnologia de exibição remota Framehawk	1811	1903	Use Thinwire com o transporte adaptativo ativado.
Suporte para Citrix Smart Scale em todas as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop). Essa funcionalidade chegará ao Fim da Vida Útil em 31 de maio de 2019.	1808	1906	Considere usar o Virtual Apps and Desktops Service no Citrix Cloud para melhorar a funcionalidade de gerenciamento de energia.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para Microsoft .NET Framework versões 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 e 4.7 por Citrix StoreFront, Citrix VDAs, Citrix Studio, Citrix Director e Citrix Delivery Controller.	7.18	1808	Atualize para .NET Framework versão 4.7.1 ou posterior. (O instalador instala automaticamente o .NET Framework 4.7.1 se ainda não estiver instalado.)
Suporte para Linux VDA no Red Hat Enterprise Linux 7.3.	7.18	1808	Instale o Linux VDA em uma versão posterior do Red Hat Enterprise Linux.
Suporte para o Linux VDA no SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Instale o Linux VDA na versão SUSE suportada.
Suporte para driver Citrix WDDM em VDAs	7.16	7.16	O driver Citrix WDDM não é mais instalado em VDAs.
VDAs no Windows 10 versão 1511 (Threshold 2) e versões anteriores de SO de sessão única Windows, incluindo Windows 8.x e Windows 7 (consulte https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (e 7.12)	7.16	Instale VDAs com SO de sessão única no Windows 10 versão mínima 1607 (Redstone 1) ou canais semestrais mais recentes. Se estiver usando 1607 LTSB, recomendamos um VDA 7.15. 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.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Desktop Composition Redirection (anteriormente conhecido como DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Use Thinwire.
Experiência clássica do Citrix Receiver para Web (interface de usuário “bolhas verdes”)	7.15 LTSR (e StoreFront 3.12)	1903	Experiência unificada do Citrix Receiver para Web.
Componentes principais no Windows Server 2012 e no Windows Server 2008 R2 (incluindo Service Packs). Inclui: Delivery Controller, Studio, Director, StoreFront, License Server e Universal Print Server.	7.15 LTSR	7.18	Instale componentes em um sistema operacional compatível.
Recurso SSPR (Redefinição de Senha de Autoatendimento) 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.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Redirecionamento Flash	7.15 LTSR	1912	Crie conteúdo de vídeo como Vídeo HTML5. Use o Redirecionamento de vídeo HTML5 para conteúdo gerenciado e o Redirecionamento de conteúdo de navegador para sites públicos. Para obter mais informações, consulte a nota Fim da Vida Útil do Redirecionamento Flash.
Integração do Citrix Online (produto Goto) com o StoreFront	7.14 (e StoreFront 3.11)	StoreFront 3.12	—
A conta de usuário CtxAppVCOMAdmin, que foi criada durante a instalação do VDA e adicionada ao grupo local de administradores na máquina VDA, não é mais criada. O mecanismo "COM" subjacente também é removido.	7.14	7.14	O serviço Windows CtxAppVService executa a mesma função. Ele é instalado e configurado automaticamente e não requer interação com o usuário.
Suporte ao componente UpsServer do Universal Print Server no Windows Server 2008 de 32 bits	7.14	7.14	Instale em um sistema operacional compatível mais recente.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
StoreFront e Receiver para Web no Internet Explorer 8	7.13	7.13	—
Opção de instalação da linha de comando de VDA /no_appv para impedir a instalação de componentes Citrix App-V	7.13	7.13	Use a opção de instalação da linha de comando /exclude "Citrix Personalization for App-V –VDA".
O instalador do produto completo não instala mais o snap-in Citrix.Common.Commands em novas instalações e o remove automaticamente ao atualizar as instalações existentes.	7.13	7.13	Alguns comandos do PowerShell fornecidos pelo snap-in Citrix.Common.Commands ainda estão disponíveis no XenApp 6.5 SDK.
Funcionalidade parcial para manipular dados de ícones fornecidos pelos cmdlets *-CtxIcon.	7.13	7.13	Agora fornecidos por cmdlets *-BrokerIcon no Broker Service.
Modo Thinwire legado	7.12	7.16	Use Thinwire. Se você estiver usando o modo Thinwire legado no Windows Server 2008 R2, migre para o Windows Server 2012 R2 ou Windows Server 2016 e use o Thinwire.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
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 com suporte 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 isso, primeiro atualize para o XenDesktop 7.6 LTSR (com a última CU); em seguida, atualize para a versão mais recente do Citrix Virtual Desktops (anteriormente XenDesktop) ou para a versão LTSR.
Instalação do Delivery Controller, Director, StoreFront ou License Server em máquinas 32 bits (x86).	7.12	7.16	Instale em um sistema operacional x64 compatível.
Concessão de conexão	7.12	7.16	Use cache de host local.
XenDesktop 5.6 usado no Windows XP. Instalações de VDA no Windows XP não são suportadas.	7.12	7.16	Instale VDAs em um sistema operacional compatível.
Suporte para conexões CloudPlatform	7.12	2003	Use outro hipervisor ou serviço de nuvem compatível.

Item	Substituição anunciada na versão	Removido na versão	Alternativa
Suporte para conexões do Azure Classic (também conhecido como Gerenciamento de Serviços do Azure)	7.12	2003	Considere usar o Virtual Apps and Desktops Service no Citrix Cloud.
Funcionalidade AppDisks (e a integração do AppDNA no Studio, que a suporta)	7.13	2003	Use o Citrix App Layering.
Funcionalidade Personal vDisk	7.15	2006†	Use a camada de usuário Citrix App Layering ou a tecnologia de camada de personalização do usuário.

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

Requisitos do sistema

September 13, 2023

Introdução

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

Revise Preparar a instalação antes de iniciar uma instalação.

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

mídia de instalação Citrix também contém alguns desses softwares de pré-requisitos.

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

Para obter informações sobre globalização, consulte o artigo do Knowledge Center CTX119253.

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

Requisitos de hardware

Os valores de RAM e espaço em disco são além dos requisitos para a imagem do produto, sistema operacional e outros softwares no computador. Seu desempenho varia, dependendo da sua configuração. Sua configuração inclui os recursos que você usa, além do número de usuários e outros fatores. Usar apenas o mínimo pode resultar em desempenho lento.

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

Componente	Mínimo
Todos os componentes principais e o StoreFront em um servidor, apenas para avaliação, não uma implantação de produção	5 GB de RAM
Todos os componentes principais e o StoreFront em um servidor, para uma implantação de teste ou um pequeno ambiente de produção	12 GB de RAM
Delivery Controller (mais espaço em disco necessário para o cache de host local)	5 GB de RAM, disco rígido de 800 MB, banco de dados: consulte a Orientação para dimensionamento
Studio	1 GB de RAM, disco rígido de 100 MB
Director	2 GB de RAM, disco rígido de 200 MB
StoreFront	2 GB de RAM, consulte a documentação do StoreFront para obter recomendações de disco
Servidor de licenças	2 GB de RAM; consulte a documentação de licenciamento para obter recomendações de disco

Dimensionamento de VMs que fornecem áreas de trabalho e aplicativos

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

Para mais informações:

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

Microsoft Visual C++

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

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

Delivery Controller

Sistemas operacionais compatíveis:

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

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente se ele (ou uma versão posterior) ainda não estiver instalado.
- Windows PowerShell 3.0, 4.0 ou 5.0.
- Microsoft Visual C++ 2015-2019 redistribuível.

Banco de dados

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

- 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 2019 com atualização cumulativa 15 é instalado ao instalar o Controller, se uma instalação existente suportada do SQL Server não for detectada.
  - Para atualizações, nenhuma versão existente do SQL Server Express é atualizada.
- SQL Server 2016 SP2, edições Express, Standard e Enterprise.

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

- Instâncias de cluster de failover AlwaysOn do SQL Server
- Grupos de disponibilidade AlwaysOn do SQL Server (incluindo grupos de disponibilidade básica)
- Espelhamento de banco de dados do SQL Server

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

Considerações sobre o cache de host local: o Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o cache de host local usa de modo autônomo. O cache de host local não requer nenhum componente do SQL Server Express que não seja o SQL Server Express LocalDB.

- Ao instalar um Controller, o Microsoft SQL Server Express LocalDB 2019 com atualização cumulativa 15 é instalado para uso com o recurso de Cache de Host Local. (Esta instalação é separada da instalação padrão do SQL Server Express para o banco de dados do site.)
- Ao atualizar um Controller, a versão existente do Microsoft SQL Server Express LocalDB não é atualizada automaticamente. Para obter requisitos e procedimentos de substituição, consulte Substituir SQL Server Express LocalDB.

Mais informações sobre o banco de dados:

- Banco de dados
- CTX114501 lista os bancos de dados suportados mais atuais
- Orientação de dimensionamento do banco de dados
- Cache do host local

Web Studio

> **Nota:**
>
> - Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois

> consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.
> - O Web Studio é um console de gerenciamento baseado na web que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. Ele foi projetado para melhorar a experiência do usuário e geralmente responde mais rápido do que o Citrix Studio, o console de gerenciamento baseado no Windows. Consulte Instalar o Web Studio.

Sistemas operacionais compatíveis:

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

Citrix Director

Sistemas operacionais compatíveis:

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

Requisitos:

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

Citrix Profile Management:

- Certifique-se de que o Citrix Profile Management e o Citrix Profile Management WMI Plug-in estejam instalados no VDA (página de **componentes adicionais** no assistente de instalação) e se o Citrix Profile Management Service estiver sendo executado para exibir os detalhes do perfil do usuário no Director.

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

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

Navegadores compatíveis para visualização do Director:

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

A resolução de tela ideal recomendada para visualização do Director é 1366 x 1024.

Virtual Delivery Agent (VDA) para SO de sessão única

Sistemas operacionais compatíveis:

- Windows 11
- Windows 10 (somente x64), qualquer versão que esteja atualmente no suporte base.
  - Para obter suporte à edição, consulte o artigo do Knowledge Center CTX224843.
  - Para ver os problemas conhecidos da Citrix com a versão 1709, consulte o artigo do Knowledge Center CTX229052.

Requisitos:

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

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

Vários recursos de aceleração de multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado no computador em que você instala o VDA. Se o computador não tiver o Media Foundation instalado, os recursos de aceleração de multimídia não serão instalados e não funcionarão. Não remova o Media Foundation do computador depois de instalar o software da Citrix. Caso contrário, os usuários não podem fazer logon no computador. Na maioria das edições Windows de SO de sessão única suportadas, o suporte ao Media Foundation já

está instalado e não pode ser removido. No entanto, as edições N não incluem certas tecnologias relacionadas à mídia; você pode obter esse software da Microsoft ou de terceiros. Para obter mais informações, consulte Preparar a instalação.

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

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

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

Virtual Delivery Agent (VDA) para SO multissessão

Sistemas operacionais compatíveis:

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

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

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

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

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

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

- Windows Media Redirection

- Redirecionamento de vídeo HTML5
- Redirecionamento de Webcam HDX RealTime

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

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

Recursos de virtualização e hosts

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

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

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

Hipervisores compatíveis:

- **Citrix Hypervisor (anteriormente XenServer)**

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

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

- **Microsoft System Center Virtual Machine Manager**

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

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

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

- **Nutanix Acropolis**

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

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

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

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

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

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

Hosts de nuvem pública compatíveis:

- **Amazon Web Services (AWS)**

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

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

- **Microsoft Azure Resource Manager**

  Para obter informações sobre como usar Microsoft Azure Resource Manager para provisionar máquinas virtuais, consulte 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 da Licença Hybrid Rights. Para obter informações sobre a Licença Hybrid Rights, consulte Transition and Trade-Up (TTU) com Hybrid Rights. Para obter informações sobre como adicionar uma licença, consulte Criar um site.
- As fontes de informação levam você para a documentação do Citrix DaaS. Se você estiver familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local tem várias diferenças.
  - No Citrix DaaS, a interface de gerenciamento é conhecida como Full Configuration. No Citrix Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio.
  - As atualizações do Citrix DaaS são lançadas aproximadamente a cada quatro semanas. Portanto, você notará que certos recursos disponíveis com o Citrix DaaS não estão disponíveis na versão local.

Níveis funcionais do Active Directory

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

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

HDX

Áudio

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

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

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

HDX e entrega do Windows Media

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

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

HDX 3D Pro

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

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

- GPU Passthrough está disponível com:
  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere e VMware ESX, onde é referido como Virtual Direct Graphics Acceleration (vDGA)
  - Microsoft Hyper-V no Windows Server 2016, onde é referido como Discrete Device Assignment (DDA).
- vGPU está disponível com:

  - Citrix Hypervisor
  - Nutanix AHV
  - VMware vSphere

Veja 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 igual ou superior a 2,3 GHz.

Unidade de processamento gráfico (GPU):

- Para compressão baseada em CPU (incluindo compressão sem perda), o HDX 3D Pro suporta qualquer adaptador de exibição 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 suportadas pelo driver GRID 10 (consulte NVIDIA GRID). A NVIDIA GRID oferece uma alta taxa de quadros, resultando em uma experiência de usuário altamente interativa.
- A aceleração gráfica virtualizada é suportada pela família de processadores Intel Xeon E3 da plataforma gráfica do datacenter. 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 suportada com o AMD RapidFire nas placas de servidor AMD FirePro S-series. Consulte Solução de virtualização AMD.

Dispositivo do usuário:

- O HDX 3D Pro suporta todas as resoluções de monitor que são suportadas pela GPU no computador host. Para um desempenho ideal com as especificações mínimas recomendadas de dispositivo do 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 de usuário tenham pelo menos 1 GB de RAM e CPU com uma velocidade de clock igual ou superior a 1,6 GHz. O uso do codec de compressão profunda padrão, que é exigido em conexões de baixa largura de banda, requer uma CPU mais poderosa, a menos que a decodificação seja feita no hardware. Para um desempenho ideal, a Citrix recomenda que os dispositivos de usuário tenham pelo menos 2 GB de RAM e uma CPU dual-core com velocidade de clock de 3 GHz ou superior.
- Para acesso a vários monitores, a Citrix recomenda dispositivos de usuário com CPUs quad-core.
- Os dispositivos do usuário não precisam de uma GPU para acessar áreas de trabalho ou aplicativos fornecidos com o HDX 3D Pro.
- O aplicativo Citrix Workspace deve ser instalado.

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

Universal Print Server

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

O componente UpsServer é compatível com:

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

Requisitos:

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

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

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

Para obter mais informações, consulte Provisionar impressoras.

Outros

Somente o Citrix License Server 11.17.2 e posterior são suportados. Para obter mais informações, consulte Licenciamento.

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 Product Matrix para obter mais informações sobre compatibilidade de versão.

Para ver as versões compatíveis com o StoreFront, consulte os requisitos do sistema StoreFront.

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

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

Várias NICs são suportadas.

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

Consulte Acesso a aplicativo local para obter informações do navegador suportado para esse recurso.

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

Este produto oferece suporte ao PowerShell versões 3 a 5.

Visão técnica geral

June 28, 2023

O Citrix Virtual Apps and Desktops é uma solução de virtualização que oferece ao pessoal de TI o controle de máquinas virtuais, aplicativos, licenciamento e segurança, ao mesmo tempo que fornece acesso em qualquer lugar para qualquer dispositivo.

O Citrix Virtual Apps and Desktops permite que:

- Usuários finais executem aplicativos e áreas de trabalho independentemente da interface e do sistema operacional do dispositivo.
- Administradores gerenciem a rede e controlem o acesso a partir de dispositivos selecionados ou de todos os dispositivos.
- Administradores gerenciem uma rede inteira a partir de um único datacenter.

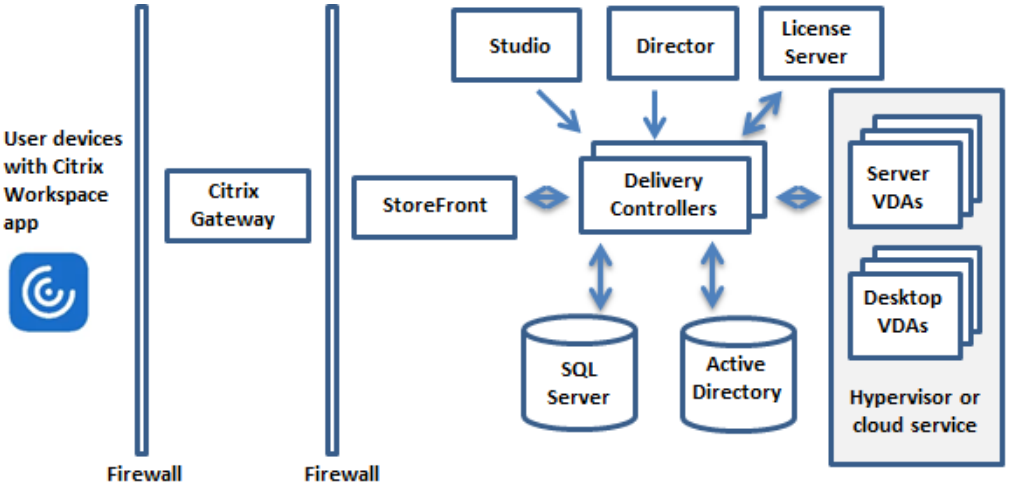
O Citrix Virtual Apps and Desktops compartilha uma arquitetura unificada chamada FlexCast Management Architecture (FMA). Os principais recursos de FMA são a capacidade de executar várias versões do Citrix Virtual Apps ou do Citrix Virtual Desktops a partir de um único site e o provisionamento integrado.

Saiba mais sobre alterações a nomes de produto.

Componentes principais

Este artigo é de grande utilidade se você for novo no Citrix Virtual Apps and Desktops. Se você tiver atualmente um farm de XenApp 6.x ou anterior, ou um site de XenDesktop 5.6 ou anterior, consulte também Alterações em 7.x.

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



Delivery Controller

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

- Distribuir aplicativos e áreas de trabalho
- Autenticar e gerenciar o acesso do usuário
- Trocar conexões entre usuários e suas áreas de trabalho e aplicativos
- Otimizar conexões do usuário
- Balancear a carga das conexões

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

O Monitor Service coleta dados históricos e os coloca no banco de dados de monitoramento. Esse 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 das áreas de trabalho iniciando-as e interrompendo-as com base na demanda e na configuração administrativa.

Banco de dados

Pelo menos um banco de dados do Microsoft SQL Server é necessário para que cada site armazene informações de configuração e sessão. Esse banco de dados armazena os dados coletados e gerenciados pelos serviços que compõem o Controller. Instale o banco de dados no seu datacenter e certifique-se de que ele tenha uma conexão persistente com o Controller.

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

Virtual Delivery Agent (VDA)

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

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

O termo "VDA"é frequentemente usado 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 multissessão. Os VDAs para sistemas operacionais Windows multissessão permitem que vários usuários se conectem ao servidor de uma só vez. Os VDAs para sistemas operacionais Windows de sessão única permitem que apenas um usuário se conecte à área de trabalho de cada vez. VDAs da Linux também estão disponíveis.

Citrix StoreFront

O StoreFront autentica usuários e gerencia as lojas de áreas de trabalho e aplicativos que os usuários acessam. Ele pode hospedar sua loja de aplicativos empresariais, que dá aos usuários acesso de autoatendimento às áreas de trabalho e aplicativos que você disponibiliza para eles. Ele também mantém o controle das 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 pontos de extremidade (como áreas de trabalho virtuais), o aplicativo Citrix Workspace oferece aos usuários acesso rápido, seguro e de autoatendimento a documentos, aplicativos e áreas de trabalho. O aplicativo Citrix Workspace fornece acesso sob demanda a aplicativos Windows, web e Software como Serviço (SaaS). Para dispositivos que não podem instalar o software do aplicativo Citrix Workspace específico ao dispositivo, o aplicativo Citrix Workspace para HTML5 fornece uma conexão por meio de um navegador da Web compatível com HTML5.

Studio

Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Esta documentação do produto abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte Citrix Virtual Apps and Desktops 7 2212 ou anterior.

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

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

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

Citrix Director

O Director é uma ferramenta baseada na Web que permite que as equipes de suporte de TI e de suporte técnico monitorem um ambiente, solucionem problemas antes que eles se tornem críticos ao sistema e executem 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 mostra:

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

O Director usa os dados heurísticos e de desempenho do ICA capturados pelo dispositivo Citrix Gateway para criar análises a partir dos dados e apresentá-los aos administradores.

Você também pode visualizar e interagir com as sessões de um usuário através do Director, usando a 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 de cada sessão de usuário, e com o Studio, para alocar arquivos de licença. Um site deve ter pelo menos um License Server para armazenar e gerenciar seus arquivos de licença.

Hipervisor ou outro serviço

O hipervisor ou outro serviço hospeda as máquinas virtuais no seu site. Essas podem ser as VMs que você usa para hospedar aplicativos e áreas de trabalho, e VMs que você usa para hospedar os componentes do Citrix Virtual Apps and Desktops. Um hipervisor é instalado em um computador host dedicado inteiramente a executar o hipervisor e hospedar máquinas virtuais.

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

Embora muitas implantações exijam um hipervisor, você não precisa de um para fornecer o Remote PC Access. Um hipervisor também não é necessário quando você estiver usando o Provisioning Services (PVS) para provisionar VMs.

Componentes adicionais

Os componentes a seguir também podem ser incluídos nas implantações do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte a documentação pertinente.

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 dispositivos

de usuário. O PVS não requer um hipervisor para fazer isso, portanto, você pode usá-lo para hospedar máquinas físicas. O PVS se comunica com o Controller para fornecer recursos aos usuários.

Citrix Gateway

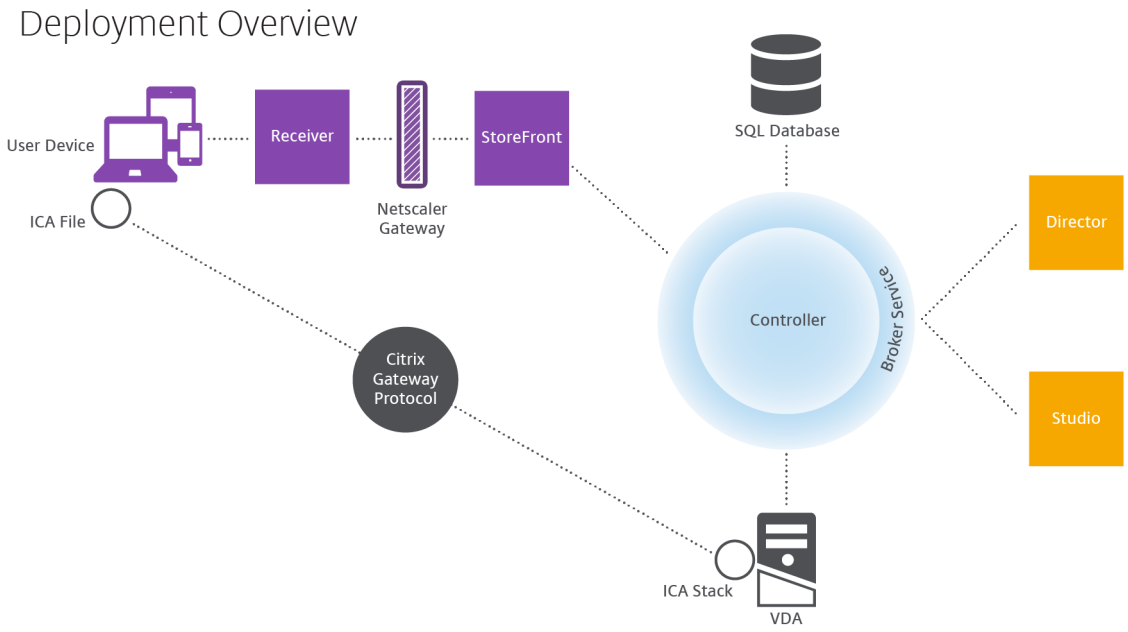
Quando os usuários se conectam de fora do firewall corporativo, o Citrix Virtual Apps and Desktops pode usar a tecnologia Citrix Gateway (anteriormente Access Gateway e NetScaler Gateway) para proteger essas conexões com TLS. O dispositivo virtual Citrix Gateway ou VPX é um dispositivo VPN SSL implantado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

Citrix SD-WAN

Em implantações em que áreas de trabalho virtuais são entregues a usuários em locais remotos, como filiais, a tecnologia Citrix SD-WAN pode ser empregada para otimizar o desempenho. Os repetidores aceleram o desempenho entre WANs. Com repetidores na rede, os usuários na filial experimentam um desempenho semelhante a 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 seja degradada na filial quando um arquivo grande ou um trabalho de impressão é enviado pela rede. A otimização de WAN HDX fornece compressão indexada e eliminação de duplicação de dados, reduzindo drasticamente os requisitos de largura de banda e melhorando o desempenho.

Como funcionam as implantações típicas

Um site é composto de computadores com funções dedicadas que permitem escalabilidade, alta disponibilidade e failover, além de fornecer uma solução segura por design. Um site consiste em computadores desktop e servidores instalados por VDA, e no Delivery Controller, que gerencia o acesso.



O VDA permite que os usuários se conectem a áreas de trabalho e aplicativos. Ele é instalado em máquinas virtuais no datacenter para a maioria dos métodos de entrega, mas também pode ser instalado em PCs físicos para Remote PC Access.

O Controller é composto de serviços independentes do Windows que gerenciam recursos, aplicativos e áreas de trabalho e otimizam e equilibram as conexões do usuário. Cada site tem um ou mais Controllers. Como as sessões são afetadas pela latência, largura de banda e confiabilidade de rede, coloque todos os Controllers na mesma LAN, se possível.

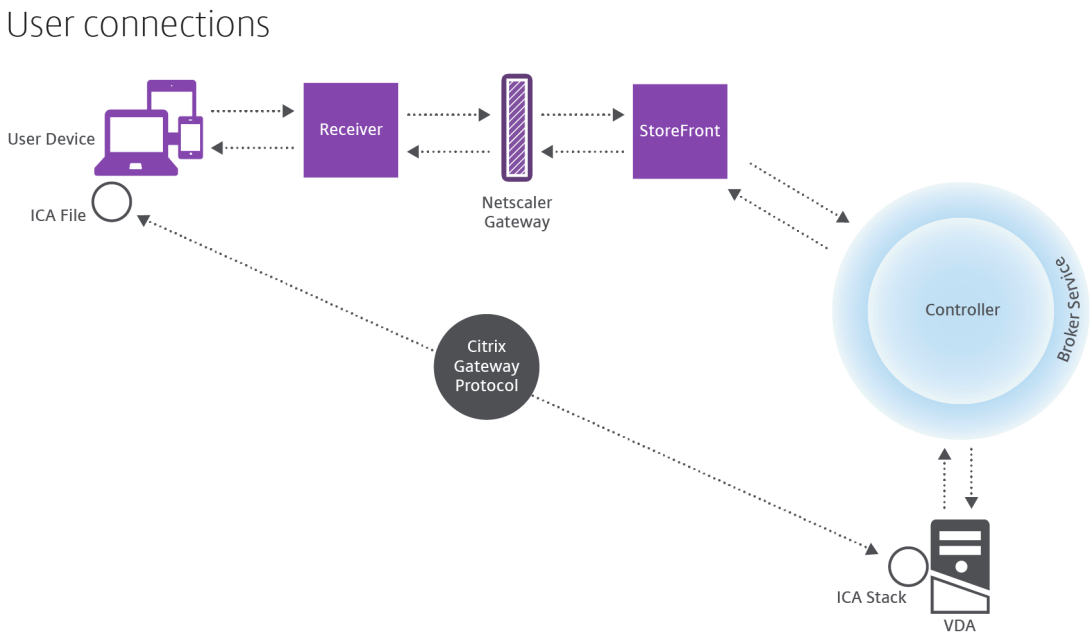
Os usuários nunca acessam diretamente o Controller. O VDA serve como um intermediário entre os usuários e o Controller. Quando os usuários fazem logon usando o StoreFront, suas credenciais passam para o Broker Service no Controller. Em seguida, o Broker Service obtém perfis e recursos disponíveis com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

Como as conexões do usuário são tratadas

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

O usuário seleciona a área de trabalho física ou virtual ou o aplicativo virtual que é necessário.

As credenciais do usuário seguem por esse caminho para acessar o Controller, que determina quais recursos são necessários através da comunicação 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 Broker Service determina quais áreas de trabalho e aplicativos o usuário tem permissão para acessar.

Depois que as credenciais forem verificadas, as informações sobre aplicativos ou áreas de trabalho disponíveis são enviadas de volta ao usuário por meio do caminho entre o StoreFront e o aplicativo Citrix Workspace. Quando o usuário seleciona aplicativos ou áreas de trabalho dessa lista, a informação volta pelo mesmo caminho para o Controller. O Controller determina o VDA apropriado para hospedar aplicativos ou área de trabalho específicos.

O Controller envia uma mensagem ao VDA com as credenciais do usuário e depois envia todos os dados sobre o usuário e a conexão ao 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 enviados para o aplicativo Citrix Workspace como parte da conversa do protocolo entre o aplicativo Citrix Workspace e o StoreFront, ou são convertidos em um arquivo ICA (Independent Computing Architecture) e baixados. Estando o site 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).

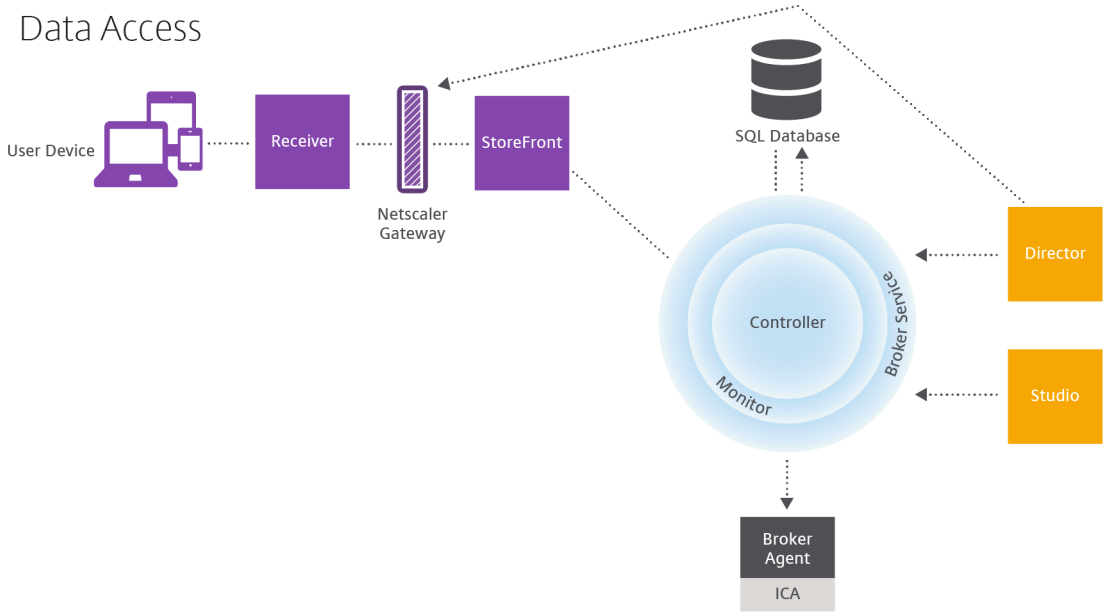
A conexão entre o aplicativo Citrix Workspace e o VDA usa o Citrix Gateway Protocol (CGP). Se uma conexão for perdida, o recurso de Confiabilidade da Sessão permite que o usuário se reconecte ao VDA em vez de ter que reiniciar através da infraestrutura de gerenciamento. A confiabilidade da sessão pode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

Depois que o cliente se conecta ao VDA, o VDA notifica o Controller que o usuário está conectado. Em

seguida, o Controller envia a informação para o banco de dados do site e inicia o registro de dados no banco de dados de monitoramento.

Como funciona o acesso a dados

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



No Controller, o Broker Service relata dados de sessão para cada sessão no computador fornecendo dados em tempo real. O Monitor Service 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 Broker Service. Ele acessa apenas dados em tempo real. O Director se comunica com o Broker Service (por meio de um plug-in no Broker Agent) para acessar o banco de dados do site.

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

Entregar áreas de trabalho e aplicativos

Você configura os computadores que fornecem aplicativos e áreas de trabalho com catálogos de máquinas. Em seguida, você cria grupos de entrega que especificam os aplicativos e áreas de

trabalho que estarão disponíveis (usando as máquinas nos catálogos) e quais usuários podem acessá-los. Opcionalmente, você pode 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 o aplicativo ou áreas de trabalho 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 instalado. Elas também têm os mesmos aplicativos ou áreas de trabalho 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 dispositivos de destino individualmente ou coletivamente usando ferramentas de distribuição eletrônica de software (ESD) de terceiros.

Os tipos de máquinas válidas são:

- **SO multissessão:** máquinas virtuais ou físicas com sistema operacional multissessão. Usado para entregar aplicativos publicados no Citrix Virtual Apps (também conhecidos como aplicativos hospedados baseados em servidor) e áreas de trabalho publicadas no Citrix Virtual Apps (também conhecidas como áreas de trabalho hospedadas em servidor). Essas máquinas permitem que vários usuários se conectem a elas de uma só vez.
- **SO de sessão única:** máquinas virtuais ou físicas com sistema operacional de sessão única. Usado para entregar áreas de trabalho VDI (áreas de trabalho que executam SOs de sessão única que podem, opcionalmente, ser personalizadas), aplicativos hospedados em VM (aplicativos de SOs de sessão única) e áreas de trabalho físicas hospedadas. Apenas um usuário de cada vez pode se conectar a cada uma dessas áreas de trabalho.
- **Remote PC Access:** permite que os usuários remotos acessem seus PCs físicos no escritório a partir de qualquer dispositivo que esteja executando o aplicativo Citrix Workspace. Os PCs de escritório são gerenciados por meio 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 Citrix Virtual Apps and Desktops Image Management e Criar catálogos de máquinas.

Grupos de entrega

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

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

Você define quais recursos os usuários do grupo de entrega podem acessar. Por exemplo, para entregar aplicativos diferentes para usuários diferentes, você pode instalar todos os aplicativos na imagem mestre de um catálogo e criar máquinas suficientes nesse catálogo para distribuir entre os vários grupos de entrega. Depois, configure cada grupo de entrega para entregar um diferente subconjunto de aplicativos que estão instalados nas máquinas.

Para obter mais informações, consulte Criar grupos de entrega.

Grupos de aplicativos

Os grupos de aplicativos oferecem vantagens de gerenciamento de aplicativos e controle de recursos em comparação com o uso de mais grupos de entrega. Usando o recurso de restrição de marcas, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciando mais máquinas. Uma restrição de marca pode ser considerada como uma subdivisão (ou partição) de máquinas em um grupo de entrega. Os grupos de aplicativos também podem ser úteis ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Para obter mais informações, consulte Criar grupos de aplicativos.

Mais informações

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

Active Directory

June 28, 2023

O Active Directory é necessário para autenticação e autorização. A infraestrutura Kerberos no Active Directory é usada para garantir a autenticidade e a confidencialidade das comunicações com os Delivery Controllers. Para obter informações sobre o Kerberos, consulte a documentação da Microsoft.

O artigo Requisitos do sistema lista os níveis funcionais suportados para a floresta e o domínio. Para usar a Modelagem de Políticas, o controlador de domínio deve estar em execução no Windows Server 2003 até o Windows Server 2012 R2. Isso não afeta o nível funcional do domínio.

Este produto suporta:

- **Implantações nas quais as contas de usuário e as contas de computador existem em domínios em uma única floresta do Active Directory.** Contas de usuário e computador podem existir em domínios arbitrários dentro de uma única floresta. Todos os níveis funcionais do domínio e níveis funcionais da floresta são suportados neste tipo de implantação.
- **Implantações nas quais existem contas de usuário em uma floresta do Active Directory diferente da floresta do Active Directory que contém as contas de computador de Controllers e áreas de trabalho virtuais.** Neste tipo de implantação, os domínios que contêm as contas de computador do Controller e da área de trabalho virtual devem confiar nos domínios que contêm contas de usuário. Relações de confiança de floresta ou externas podem ser usadas. Todos os níveis funcionais do domínio e níveis funcionais da floresta são suportados neste tipo de implantação.
- **Implantações nas quais existam contas de computador para Controllers em uma floresta do Active Directory diferente de uma ou mais florestas adicionais do Active Directory que contêm as contas de computador das áreas de trabalho virtuais.** Neste tipo de implantação deve existir uma confiança bidirecional entre os domínios que contêm as contas de computador do Controller e todos os domínios que contêm as contas de computador de área de trabalho virtual. Neste tipo de implantação, todos os domínios que contêm contas de computador do Controller ou de áreas de trabalho virtuais devem estar no nível funcional "Windows 2000 nativo"ou superior. Todos os níveis funcionais da floresta são suportados.
- **Controladores de domínio graváveis.** Os controladores de domínio somente leitura não são suportados.

Opcionalmente, os Virtual Delivery Agents (VDAs) podem usar informações publicadas no Active Directory para determinar em quais Controllers eles podem se registrar (descoberta). Esse método é suportado principalmente para compatibilidade com versões anteriores e está disponível somente se os VDAs estiverem na mesma floresta do Active Directory que os Controllers. Para obter informações sobre esse método de descoberta, consulte Detecção baseada em unidade organizacional do Active Directory e CTX118976.

> **Nota:**
>
> Não altere o nome do computador ou a associação de domínio de um Delivery Controller após a configuração do site.

Implantar em um ambiente multifloresta do Active Directory

Estas informações se aplicam às versões mínimas XenDesktop 7.1 e XenApp 7.5. Elas não se aplicam 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 pode usar encaminhadores de DNS ou encaminhadores condicionais para pesquisa de nomes e registro. Para permitir que os usuários apropriados do Active Directory criem contas de computador, use o Assistente para Delegação de Controle. Consulte a documentação da Microsoft para obter detalhes sobre esse assistente.

Nenhuma zona DNS inversa é necessária na infraestrutura DNS se os encaminhadores DNS apropriados estiverem incluídos 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 seguintes informações para adicionar a chave do registro ao VDA e aos Delivery Controllers:

> **Cuidado:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. 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 da configuração de DNS reverso se o seu espaço de nome de DNS for diferente daquele do Active Directory.

Uma entrada de registro foi adicionada para evitar a ativação indesejada da autenticação NTLM em VDAs, o que é menos seguro que o Kerberos. Essa 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 multifloresta de confiança bidirecional que permite que você remova a autenticação baseada em NTLM durante o processo de registro inicial.

Se as relações de confiança externas estiverem em vigor 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 Controllers. (SIDs são incluídos nos resultados do cmdlet `Get-BrokerController`.)

Quando houver relações de confiança externas em vigor, 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.

Depois de adicionar a chave do registro `ListOfSIDs` e editar o arquivo `brokeragent.exe.config`, reinicie o Citrix Desktop Service 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
External	Não transitivo	Unidirecional ou bidirecional	Sim
Floresta	Transitivo	Unidirecional ou bidirecional	Sim
Atalho	Transitivo	Unidirecional ou bidirecional	Sim
Realm	Transitivo ou não transitivo	Unidirecional ou bidirecional	Não

Para obter mais informações sobre ambientes complexos do Active Directory, consulte CTX134971.

Bancos de dados

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

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

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

Cada Delivery Controller se comunica com o banco de dados do site. A autenticação do Windows é necessária entre o Controller e os bancos de dados. Um Controller pode ser desconectado ou desligado sem afetar outros Controllers no site. Isso significa, no entanto, que o banco de dados do site

forma um ponto único de falha. Se o servidor de banco de dados falhar, as conexões existentes continuarão a funcionar até que um usuário faça logoff ou se desconecte. Para obter informações sobre o comportamento da conexão quando o banco de dados do site fica indisponível, consulte Cache de host local.

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

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

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

Alta disponibilidade

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

- **Grupos de disponibilidade AlwaysOn (incluindo os grupos de disponibilidade básica):** esta solução de alta disponibilidade e recuperação de desastres de nível empresarial introduzida no SQL Server 2012 permite maximizar a disponibilidade de um ou mais bancos de dados. Os grupos de disponibilidade AlwaysOn exigem que as instâncias do SQL Server residam nos nós do Windows Server Failover Clustering (WSFC). Para obter mais informações, consulte Windows Server Failover Clustering 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 aconteça em questão de segundos, de modo que os usuários não sejam afetados no geral. Esse método é mais caro do que outras soluções porque são necessárias licenças completas do SQL Server em cada servidor de banco de dados. Não é possível usar a edição do SQL Server Express em um ambiente espelhado.
- **Clustering de SQL:** a tecnologia de cluster do Microsoft SQL pode ser usada para permitir automaticamente que um servidor assuma as tarefas e responsabilidades de outro servidor que falhou. No entanto, configurar essa solução é mais complicado, e o processo de failover automático geralmente é mais lento do que alternativas como o espelhamento de SQL.

- **Usando os recursos de alta disponibilidade do hipervisor:** com este método, você implanta o banco de dados como uma máquina virtual e usa os recursos de alta disponibilidade do seu hipervisor. Essa solução é menos dispendiosa do que o espelhamento porque usa o seu software de hipervisor existente e você também pode usar a edição do SQL Server Express. No entanto, o processo de failover automático é mais lento, pois pode demorar até que outro computador seja iniciado para o banco de dados, o que pode interromper o serviço para os usuários.

O recurso de cache de host local complementa as práticas recomendadas de alta disponibilidade do SQL Server. O Cache de Host Local permite que os usuários se conectem e se reconectem a aplicativos e áreas de trabalho 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 no modo de alta disponibilidade, o que permite que os usuários continuem acessando suas áreas de trabalho e aplicativos. No modo de alta disponibilidade, o VDA aceita conexões ICA diretas dos usuários, em vez de conexões intermediadas pelo Controller. Use esse recurso somente na rara eventualidade de a comunicação com todos os Controllers falhar. O recurso não é uma alternativa a outras soluções de alta disponibilidade. Para obter mais informações, consulte CTX 127564.

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

Instalar o software de banco de dados

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

A instalação padrão usa as permissões e contas de serviço 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 do serviço de rede nessa configuração. O Controller não requer nenhuma função ou permissão adicional do SQL Server.

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

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

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

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

Use o Windows Update para manter o SQL Server atualizado.

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

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

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

Você pode alterar a localização do banco de dados de monitoramento e registro de configuração em log posteriormente, depois de criar o site. Consulte Alterar a localização dos bancos de dados.

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

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

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

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

Configuração automática

Se você tiver os privilégios de banco de dados necessários, selecione **Create and set up databases from Studio** na página **Databases** do assistente de criação de site. Em seguida, forneça os nomes e endereços dos principais bancos de dados.

Se existir um banco de dados 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 indagado se deseja que o banco de dados seja criado para você. Quando você confirma essa ação, o Web Studio cria automaticamente os bancos de dados e, em seguida, aplica os scripts de inicialização para os bancos de dados principal e de réplica.

Configuração com script

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

1. Na página **Databases** do assistente de criação de site, selecione **Generate scripts to manually set up**. Essa ação gera os três tipos de scripts a seguir para cada um dos seguintes bancos de dados principal e de réplica: banco de dados de site, monitoramento e log.

   - *Script contendo "SysAdmin"no nome*. Um script que cria os bancos de dados e o login do Delivery Controller. Essas tarefas exigem direitos securityadmin.
   - *Script contendo "DbOwner"no 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"no nome*. todas as tarefas em um script, independentemente dos direitos necessários.

   Você pode indicar onde armazenar os scripts.

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

2. Forneça esses scripts ao seu administrador de banco de dados. O assistente de criação do site para automaticamente nesse momento. Posteriormente, você será solicitado para continuar a criação do site quando voltar a ele.

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

- Usar um agrupamento que termine com `_CI_AS_KS`. Recomendamos o uso de um agrupamento que termine com `_100_CI_AS_KS`.

- Para um desempenho ideal, ative o instantâneo de leitura confirmada do SQL Server. Para obter detalhes, consulte CTX 137161.
- Recursos de alta disponibilidade configurados, se aplicável.
- Para configurar o espelhamento, primeiro defina o banco de dados para usar o modelo de recuperação completa (o modelo simples é o padrão). Faça backup do banco de dados principal para um arquivo e copie-o para o servidor de espelhamento. Em seguida, restaure o arquivo de backup no servidor de espelhamento. Por fim, comece a espelhar 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 do banco de dados do SQL Server de alta disponibilidade (se a alta disponibilidade estiver configurada)
- Executar cada um dos scripts `xxx\\_Principal.sql` nas instâncias principais do banco de dados do SQL Server.

Consulte a documentação da Microsoft para obter informações detalhadas sobre SQLCMD.

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

O Web Studio solicita que você continue a criação do site. Você retornará à página **Databases**. Insira os endereços. Se algum dos servidores que hospedam um banco de dados não puder ser contatado, uma mensagem de erro é exibida.

Permissões necessárias para configurar bancos de dados

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

Operação	Finalidade	Função de servidor	Função de banco de dados
Criar um banco de dados	Criar um banco de dados vazio apropriado	`dbcreator`	

Operação	Finalidade	Função de servidor	Função de banco de dados
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 espelhado)	Adicionar um login do Controller ao servidor de banco de dados atualmente na função de espelho de um banco de dados espelhado	securityadmin*	
Remover o Controller	Remover o Controller do site	**	db_owner
Atualizar um esquema	Aplicar atualizações de esquema ou hotfixes		db_owner

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

** Quando um Controller é removido de um site, o logon do Controller no servidor de banco de dados não é removido. Isso ocorre para evitar a possibilidade de remover um login utilizado por outros serviços, que não este produto Citrix, na mesma máquina. O login deve ser removido manualmente se não for mais necessário. Esta ação requer associação de função de servidor securityadmin.

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

Scripts preferenciais de direitos de bancos de dados

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

Usando o PowerShell, você pode especificar os direitos preferidos de banco de dados. 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 do Citrix, sem precisar entrar em contato com um administrador de banco de dados.

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

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

Para obter mais informações, consulte a ajuda do cmdlet.

Formatos de endereço de banco de dados

Você pode especificar um endereço de banco de dados em uma das seguintes formas:

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

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

Alterar a localização dos bancos de dados

Depois de criar um site, você pode alterar o local dos bancos de dados de monitoramento e registro de configuração em log. (Não é possível alterar a localização do banco de dados do site.) Quando você altera a localização de um banco de dados:

- Os dados 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 quando recuperados.
- A primeira entrada de log no novo banco de dados indica que ocorreu uma alteração no banco de dados, mas não identifica o banco de dados anterior.

Não é possível alterar a localização do banco de dados de registro de configuração em log quando o registro em log obrigatório está habilitado.

Para alterar a localização de um banco de dados:

1. Verifique se uma versão suportada do Microsoft SQL Server está instalada no servidor onde você deseja que o banco de dados resida. Configure recursos de alta disponibilidade conforme necessário.
2. Entre no Web Studio e selecione **Settings** no painel esquerdo.

3. Localize o bloco **Database** e selecione **Edit**.
4. Na página **Manage Database**, selecione o banco de dados para o qual deseja especificar um novo local e selecione **Change Database** na barra de ações.
5. Especifique o novo local e o nome do banco de dados.
6. Se você quiser que o Studio crie o banco de dados, e tiver as permissões apropriadas, clique em **Done**. Quando solicitado, clique em **Done** e o Web Studio criará o banco de dados automaticamente. O Web Studio tenta acessar o banco de dados usando suas credenciais. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. Em seguida, o Web Studio carrega o esquema do banco de dados para o banco de dados. As credenciais são retidas apenas durante o período de criação do banco de dados.
7. Se você não quiser que o Web Studio crie o banco de dados ou não tiver permissões suficientes, clique em **Generate database script**. Os scripts gerados incluem instruções para criar manualmente o banco de dados e um banco de dados espelhado, se necessário. Antes de carregar o esquema, verifique se o banco de dados está vazio e que pelo menos um usuário tenha permissão para acessar e alterar o banco de dados.

Mais informações

- Database sizing tool.
- Sizing the site database e Configuring connection strings quando usar soluções de alta disponibilidade do SQL Server.

Métodos de entrega

June 28, 2023

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

- **Aplicativo instalado:** o aplicativo faz parte da imagem base da área de trabalho. O processo de instalação envolve dll, exe e outros arquivos copiados para a unidade de imagem, além de modificações do registro. Para obter detalhes, consulte Criar catálogos de máquinas.

- **Aplicativo por streaming (Microsoft App-V):** o aplicativo é incluído em um perfil e entregue às áreas de trabalho em toda a rede sob demanda. Arquivos de aplicativos e configurações de registro são colocados em um contêiner na área de trabalho virtual e isolados do sistema operacional base e uns dos outros. Esse isolamento ajuda a resolver problemas de compatibilidade. Para obter detalhes, consulte Implementar e entregar aplicativos App-V.
- **Aplicativo em camadas (Citrix App Layering):** cada camada contém um único aplicativo, agente ou sistema operacional. Ao integrar uma camada de SO, uma camada de plataforma (VDA, agente Citrix Provisioning) e muitas camadas de aplicativos, um administrador pode criar facilmente imagens novas e implantáveis. A camada simplifica a manutenção contínua, pois existe um sistema operacional, um agente e um aplicativo em uma única camada. Quando você atualiza a camada, todas as imagens implantadas que contêm essa camada são atualizadas. 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 uma área de trabalho. Um usuário acessa o aplicativo do Windows hospedado diretamente a partir de um dispositivo de ponto de extremidade ou área de trabalho VDI, ocultando o fato de que o aplicativo está sendo executado remotamente. Para obter detalhes, consulte Criar grupos de entrega.
- **Aplicativo local:** um aplicativo implantado no dispositivo de ponto de extremidade. A interface do aplicativo aparece dentro da sessão VDI hospedada do usuário, mesmo sendo executada no endpoint. Para obter detalhes, consulte Acesso ao aplicativo local e redirecionamento de URL.

Nas áreas de trabalho, pode-se utilizar áreas de trabalho publicadas ou áreas de trabalho VDI.

Áreas de trabalho e aplicativos publicados do Citrix Virtual Apps

Use máquinas com SO multissessão para entregar aplicativos publicados e áreas de trabalho publicadas do Citrix Virtual Apps and Desktops.

Caso de uso:

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

Benefícios e considerações:

- Solução gerenciável e dimensionável em seu data center.
- Solução de entrega de aplicativos mais rentável.

- Os aplicativos hospedados são gerenciados centralmente e os usuários não podem modificar o aplicativo. Isso oferece uma experiência de usuário consistente, segura e confiável.
- Os usuários devem estar online para acessar seus aplicativos.

Experiência do usuário:

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

Processamento, hospedagem e entrega de aplicativos:

- O processamento de aplicativos ocorre em máquinas de hospedagem, em vez de ocorrer nos dispositivos do usuário. A máquina de hospedagem pode ser uma máquina física ou virtual.
- Aplicativos e áreas de trabalho residem em uma máquina com SO multissessão.
- As máquinas ficam disponíveis através de catálogos de máquinas.
- Máquinas de catálogos de máquinas são organizadas em grupos de entrega que fornecem o mesmo conjunto de aplicativos para grupos de usuários.
- As máquinas com SO multissessão suportam grupos de entrega que hospedam áreas de trabalho ou aplicativos ou ambos.

Gerenciamento e atribuição de sessões:

- As máquinas com SO multissessão executam várias sessões a partir de uma única máquina para fornecer vários aplicativos e áreas de trabalho a vários usuários conectados simultaneamente. Cada usuário requer uma única sessão a partir da qual pode executar todos os aplicativos hospedados.

  Por exemplo, um usuário faz logon e solicita um aplicativo. Uma sessão nessa máquina fica indisponível para outros usuários. Um segundo usuário faz logon e solicita um aplicativo que essa máquina hospeda. Uma segunda sessão na mesma máquina fica agora indisponível. Se ambos os usuários solicitarem mais aplicativos, nenhuma sessão adicional será necessária porque cada usuário pode executar vários aplicativos usando a mesma sessão. Se mais dois usuários efetuarem logon e solicitarem áreas de trabalho e duas sessões estiverem disponíveis nessa mesma máquina, essa única máquina agora estará usando quatro sessões para hospedar quatro usuários diferentes.

- Dentro do grupo de entrega ao qual um usuário está atribuído, uma máquina no servidor menos carregado é selecionada. Uma máquina com disponibilidade de sessão é atribuída aleatoriamente para entregar aplicativos a um usuário quando esse usuário fizer logon.

Aplicativos hospedados em VM

Use máquinas com SO de sessão única para fornecer aplicativos hospedados por VM

Caso de uso:

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

Benefícios e considerações:

- Os aplicativos e áreas de trabalho na imagem principal são gerenciados, hospedados e executados com segurança em máquinas dentro de seu data center, oferecendo uma solução de entrega de aplicativos mais econômica.
- No logon, os usuários podem ser atribuídos aleatoriamente a uma máquina dentro de um grupo de entrega configurado para hospedar o mesmo aplicativo. Você também pode atribuir estaticamente uma única máquina para entregar um aplicativo a um único usuário sempre que o usuário fizer logon. As máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de várias sessões não é suportada em máquinas com SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega quando faz logon, e os usuários devem estar online para acessar seus aplicativos.
- Esse método pode aumentar a quantidade de recursos do servidor para processamento de aplicativos e aumentar a quantidade de armazenamento de dados dos usuários.

Experiência do usuário:

- A mesma experiência de aplicativos que se tem ao hospedar aplicativos compartilhados em máquinas com SO multissessão.

Processamento, hospedagem e entrega de aplicativos:

- O mesmo que as máquinas com SO multissessão, exceto se trata de máquinas virtuais de SO de sessão única.

Gerenciamento e atribuição de sessões:

- As máquinas com SO de sessão única executam uma única sessão de área de trabalho a partir de uma única máquina. Quando acessa apenas aplicativos, um 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.

Áreas de trabalho VDI

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

As áreas de trabalho VDI são hospedadas em máquinas virtuais e fornecem a cada usuário um sistema operacional de área de trabalho.

As áreas de trabalho VDI requerem mais recursos do que as áreas de trabalho publicadas, mas não exigem que os aplicativos instalados neles suportem sistemas operacionais baseados em servidor. Além disso, dependendo do tipo de área de trabalho VDI que você escolher, essas áreas de trabalho podem ser atribuídas a usuários individuais. Isso permite aos usuários um alto nível de personalização.

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

- **Área de trabalho aleatória não persistente, também conhecida como área de trabalho VDI em pool:** cada vez que um usuário faz logon em uma dessas áreas de trabalho, esse usuário se conecta a uma área de trabalho selecionada a partir de um pool de áreas de trabalho. Esse pool é baseado em uma única imagem mestre. Todas as alterações na área de trabalho são perdidas quando a máquina é reiniciada.
- **Área de trabalho não persistente estática:** durante o primeiro logon, uma área de trabalho é atribuída a um usuário a partir de um pool de áreas de trabalho. (Cada máquina no pool é baseada em uma única imagem mestre.) Após o primeiro uso, cada vez que um usuário faz logon para usar uma área de trabalho, esse usuário se conecta à mesma área de trabalho que foi atribuída na primeira utilização. Todas as alterações na área de trabalho são perdidas quando a máquina é reiniciada.
- **Área de trabalho persistente estática:** ao contrário de outros tipos de áreas de trabalho VDI, os usuários podem personalizar totalmente estas áreas de trabalho. Durante o primeiro logon, uma área de trabalho é atribuída a um usuário a partir de um pool de áreas de trabalho. Os logons subsequentes desse usuário conectam-se à mesma área de trabalho que foi atribuída na primeira utilização. As alterações na área de trabalho são mantidas quando a máquina é reiniciada.

Remote PC Access

O Remote PC Access é um recurso do Citrix Virtual Apps and Desktops que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

O Remote PC Access usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam áreas de trabalho e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos que os necessários para implantar o Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

Para obter mais informações, consulte Acesso remoto ao PC.

Portas de rede

June 28, 2023

Informações completas da porta de rede são fornecidas em Communication Ports Used by Citrix Technologies.

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

Você pode precisar de informações sobre a porta:

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

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

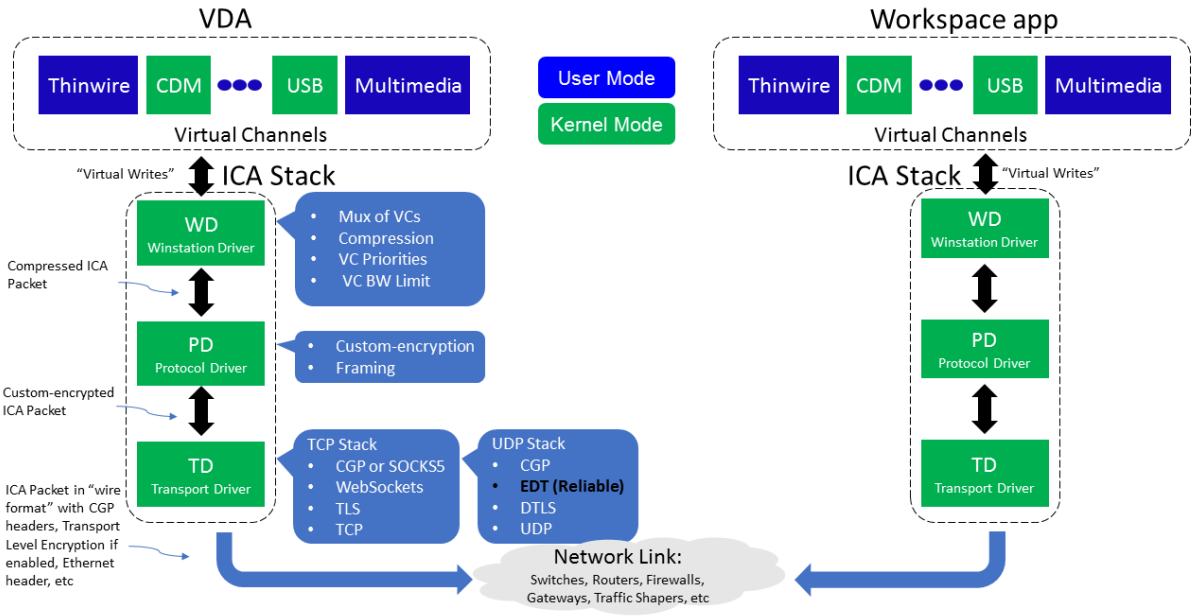
Além disso, os sistemas operacionais no VDA e Delivery Controller exigem portas de entrada para uso próprio. Consulte a documentação do Microsoft Windows para obter detalhes.

HDX

June 28, 2023

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

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



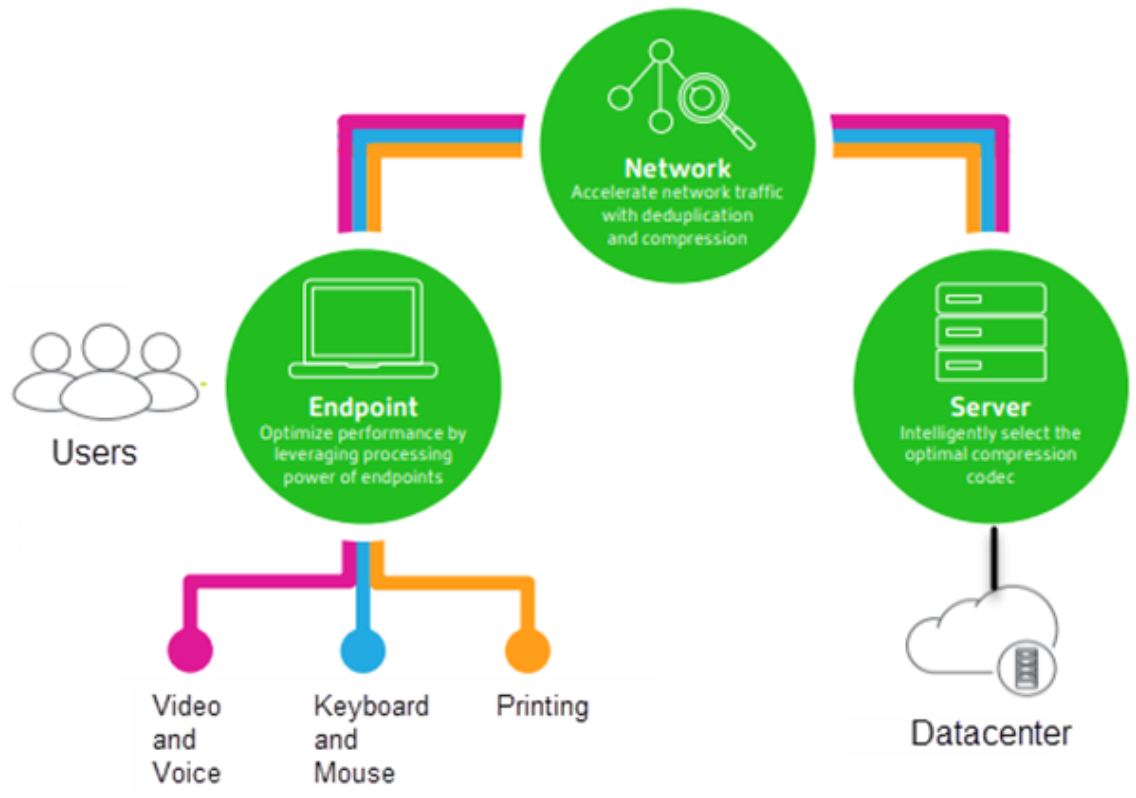
O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente

- Compactação adaptativa
- Desduplicação de dados

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

- **Redirecionamento inteligente** - o redirecionamento inteligente examina a atividade da tela, comandos de aplicativos, dispositivo de ponto de extremidade e recursos de rede e servidor para determinar instantaneamente como e onde renderizar uma atividade de aplicativo ou área de trabalho. A renderização pode ocorrer no dispositivo de ponto de extremidade ou no servidor de hospedagem.
- **Compactação adaptativa** - a compactação adaptativa permite que exibições multimídia avançadas sejam entregues em conexões de rede fina. O HDX primeiro avalia algumas variáveis, como o tipo de entrada, dispositivo e exibição (texto, vídeo, voz e multimídia). Ele escolhe o codec de compactação ideal e a melhor proporção de utilização entre CPU e GPU. Em seguida, ele se adapta de forma inteligente com base em cada usuário e base únicos. Essa adaptação inteligente é por usuário, ou mesmo por sessão.



- **Desduplicação de dados** - a eliminação de duplicação do tráfego de rede reduz os dados agregados enviados entre cliente e servidor. Isso é feito aproveitando padrões repetidos em dados comumente acessados, como gráficos de bitmap, documentos, trabalhos de impressão e conteúdo de streaming. O armazenamento em cache desses padrões permite que somente as al-

terações sejam transmitidas através da rede, eliminando o tráfego duplicado. O HDX também suporta multicast de stream de multimídia, onde uma única transmissão de uma fonte é vista por vários assinantes em um local, em vez de uma conexão individual para cada usuário.

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

No dispositivo

O HDX usa a capacidade de computação dos dispositivos do usuário para melhorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários tenham uma experiência sem atropelos com o conteúdo multimídia em suas áreas de trabalho ou aplicativos virtuais. O controle do espaço de trabalho permite que os usuários pausem as áreas de trabalho e aplicativos virtuais e retomem o trabalho a partir de um dispositivo diferente no ponto em que pararam.

Na rede

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

Os recursos HDX se adaptam às mudanças no ambiente. Os recursos equilibram o desempenho e a largura de banda. Eles aplicam as melhores tecnologias para cada cenário de usuário, independentemente se a área de trabalho ou aplicativo é ou não acessados localmente na rede corporativa ou remotamente de fora do firewall corporativo.

No data center

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

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

HDX Insight

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

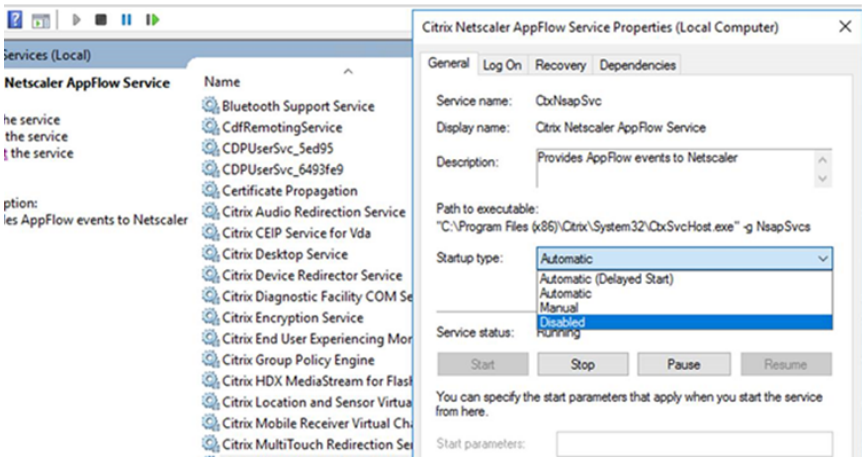
Você pode habilitar o NetScaler para usar o canal virtual HDX Insight para mover todos os pontos de dados necessários em um formato descompactado. Se você desabilitar esse recurso, o dispositivo NetScaler descriptografa e descompacta o tráfego ICA espalhado por vários canais virtuais. O uso de um único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

Requisitos mínimos:

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp e XenDesktop 7.17
- NetScaler versão 12.0 compilação 57.x
- Aplicativo Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.10
- Aplicativo Citrix Workspace para Mac 1808
- Citrix Receiver para Mac 12.8

Ativar ou desativar o canal virtual HDX Insight

Para desativar esse recurso, defina as propriedades do serviço Citrix NetScaler Application Flow como Desativado. Para ativar, defina o serviço como Automático. Em ambos os casos, recomendamos que você reinicie a máquina do servidor depois de alterar essas propriedades. Por padrão, esse serviço está habilitado (Automático).



Experimente os recursos HDX da sua área de trabalho virtual

- Para ver como o redirecionamento de conteúdo do navegador, uma das quatro tecnologias de redirecionamento multimídia HDX, acelera a entrega de conteúdo multimídia HTML5 e WebRTC:
  1. Baixe a extensão do navegador Chrome e instale-a na área de trabalho virtual.
  2. Para experimentar como o redirecionamento de conteúdo do navegador acelera a entrega de conteúdo multimídia para áreas de trabalho virtuais, assista a um vídeo em sua área

de trabalho a partir de um site que contenha vídeos HTML5, como o YouTube. Os usuários não sabem quando o redirecionamento de conteúdo do navegador está sendo executado. Para ver se o redirecionamento de conteúdo do navegador está sendo usado, arraste a janela do navegador rapidamente. Você verá um atraso ou deslocamento do quadro entre o visor e a interface do usuário. Você também pode clicar com o botão direito do mouse na página da Web e procurar **Sobre o redirecionamento do navegador HDX** no menu.

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

  1. Configure seu cliente Citrix para obter a máxima qualidade de áudio; consulte a documentação do aplicativo Citrix Workspace para obter detalhes.
  2. Reproduza arquivos de música usando um player de áudio digital (como o iTunes) em sua área de trabalho.

O HDX fornece uma experiência superior com gráficos e vídeos para a maioria dos usuários por padrão, e a configuração não é necessária. As configurações da política da Citrix que oferecem a melhor experiência para a maioria dos casos de uso são ativadas por padrão.

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

É bom saber:

- Para obter informações sobre suporte e requisitos para recursos HDX, consulte o artigo Requisitos do sistema. Exceto quando indicado de outra forma, os recursos HDX estão disponíveis para máquinas com Windows com SO multissessão e SO de sessão única suportadas, além de áreas de trabalho de acesso ao PC remoto.
- Este conteúdo descreve como otimizar a experiência do usuário, melhorar a escalabilidade do servidor ou reduzir os requisitos de largura de banda. Para obter informações sobre como usar as políticas da Citrix e as configurações de políticas, consulte a documentação de políticas da Citrix para esta versão.

- Em instruções que incluem a edição do registro, tenha cuidado: editar o registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Reconexão automática de cliente e confiabilidade da sessão

Ao acessar aplicativos ou áreas de trabalho hospedados, pode ocorrer interrupção de rede. Para experimentar uma reconexão mais descomplicada, oferecemos reconexão automática de cliente e confiabilidade da sessão Em uma configuração padrão, a confiabilidade da sessão é iniciada e, em seguida, ocorre a reconexão automática de cliente.

Reconexão automática de cliente:

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

- **Áreas de trabalho.** A janela da sessão fica acinzentada e um temporizador de contagem regressiva mostra o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela da sessão é fechada e uma caixa de diálogo aparece para o usuário contendo um temporizador de contagem regressiva mostrando o tempo até as tentativas de reconexão.

Durante a reconexão automática de cliente, as sessões reiniciam esperando que haja conectividade de rede. O usuário não pode interagir com sessões enquanto a reconexão automática de cliente estiver em andamento.

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

Configurações padrão de reconexão automática de cliente:

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

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

Confiabilidade da sessão:

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

- **Áreas de trabalho.** A janela de sessão torna-se translúcida e um temporizador de contagem regressiva mostra o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela torna-se translúcida e são lançados pop-ups de conexão interrompida na bandeja do sistema.

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

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

Configurações padrão de confiabilidade da sessão

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

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

NetScaler com reconexão automática de cliente e confiabilidade da sessão:

Se as políticas Multistream e Multiporta estiverem habilitadas no servidor e uma ou todas estas condições forem verdadeiras, a reconexão automática de cliente não funciona:

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

Taxa de transferência adaptativa HDX

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

de arquivos mais rápida, reprodução de vídeo mais uniforme, maior taxa de quadros e de resolução resulta em uma experiência de usuário melhorada.

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

> **Importante:**
>
> A taxa de transferência adaptativa HDX muda a forma como os buffers de saída são ajustados, movendo o mecanismo do cliente para o VDA, sem nenhuma configuração manual.

Esse recurso tem os seguintes requisitos:

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

Melhorar a qualidade da imagem enviada aos dispositivos do usuário

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

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

Melhorar o desempenho de videoconferências

Vários aplicativos populares de videoconferência são otimizados para a entrega com o Citrix 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 a videoconferência em uma sessão. Esta tecnologia transmite o tráfego da webcam através de um canal virtual

multimídia dedicado. Essa tecnologia usa menos largura de banda em comparação com o suporte de redirecionamento USB Plug-n-Play HDX isócrono e funciona bem em conexões WAN.

Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração Mic & Webcam do Desktop Viewer **Não usar meu microfone ou webcam**. Para evitar que os usuários mudem a compactação de vídeo da webcam HDX, desative o redirecionamento do dispositivo USB usando as configurações da política em Configurações de política em ICA policy settings > USB Devices policy.

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

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing

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 do software, adicione o seguinte valor de chave DWORD à chave de registro: HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Prioridades de tráfego de rede

As prioridades são atribuídas ao tráfego de rede através de várias conexões para uma sessão usando roteadores suportados pela qualidade de serviço. Quatro streams TCP e dois streams UDP estão disponíveis para transportar o tráfego ICA entre o dispositivo do usuário e o servidor:

- Streams TCP - tempo real, interativo, em segundo plano e em massa
- Streams UDP - voz e telas remotas Framehawk

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

Conexões de streaming multicanal são compatíveis com os VDAs (Virtual Delivery Agents) instalados em computadores Windows 10, Windows 8 e Windows 7. Fale com o seu administrador de rede para garantir que as portas do CGP (Common Gateway Protocol) definidas na configuração de política multiporta estejam atribuídas corretamente nos roteadores de rede.

A Qualidade de Serviço (QoS) é suportada somente quando várias portas de confiabilidade da sessão, ou as portas CGP, são configuradas.

> **Aviso:**
>
> Use a segurança de transporte quando usar esse recurso. A Citrix recomenda o uso de IPsec (Internet Protocol Security) ou TLS (Transport Layer Security). As conexões TLS só são suportadas quando as conexões atravessam um NetScaler Gateway compatível com ICA multistream Em uma rede corporativa interna, as conexões multistream com TLS não são suportadas.

Para definir a qualidade de serviço para várias conexões de streaming, adicione as seguintes configurações da política da Citrix a uma política (consulte Configurações de políticas de conexões multistream para obter detalhes):

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

  Configure explicitamente os firewalls nos VDAs para permitir o tráfego TCP adicional.
- Configuração do computador para multistream - esta configuração está desativada por padrão. Se você usar o Citrix NetScaler SD-WAN com suporte a multistream no seu ambiente, não será necessário definir essa configuração. Defina essa configuração da política quando usar roteadores de terceiros ou NetScaler SD-WAN legados para alcançar a Qualidade de Serviço (QoS) desejada.
- Configuração do usuário multistream - esta configuração está desativada por padrão.

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

Mostrar ou ocultar a barra de idiomas remota

A barra de idiomas exibe o idioma de entrada preferido em uma sessão de aplicativo. Se esse recurso estiver ativado (padrão), você poderá mostrar ou ocultar a barra de idiomas na interface do usuário **Preferências avançadas > Barra de idiomas** no aplicativo Citrix Workspace para Windows. Ao usar uma configuração de registro no lado VDA, você pode desativar o controle cliente do recurso da barra de idiomas. Se esse recurso estiver desativado, a configuração da interface do usuário cliente não entrará em vigor e a configuração atual por usuário determinará o estado da barra de idiomas. Para obter mais informações, consulte Melhorar a experiência do usuário.

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

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

Mapeamento de teclado Unicode

Citrix Receivers não Windows usam o layout do teclado local (Unicode). Se um usuário alterar o layout do teclado local e o layout do teclado do servidor (código de varredura), eles podem ficar fora de sincronia e a saída ficará incorreta. Por exemplo, o usuário-1 altera a configuração do teclado local de inglês para alemão. O usuário-1 então altera o teclado do lado do servidor para alemão. Mesmo que ambos os layouts de teclado sejam alemães, eles podem não estar em sincronia, o que causa a saída de caracteres incorretos.

Ativar ou desativar o mapeamento de layout de teclado Unicode

Por padrão, o recurso é desabilitado no lado do VDA. Para ativar o recurso, alterne o recurso usando o editor de registro regedit no VDA. Adicione a seguinte chave de registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: EnableKlMap

Tipo: DWORD

Valor: 1

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

Ativar modo compatível com mapeamento de layout de teclado Unicode

Por padrão, o mapeamento de layout de teclado Unicode conecta automaticamente algumas APIs do Windows para recarregar o novo mapa de layout do teclado Unicode quando você altera o layout do teclado no lado do servidor. Alguns poucos aplicativos não podem ser vinculados. Para manter a compatibilidade, você pode alterar o recurso para o modo compatível para dar suporte a esses aplicativos sem gancho de vinculação. Adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valor: 1

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

Canais virtuais Citrix ICA

June 28, 2023

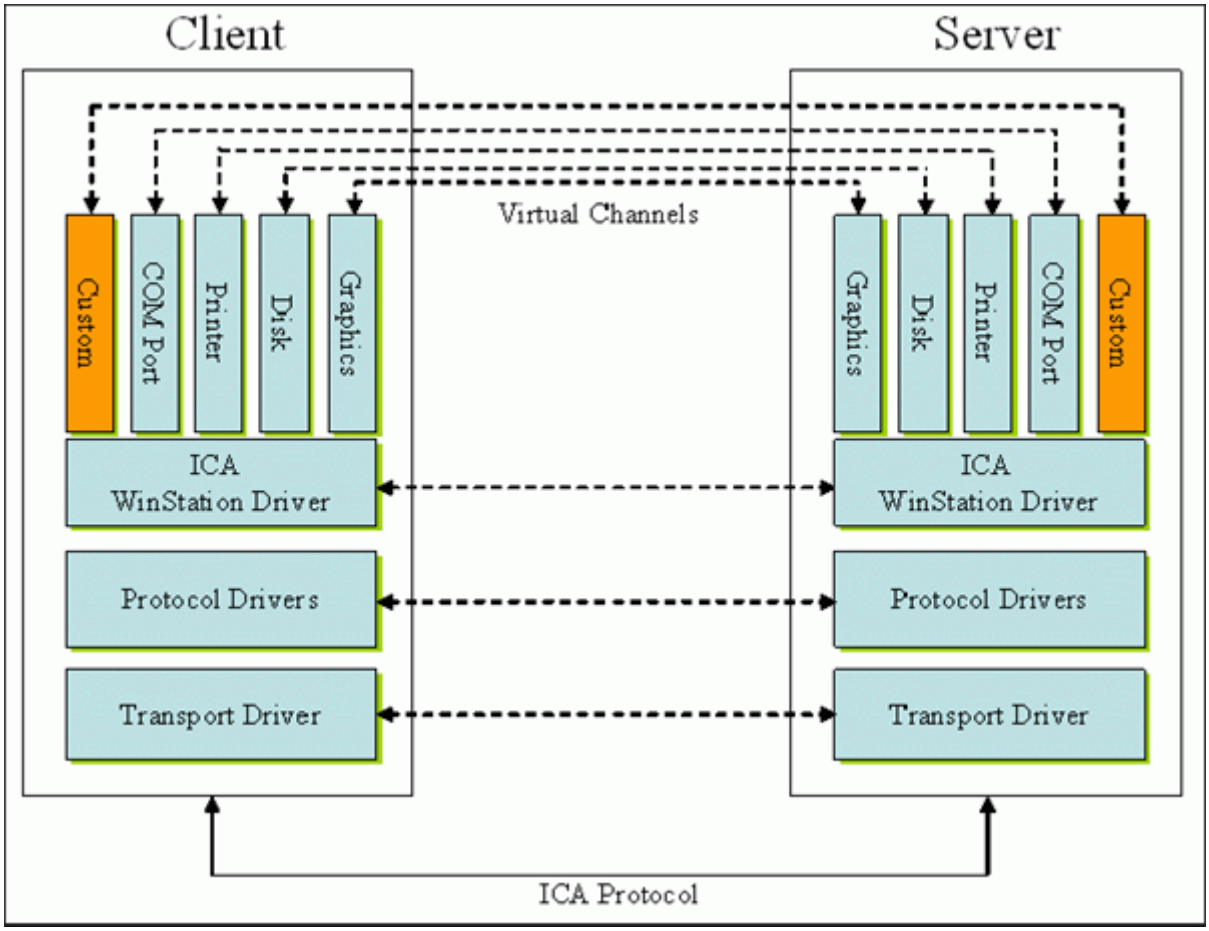
> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco.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

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

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

Às vezes, novos canais virtuais são lançados com novas versões dos servidores Citrix Virtual Apps and Desktops e produtos de aplicativos Citrix Workspace para oferecer mais funcionalidades.



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

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

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

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

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


Ou

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

- Thinwire3.0 (Obrigatório)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Área de transferência
- ClientComm
- ClientAudio
- LicenseHandler (Obrigatório)
- TWI (Obrigatório)
- SmartCard
- ICACTL (Obrigatório)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**
>
> Você pode desativar a funcionalidade específica do cliente removendo um ou mais desses valores da chave de registro. Por exemplo, se você quiser remover a Área de transferência cliente, remova a palavra **Clipboard**.

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

- vd3dn.dll —Canal virtual Direct3D usado para redirecionamento de composição de área de trabalho
- vdcamN.dll —Áudio bidirecional
- vdcdm30n.dll —Mapeamento da unidade cliente
- vdcom30N.dll –Mapeamento de porta COM cliente
- vdcpm30N.dll —Mapeamento da impressora cliente
- vdctln.dll —Canal de controles ICA
- vddvc0n.dll —Canal virtual dinâmico
- vdeuemn.dll —Monitoramento da experiência do usuário final
- vdgusbn.dll —Canal virtual USB genérico
- vdkbhook.dll —Passagem de chave transparente

- vdlfpn.dll —Canal de exibição Framehawk por UDP como transporte
- vdmmn.dll —Suporte multimídia
- vdmrvc.dll —Canal virtual do Mobile Receiver
- vdmtchn.dll –Suporte multitoque
- vdscardn.dll —Suporte a cartão inteligente
- vdsens.dll —Canal virtual de sensores
- vdspl30n.dll —UPD cliente
- vdsspin.dll —Kerberos
- vdtuin.dll —Interface do usuário transparente
- vdtw30n.dll —Cliente Thinwire
- vdtwin.dll —Contínuo
- vdtwn.dll —Twain

Alguns canais virtuais são compilados em outros arquivos. Por exemplo, o mapeamento da área de transferência está disponível em wfica32.exe

Compatibilidade com 64 bits

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

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

Canal virtual USB genérico

A implementação do canal virtual USB genérico usa dois drivers no modo kernel juntamente com o driver de canal virtual vdgusbn.dll:

- ctxusbm.sys

- ctxusbr.sys

Como funcionam os canais virtuais ICA

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

Módulos de canais virtuais carregados pelo Shell, por exemplo:

- EUEM
- Twain
- Área de transferência
- Multimídia
- Compartilhamento de sessão contínuo
- Fuso horário

Alguns são carregados como modo kernel, por exemplo:

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

Canal virtual gráfico no lado do servidor

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

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

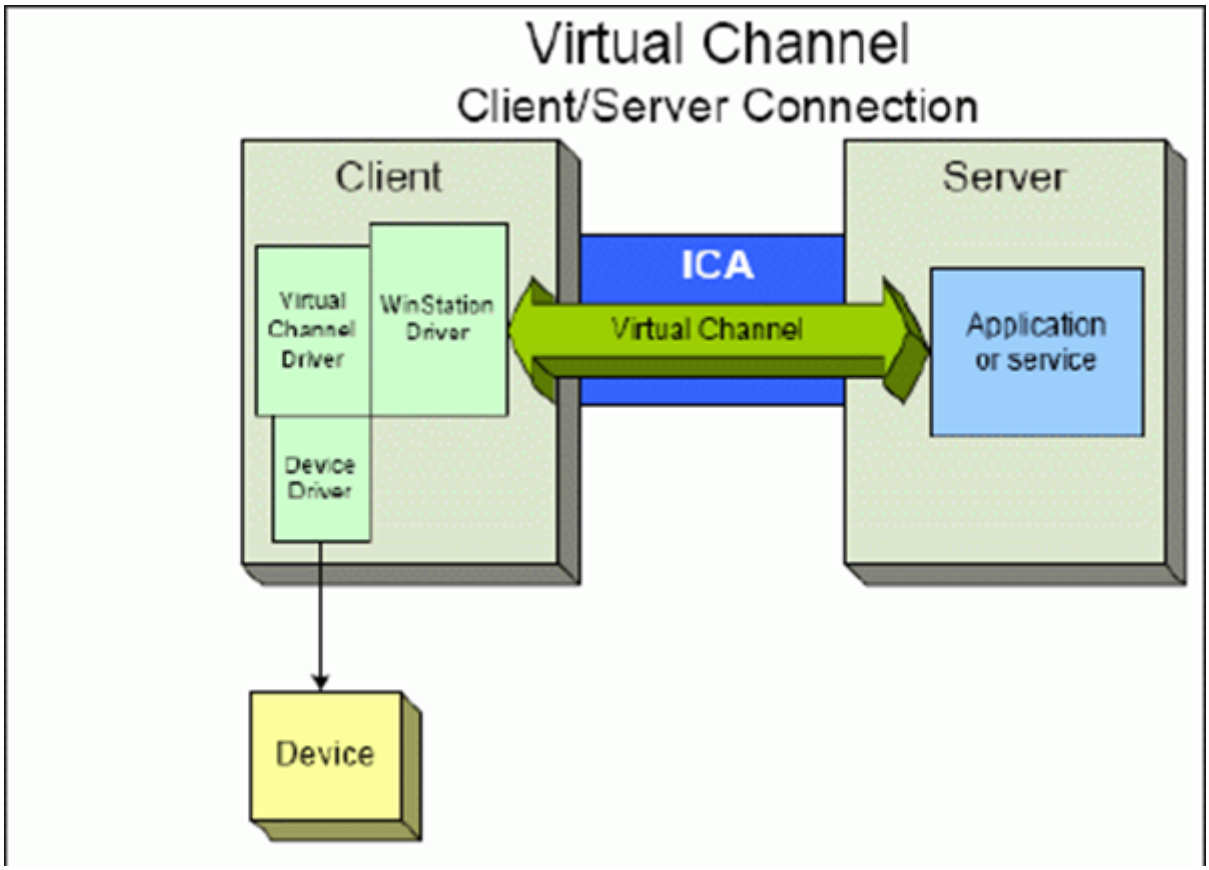
Hospedagem de canais especializados em serviços Windows

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

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops somente)

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

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



Esta ilustração mostra a troca de dados cliente-servidor usando um canal virtual.

1. O cliente se conecta ao servidor Citrix Virtual Apps and Desktops. O cliente passa informações sobre os canais virtuais aos quais dá suporte para o servidor.
2. O aplicativo do lado do servidor é iniciado, obtém um identificador para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.

3. O driver virtual cliente e o aplicativo do lado do servidor passam dados usando os dois métodos a seguir:
    - Se o aplicativo do servidor tiver dados para enviar ao cliente, os dados serão enviados para o cliente imediatamente. Quando o cliente recebe os dados, o driver do WinStation desmultiplexa os dados do canal virtual a partir do stream do ICA e os passa imediatamente para o driver virtual cliente.
    - Se o driver virtual cliente tiver dados para enviar para o servidor, os dados serão enviados na próxima vez que o driver do WinStation fizer a sondagem. Quando o servidor recebe os dados, eles são enfileirados até que o aplicativo de canal virtual os leia. Não há como alertar o aplicativo de canal virtual do servidor que os dados foram recebidos.
4. Quando o aplicativo do canal virtual do servidor é concluído, ele fecha o canal virtual e libera todos os recursos alocados.

Criando o seu próprio canal virtual usando o Virtual Channel SDK

> **Nota:**
>
> Os SDKs da Citrix estão disponíveis no portal Citrix Developer em https://developer.cloud.com.

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

> **Nota:**
>
> - O SDK de canal virtual requer que o WFAPI SDK para gravar no lado do servidor do canal virtual.
> - Devido à segurança aprimorada do Citrix Virtual Apps and Desktops, você deve especificar quais canais virtuais podem ser abertos em uma sessão do ICA. Para obter mais informações, consulte Configurações de política de lista de permissões de canal virtual.

Criando o seu próprio canal virtual usando o ICA Client Object SDK

Criar um canal virtual usando o ICA Client Object (ICO) é mais fácil do que usando o Virtual Channel SDK. Use o ICO criando um objeto nomeado no seu programa usando o método **CreateChannels**.

> **Importante:**
>
> Devido à segurança aprimorada, a partir da versão 10.00 do Citrix Receiver para Windows e posterior (e aplicativos Citrix Workspace para Windows), é necessária uma etapa extra ao criar um

> canal virtual ICO.

Funcionalidade de passagem de canais virtuais

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

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

- Mapeamento de porta COM cliente
- Client drive mapping
- Mapeamento da impressora cliente
- UPD cliente
- Monitoramento da experiência do usuário
- USB genérico
- Kerberos
- Suporte multimídia
- Suporte a cartão inteligente
- Passagem de chave transparente
- Twain

Com a natureza inerente de latência e fatores como compressão e descompressão e renderização sendo executada em cada salto, o desempenho pode ser afetado com cada salto adicional sobre o cliente. As áreas afetadas são:

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

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

Funcionalidade de passagem de canais virtuais entre uma sessão do Citrix Virtual Desktops e uma sessão do Citrix Virtual Apps

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

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

Oferecemos suporte aos seguintes canais virtuais tradicionais e suas funcionalidades:

- Cliente
- Mapeamento de porta COM cliente
- Client drive mapping
- Mapeamento da impressora cliente
- USB genérico (limitado pelo desempenho)
- Suporte multimídia
- Suporte a cartão inteligente
- SSON
- Passagem de chave transparente

A segurança e os canais virtuais ICA

A proteção da utilização é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança no decorrer deste documento.

Práticas recomendadas

Abra os canais virtuais quando se **Conectar** e **Reconectar**. Feche os canais virtuais quando fizer logoff e se **Desconectar**.

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

Nomenclatura de canais virtuais:

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

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

Os canais virtuais são referidos por um nome em ASCII de sete caracteres (ou mais curto). Em algumas versões anteriores do protocolo ICA, os canais virtuais eram numerados. Os números agora são atribuídos dinamicamente com base no nome em ASCII, facilitando a implementação. Os usuários que estão desenvolvendo códigos de canal virtual apenas para uso interno podem usar qualquer nome de sete caracteres que não entre em conflito com os canais virtuais existentes. Use

apenas números e maiúsculas e minúsculas em ASCII. Siga a convenção de nomenclatura existente ao adicionar seus próprios canais virtuais. Existem vários canais predefinidos. Os canais predefinidos começam com o identificador OEM CTX e são apenas para uso pela Citrix.

Suporte para salto duplo:

Canal virtual	O salto duplo é suportado?
Áudio	Não
Redirecionamento de conteúdo do navegador	Não
CDM	Sim
CEIP	Não
Área de transferência	Sim
Continuum (MRVC)	Não
Control VC	Sim
Redirecionamento de vídeo HTML5 (v1)	Sim
Teclado, Mouse	Sim
MultiTouch	Não
NSAPVC	Não
Impressão	Sim
SensVC	Não
Smartcard	Sim
Twain	Sim
USB VC	Sim
Dispositivos WAYCOM -K2M usando USB VC	Sim
Compressão de vídeo de webcam	Sim
Windows Media Redirection	Sim

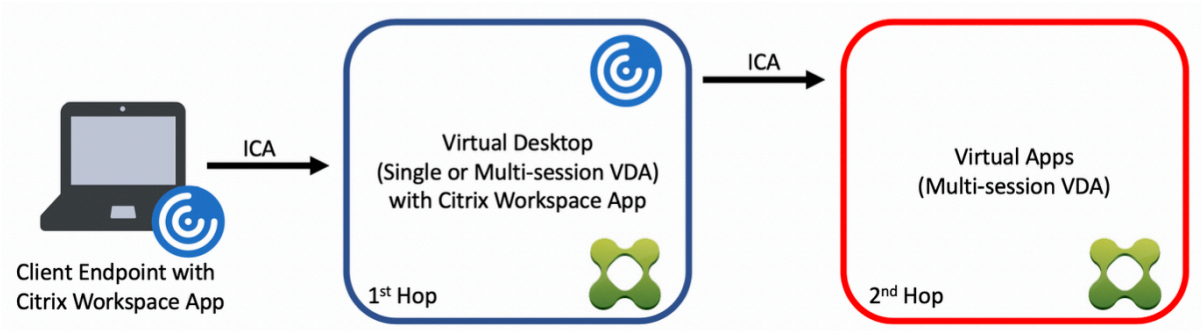
Veja também

- ICA Virtual Channel SDK
- Citrix Developer Network reúne todos os recursos técnicos e discussões envolvendo o uso de SDKs da Citrix. Nessa rede de recursos, você tem acesso a SDKs, exemplos de códigos e scripts, extensões e plug-ins, e documentação do SDK. Inclui também os fóruns do Citrix Developer Network, onde as discussões técnicas acontecem em torno de cada um dos SDKs da Citrix.

Salto duplo no Citrix Virtual Apps and Desktops

June 28, 2023

No contexto de uma sessão de cliente Citrix, o termo "salto duplo"refere-se a uma sessão do Citrix Virtual Apps que está sendo executada em uma sessão do Citrix Virtual Desktops. O diagrama a seguir ilustra um salto duplo.



Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktops em execução em um SO VDA de sessão única (conhecido como VDI) ou em um SO VDA multissessão (conhecido como área de trabalho publicada), esse é considerado o primeiro salto. Depois que o usuário se conecta à área de trabalho virtual, o usuário pode iniciar uma sessão do Citrix Virtual Apps. Esse é considerado o segundo salto.

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

Requisitos do sistema

Todas as edições Citrix Virtual Apps and Desktops, incluindo o serviço Citrix Cloud, suportam salto duplo.

O primeiro salto deve usar uma versão compatível do SO VDA de sessão única ou multissessão e do aplicativo Citrix Workspace. O segundo salto deve usar uma versão suportada do SO VDA multissessão. Consulte a página Product Matrix para ver as versões compatíveis.

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

Em ambientes em que o primeiro salto envolve uma solução de área de trabalho virtual de terceiros (não Citrix) em combinação com uma sessão do Citrix Virtual Apps, o suporte é limitado ao ambiente do Citrix Virtual Apps. No caso de problemas relacionados à área de trabalho virtual de ter-

ceiros, incluindo compatibilidade de aplicativos Citrix Workspace, redirecionamento de dispositivos de hardware e desempenho da sessão, a Citrix pode fornecer suporte técnico com capacidade limitada. Talvez seja necessário o Citrix Virtual Desktops no primeiro salto como parte da solução de problemas.

Considerações de implantação para HDX no salto duplo

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

Gráficos

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

Latência

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

Multimídia

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

Redirecionamento de dispositivo USB

O HDX inclui modos de redirecionamento genéricos e otimizados para suportar uma ampla gama de tipos de dispositivos USB. Preste especial atenção ao modo em uso em cada salto e use a tabela a

seguir como referência para melhores resultados. Para obter mais informações sobre modos de redirecionamento genéricos e otimizados, consulte Dispositivos USB genéricos.

Primeiro salto (VDI ou área de trabalho publicada)	Segundo salto (Virtual Apps)	Notas de suporte de compatibilidade
Otimizado	Otimizado	Recomendado (com base na compatibilidade dos dispositivos). Por exemplo, armazenamento em massa USB, scanners TWAIN, Webcam, áudio.
Genérico	Genérico	Para dispositivos onde a opção otimizada não está disponível.
Genérico	Otimizado	Embora tecnicamente possível, recomenda-se usar o modo otimizado em ambos os saltos quando o suporte de compatibilidade ao dispositivo estiver disponível.
Otimizado	Genérico	Sem suporte

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

Exceções de suporte

As sessões de salto duplo suportam a maioria das funcionalidades e recursos do HDX, exceto:

- Redirecionamento de conteúdo do navegador
- Acesso a aplicativo local
- RealTime Optimization Pack para Skype for Business
- Otimização para Microsoft Teams

Instalar e configurar

September 13, 2023

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

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

Preparar

Veja Prepare-se para instalar e conclua todas as tarefas necessárias.

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

Instalar componentes principais

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

Criar um site

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

Instalar um ou mais Virtual Delivery Agents (VDAs)

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

Para máquinas com um sistema operacional Linux, siga as orientações no Linux Virtual Delivery Agent.

Para uma implantação do Remote PC Access, instale um VDA para SO de sessão única em cada PC do escritório. Se você precisar apenas dos principais serviços VDA, use o instalador

`VDAWorkstationCoreSetup.exe` autônomo e os seus métodos existentes de Distribuição Eletrônica de Software (ESD). (Preparar a instalação descreve os instaladores de VDA disponíveis.)

Instalar componentes opcionais

Se você planeja usar o Citrix Universal Print Server, instale seu componente de servidor nos servidores de impressão. Consulte 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 que os usuários tenham maior controle sobre suas contas de usuário, instale Self-Service Password Reset.

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

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

Criar um catálogo de máquinas

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

Um catálogo pode conter máquinas físicas ou virtuais (VMs). Máquinas virtuais podem ser criadas a partir de uma imagem mestre. Quando usa um hipervisor ou outro serviço para fornecer VMs, você primeiro cria uma imagem mestre no host. Depois, quando cria o catálogo, você especifica a imagem, que é usada ao criar VMs.

Criar um grupo de entrega

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

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

Criar um grupo de aplicativos (opcional)

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

Preparar a instalação

June 28, 2023

A implantação do Citrix Virtual Apps and Desktops começa com a instalação dos seguintes componentes. Esse processo se prepara para a entrega de aplicativos e áreas de trabalho aos usuários dentro do seu firewall.

- Um ou mais Delivery Controllers
- Citrix Director
- Citrix StoreFront
- Citrix License Server
- Um ou mais Citrix Virtual Delivery Agents (VDAs)
- Componentes e tecnologias opcionais, como o Servidor de impressão universal, o Serviço de autenticação federada e o Autoatendimento de redefinição de senha

Para usuários fora do firewall, instale e configure um componente extra, como o Citrix Gateway. Para obter uma introdução, consulte Integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway.

Se sua implantação incluir cargas de trabalho do Windows Server, Configurar um Microsoft RDS License Server.

Você pode usar o instalador do produto completo no ISO do produto para implantar muitos componentes e tecnologias. Você pode usar um instalador autônomo de VDA para instalar VDAs. Os instaladores autônomos de VDA 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 exemplos de scripts que instalam, atualizam ou removem VDAs para máquinas no Active Directory. Você também pode usar os scripts para gerenciar imagens usadas por Machine Creation Services (MCS) e Citrix Provisioning (anteriormente Provisioning Services). Para obter detalhes, consulte Instalar VDAs usando scripts.

Informações para revisar antes da instalação

- Visão técnica geral: se você não estiver familiarizado com o produto e seus componentes.

- Segurança: quando planejar seu ambiente de implantação.
- Problemas conhecidos: problemas que você pode encontrar nesta versão.
- Bancos de dados: obter informações 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 o banco de dados do site. Você configura a maioria das informações do banco de dados ao criar um site, depois de instalar os componentes principais.
- Remote PC Access: 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 áreas de trabalho. Você pode configurar a primeira conexão ao criar um site (depois de 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 áreas de trabalho, ou se estiver usando o recurso Wake on LAN com Remote PC Access.
- **Conexões de host de nuvem pública:** se você tiver a licença Hybrid Rights, poderá criar conexões de host com a nuvem pública. Para obter informações relacionadas à licença Hybrid Rights, consulte Hybrid Rights Renewals. Para obter informações relacionadas ao direito à nuvem pública e o motivo dessa alteração, consulte CTX270373.

Onde instalar componentes

Revise os Requisitos de sistema para as plataformas, sistemas operacionais e versões compatíveis. Os pré-requisitos dos componentes são instalados automaticamente, exceto conforme indicado. Consulte a documentação do Citrix StoreFront e do Citrix License Server para obter 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 servidor pode funcionar para avaliação, teste ou pequenas implantações de produção.
- Para acomodar a expansão futura, considere a instalação de componentes em diferentes servidores. 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 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 suportado em um Server CoreOS (como um Delivery Controller), você deve usar a linha de comando. Esse tipo de SO não oferece uma interface gráfica, portanto, instale o Studio e outras ferramentas em outro lugar e, em seguida, aponte-as para o servidor do Controller.

Você pode instalar um Delivery Controller e um VDA de SO multissessão 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 o SO multissessão.

Certifique-se de que todos os sistemas operacionais tenham as atualizações mais recentes.

Certifique-se de que todas as máquinas tenham o relógio do sistema sincronizado. A infraestrutura Kerberos que protege a comunicação entre as máquinas requer sincronização.

Com Citrix Hypervisors, o estado de energia da máquina virtual pode aparecer como desconhecido, mesmo que pareça ter sido registrado. Para resolver esse problema, edite o valor `HostTime` da chave do registro para desativar a sincronização de horário 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 esse valor para algo diferente de UTC, por exemplo, `Local`. Essa alteração desativa efetivamente a sincronização de horário com o host.

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

Onde NÃO instalar componentes:

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

Se você tentar instalar ou atualizar um VDA em um sistema operacional Windows ao qual esta versão de produto não oferece suporte, uma mensagem indicará um artigo que descreve as opções.

Requisitos de permissão e do Active Directory

Você deve ser um usuário de domínio e um administrador local nas máquinas em que está instalando componentes.

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

Configure o 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 o Active Directory Domain Services.
- Não instale nenhum componente do Citrix Virtual Apps and Desktops em um controlador de domínio.
- Não use barra (/) ao especificar nomes de Unidade Organizacional no Studio.

A conta de usuário do Windows usada para instalar o Citrix License Server é configurada automaticamente como administrador completo de administração delegada.

Para mais informações:

- Práticas de segurança recomendadas
- Administração delegada
- Documentação da Microsoft para configuração do Active Directory

Instruções de instalação, considerações e práticas recomendadas

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 há uma reinicialização pendente de uma instalação anterior do Windows na máquina, o instalador para com o código 9 de saída/retorno. Você é solicitado a reinicializar a máquina.

  Esta não é uma reinicialização forçada da Citrix. Ela se dá devido a outros componentes instalados anteriormente na máquina. Se isso ocorrer, reinicie a máquina e inicie o instalador Citrix novamente.

  Ao usar a interface de linha de comando, você pode impedir a verificação de reinicialização pendente, incluindo a opção `/no_pending_reboot_check` no comando.

- Normalmente, se um componente tiver pré-requisitos, o instalador os implanta se eles não estiverem presentes. Alguns pré-requisitos podem exigir a reinicialização da máquina.

- Quando criar objetos antes, durante e depois da 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 sucesso 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 automaticamente para o Citrix quando a instalação é concluída. Além disso, ao instalar componentes, você é automaticamente registrado no Programa de Aperfeiçoamento da Experiência do Usuário (CEIP) da Citrix, que carrega dados anônimos.

  Durante a instalação, você também pode optar por participar de outras tecnologias Citrix que coletam diagnósticos para manutenção e solução de problemas. Para obter informações sobre esses programas, consulte Citrix Insight Services.
- Os dados do Google Analytics são coletados (e posteriormente carregados) automaticamente quando você instala (ou atualiza) o Studio. Depois de instalar o Studio, você pode alterar essa configuração com a chave do registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. O valor **1** ativa a coleta e o carregamento, **0** desativa a coleta e o carregamento.
- Se a instalação de um VDA falhar, um analisador MSI analisa o log MSI com falha, exibindo o código de erro exato. O analisador sugere um artigo CTX, se for um problema conhecido. O analisador também coleta dados anonimizados sobre o código de erro da falha. Esses dados são incluídos com outros dados coletados pelo CEIP. Se você terminar o registro no CEIP, os dados do analisador MSI coletados não serão mais enviados para a Citrix.

Durante a instalação do VDA

- O aplicativo Citrix Workspace para Windows está disponível, mas não é instalado por padrão quando você instala 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. Como alternativa, você pode disponibilizar os aplicativos Citrix Workspace no servidor StoreFront. Consulte a documentação do StoreFront.
- O serviço de Spooler de Impressão da Microsoft deve estar ativado. Você não consegue instalar um VDA com êxito se esse serviço estiver desativado.
- A maioria das edições suportadas do Windows 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.
  - Windows Media Redirection
  - Redirecionamento de vídeo HTML5
  - Redirecionamento de Webcam HDX RealTime

Você pode aceitar a limitação ou encerrar a instalação do VDA e reiniciá-la mais tarde, depois de instalar o Media Foundation. Na interface gráfica, essa escolha é apresentada em uma mensagem. Na linha de comando, você pode usar a opção `/no_mediafoundation_ack` para aceitar a limitação.

- Quando você instala o VDA, um novo grupo de usuários local chamado **Direct Access Users** é criado automaticamente. Em um VDA para SO de sessão única, esse grupo se aplica somente às conexões RDP. Em um VDA para SO multissessão, esse grupo se aplica às conexões ICA e RDP.
- O VDA deve ter endereços válidos de Controller com os quais se comunicar. Caso contrário, as sessões não podem ser estabelecidas. Você pode especificar endereços do Controller ao instalar o VDA ou posteriormente. Lembre-se que isso deve ser feito. Para obter mais informações, consulte Registro VDA.

Ferramentas de suporte de VDA

Cada instalador de VDA inclui um MSI de suporte que contém ferramentas Citrix para verificar o desempenho do VDA, como sua integridade geral e a qualidade das conexões. Ativar ou desativar a instalação desse MSI na página de **componentes adicionais** da interface gráfica do instalador de VDA. A partir da linha de comando, você pode desativar a instalação com a opção `/exclude "Citrix Supportability Tools"`.

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

Ferramentas atualmente no suporte MSI:

- Citrix Health Assistant: para obter detalhes, consulte CTX207624.
- VDA Cleanup Utility: para obter detalhes, consulte CTX209255.

Se você não instalar as ferramentas quando instalar o VDA, o artigo CTX contém um link para o download do pacote atual.

Reinicializações após e durante a instalação do VDA

Uma reinicialização é necessária no final da instalação do VDA. Essa reinicialização ocorre automaticamente por padrão.

Quando você está atualizando um VDA para a versão 7.17 (ou uma versão mais recente suportada), ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

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

- Certifique-se de que uma versão suportada do .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas de SO multissessão Windows, instale e ative os serviços de função do RDS antes de instalar o VDA.

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

- Se você estiver usando a interface gráfica ou a interface da linha de comando sem a opção `/noreboot`, a máquina reinicializa automaticamente após a instalação do pré-requisito.
- Se você estiver usando a interface da linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Quando você está atualizando um VDA para a versão 7.17 ou uma versão posterior suportada, ocorre uma reinicialização durante a atualização. Isso não pode ser evitado.

Restaurar em caso de falha de instalação ou atualização

> **Nota:**
>
> Esse recurso está disponível para VDAs de sessão única e multissessão

Se uma instalação ou atualização do VDA de sessão única falhar e o recurso "restaurar em caso de falha"estiver ativado, a máquina será retornada a um ponto de restauração definido antes do início da instalação ou atualização.

Se uma instalação ou atualização do VDA multissessão falhar e o recurso "restaurar em caso de falha" estiver ativado, a máquina será retornada a um backup executado antes do início da instalação ou atualização.

Quando uma instalação ou atualização do VDA de sessão única começa com esse recurso ativado, o instalador cria um ponto de restauração do sistema antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina será retornada ao estado do ponto de restauração. A pasta `%temp%/Citrix` contém registros de implantação e outras informações sobre a restauração.

Quando uma instalação ou atualização do VDA multissessão começa com esse 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 será retornada ao estado do backup. A pasta `%temp%/Citrix` contém registros de implantação e outras informações sobre a restauração. O tempo necessário 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\nomedoservidor*.

Por padrão, este recurso está desativado.

Se você planeja habilitar esse recurso, verifique se a restauração do sistema não está desativada por meio de uma configuração de GPO (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

> **Nota:**
>
> Essa configuração do objeto de política de grupo (GPO) não se aplica à restauração de um VDA multissessão.

Para habilitar esse recurso ao instalar ou atualizar um VDA multissessão:

- Ao usar a interface gráfica de um instalador VDA (como usar o **Autostart** ou o comando `XenDesktopVDASetup.exe` sem opções de restauração ou silencioso), marque a caixa de seleção **Enable automatic restore if update fails** na página **Summary**.

  Se a instalação/atualização for concluída com êxito, o ponto de restauração/backup não será usado, mas será mantido.

- 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 êxito, 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 mantido.

Instaladores

Instalador de produto completo

Usando o instalador de produto completo fornecido no ISO, você pode:

- Instalar, atualizar ou remover componentes principais: Delivery Controller, Studio, Director e License Server.
- Instalar ou atualizar o StoreFront.
- Instalar ou atualizar Windows VDAs para sistemas operacionais de sessão única ou multissessão.
- Instalar o componente `UpsServer` do Servidor de Impressão Universal em seus servidores de impressão.

- Instale o Federated Authentication Service.
- Instale o Session Recording.
- Instale o Workspace Environment Management.

> **Nota:**
>
> O instalador do Workspace Environment Management Agent não está traduzido. Ele está disponível somente em inglês.

Para fornecer uma área de trabalho a partir de um SO multissessão para um usuário (por exemplo, para desenvolvimento da web), use a interface de linha de comando do instalador do produto completo. Para obter detalhes, consulte Server VDI.

Instaladores autônomos de VDA

Instaladores autônomos de VDA estão disponíveis nas páginas de download da Citrix. (Eles não estão disponíveis na mídia de instalação do produto.) Os instaladores autônomos de VDA são muito menores do que o ISO do produto completo. Eles acomodam mais facilmente implantações que:

- Usam pacotes ESD (Electronic Software Distribution) que são preparados ou copiados localmente
- Possuem máquinas físicas
- Possuem escritórios remotos

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

Três instaladores autônomos de VDA estão disponíveis para download.

VDAServerSetup.exe:

Instala um VDA para SO multissessão. Aceita todas as opções de VDA multissessão que estão disponíveis com o instalador do produto completo.

VDAWorkstationSetup.exe:

Instala um VDA para SO de sessão única. Aceita todas as opções de VDA de sessão única que estão disponíveis com o instalador do produto completo.

VDAWorkstationCoreSetup.exe:

Instala um VDA para SO de sessão única que é otimizado para implantações do Remote PC Access ou instalações básicas de VDI. O Remote PC Access usa máquinas físicas. As instalações básicas de VDI são

VMs que não estão sendo usadas como uma imagem. Instala apenas os serviços básicos necessários para conexões de VDA a tais implantações. Portanto, suporta apenas um subconjunto das opções que são válidas com instaladores do produto completo ou `VDAWorkstationSetup.exe`.

Este instalador não instala nem contém os componentes usados para:

- App-V.
- Profile Management. Excluir o Citrix Profile Management da instalação afeta as exibições do Citrix Director. Para obter detalhes, consulte Instalar VDAs.
- Machine Identity Service.
- Citrix Supportability Tools.
- Citrix Files for Windows.
- Citrix Files for Outlook.

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

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

- Na interface gráfica: selecionar a opção Remote PC Access na página **Environment**.
- Na interface da 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 que você instale todos os componentes ausentes.

O instalador `VDAWorkstationCoreSetup.exe` instala automaticamente o MSI de redirecionamento de conteúdo do navegador. Essa instalação automática se aplica à versão de VDA 2003 e versões suportadas posteriores.

Códigos de retorno da instalação Citrix

O log de instalação contém o resultado de instalações de componentes como um código de retorno Citrix, não um valor da Microsoft.

- 0 = Success
- 1 = Failed
- 2 = PartialSuccess
- 3 = PartialSuccessAndRebootNeeded
- 4 = FailureAndRebootNeeded
- 5 = UserCanceled
- 6 = MissingCommandLineArgument

- 7 = NewerVersionFound

Por exemplo, ao usar ferramentas como o Microsoft System Center Configuration Manager, uma instalação de VDA com script pode parecer falhar quando o log de instalação contém o código de retorno 3. Isso pode ocorrer quando o instalador de VDA está aguardando uma reinicialização que você deve iniciar (por exemplo, após a instalação de um pré-requisito da função RDS em um servidor). Uma instalação de VDA é considerada bem-sucedida somente após todos os pré-requisitos e componentes selecionados serem instalados, e a máquina ser reinicializada após a instalação.

Como alternativa, você pode preparar sua instalação em scripts CMD (que retornam os códigos de saída da Microsoft) ou alterar os códigos de sucesso no seu pacote do Configuration Manager.

Configurar um servidor de licenças Microsoft RDS para cargas de trabalho do Windows Server

Este produto acessa os recursos de sessão remota do Windows Server ao fornecer uma carga de trabalho do Windows Server, como o Windows 2016. Normalmente, isso requer uma licença de acesso ao cliente dos Serviços de Área de Trabalho Remota (RDS CAL). O VDA deve poder entrar em contato com um servidor de licença RDS para solicitar RDS CALs. Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento Microsoft Activate the Remote Desktop Services license server Para ambientes de prova de conceito, você pode usar o período de tolerância fornecido pela Microsoft.

Com este método, você pode fazer com que esse serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações da Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft License your RDS deployment with client access licenses (CALs).

Para configurar o servidor de licenças RDS usando as configurações da política de grupo:

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 poder acessar esse servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Specify the Remote Desktop Licensing Mode for an RD Session Host Server.

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

Ambientes de nuvem do Microsoft Azure Resource Manager

January 3, 2024

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/
- Consent framework: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Service principal: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Provisionamento sob demanda do Azure

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

Quando você usa o MCS para criar catálogos de máquina no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz os custos de armazenamento
- Oferece criação de catálogos mais rápida

Quando você cria um catálogo MCS, o portal do Azure exibe 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 inicialização para ela. Existem dois tipos de máquinas com as seguintes diferenças:

- No caso de uma máquina em pool, o disco do sistema operacional e o cache de write-back existem somente quando a VM existe. Quando você desliga uma máquina em pool no console, a VM não fica visível no portal do Azure. Há uma economia significativa nos custos de armazenamento se você desligar as máquinas rotineiramente (por exemplo, fora do horário de trabalho).
- Para uma máquina dedicada, o disco do sistema operacional é criado na primeira vez que a VM é ligada. A VM no portal do Azure permanece armazenada até que a identidade da máquina seja excluída. Quando você encerra uma máquina dedicada no console, a VM ainda fica visível no portal do Azure.

Conexão com o Azure Resource Manager

O artigo Conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos das conexões do Azure Resource Manager.

Considerações:

- A Citrix recomenda usar o Service Principal com a função de colaborador. No entanto, consulte a seção Minimum permissions para obter a lista de permissões mínimas.
- Ao criar a primeira conexão, o Azure solicita que você conceda as permissões necessárias. Em conexões futuras, ainda será necessário que você se autentique, mas o Azure se lembra do seu consentimento anterior e não exibe o prompt novamente.
- As contas usadas para autenticação devem ser coadministradores da assinatura.
- A conta usada para autenticação deve ser um membro do diretório da assinatura. É preciso distinguir dois tipos de conta: 'Trabalho ou escola' e 'conta pessoal da Microsoft'. Veja CTX219211 para obter mais detalhes
- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, pode haver complicações se o usuário tiver recebido anteriormente acesso de convidado a um dos recursos do diretório. Nesse caso, eles podem ter uma entrada de espaço reservado no diretório que não lhes concede as permissões necessárias e é retornado um erro.

  Retifique isso removendo os recursos do diretório e adicione-os de volta explicitamente. No entanto, use essa opção com cuidado, pois ela tem efeitos não intencionais em outros recursos que a conta pode acessar.
- Há um problema conhecido em que determinadas contas são detectadas como convidados do diretório quando na verdade são membros. Configurações como essa geralmente ocorrem com contas de diretório estabelecidas mais antigas. Solução alternativa: adicione uma conta ao diretório, que recebe o valor de associação adequado.
- Os grupos de recursos são simplesmente contêineres de recursos e podem conter recursos de regiões diferentes da sua própria região. Isso pode ser confuso se você espera que os recursos exibidos na região de um grupo de recursos estejam disponíveis.
- Sua rede e sub-rede devem ser grandes o suficiente para hospedar o número de máquinas necessárias. Isso requer alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientações sobre a capacidade do espaço de endereço.

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.

Crie uma entidade de serviço

> **Importante:**
>
> Esse recurso ainda não está disponível para assinaturas do Azure China e do Azure Germany.

Antes de começar, autentique-se no Azure. Pré-requisitos:

- Você tem uma conta de usuário no locatário do Azure Active Directory da sua assinatura.
- A conta de usuário do Azure AD também é coadministradora da assinatura do Azure que você deseja usar para provisionar recursos.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativos para autenticação. Essas permissões podem ser revogadas após a criação da conexão com o host. Para obter mais informações sobre funções, consulte Funções internas do Azure AD.

Quando você se autentica 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. Lembre-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 **Add Connection and Resources** :

1. Na página **Connection**, selecione **Create a new connection**, o tipo de conexão **Microsoft Azure** e seu ambiente do Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Next**.
3. Na página **Connection Details**, insira seu ID de assinatura do Azure e um nome para a conexão. Depois de inserir o ID da assinatura, o botão **Create new** será ativado.

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

4. Selecione **Create new** e insira o nome de usuário e a senha da conta do Azure Active Directory.
5. Selecione **Sign in**.
6. Selecione **Accept** 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 **Accept**, você retorna à página **Connection** no assistente.

> **Nota:**
>
> Depois de autenticar com êxito no Azure, os botões **Create new** e **Use existing** desaparecem. O texto **Connection successful** aparece, com uma marca de seleção verde, indicando a conexão bem-sucedida com sua assinatura do Azure.

8. Na página **Connection Details**, selecione **Next**.

> **Nota:**
>
> Você não pode prosseguir para a próxima página até que você se autentique com êxito no Azure e faça a concessão das permissões necessárias.

9. Configure recursos para a conexão. Os recursos compreendem a região e a rede.
   - Na página **Region**, selecione uma região.
   - Na página **Network**, faça o seguinte:
     - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco 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 fornecerá combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.
10. Na página **Summary**, exiba um resumo das configurações e selecione **Finish** para concluir a configuração.

Use os detalhes de uma entidade de serviço criada anteriormente para se conectar ao Azure

Para criar uma entidade 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 do locatário do aplicativo que você registrou no Azure AD.
- **ApplicationName:** Nome do aplicativo a ser criado no Azure AD.

Para criar uma entidade de serviço:

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

   ```
   Connect-AzAccount
   ```


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

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

3. Crie o aplicativo em seu locatário do AD.

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

4. Crie uma entidade de serviço.

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

5. Atribua uma função à entidade de serviço.

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

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

No assistente **Add Connection and Resources**:

1. Na página **Connection**, selecione **Create a new connection**, o tipo de conexão **Microsoft Azure** e seu ambiente do Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Next**.
3. Na página **Connection Details**, insira seu ID de assinatura do Azure e um nome para a conexão.

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

4. Selecione **Use existing**. Na janela **Existing Service Principal Details**, insira as seguintes configurações para a entidade de serviço existente. Depois de inserir os detalhes, o botão **Save** é ativado. Selecione **Save**. Você não pode progredir além desta página até fornecer detalhes válidos.

   - **Subscription ID**. Insira seu ID de assinatura do Azure. Para obter sua ID de assinatura, entre no portal do Azure e navegue até **Subscriptions > Overview**.
   - **ID do Active Directory** (ID do locatário). Insira a ID do Diretório (locatário) do aplicativo que você registrou no Azure AD.
   - **Application ID**. Insira a ID do aplicativo (cliente) do aplicativo que você registrou no Azure AD.

- **Application secret**. 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. Lembre-se de salvar a chave porque você não poderá recuperá-la mais tarde.
- **Secret expiration date**. Insira a data após a qual o segredo do aplicativo expira. Você recebe um alerta no console antes que a chave secreta expire. No entanto, se a chave secreta expirar, você receberá erros.

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

- **Authentication URL**. Esse campo é preenchido automaticamente e não é editável.
- **Management URL**. Esse campo é preenchido automaticamente e não é editável.
- **Storage suffix**. Esse campo é preenchido automaticamente e não é editável.

  O acesso aos seguintes pontos de extremidade é necessário para criar um catálogo MCS no Azure. O acesso a esses pontos de extremidade otimiza a conectividade entre sua rede e o portal do Azure e seus serviços.

  - URL de autenticação: https://login.microsoftonline.com/
  - URL de gerenciamento: `https://management.azure.com/`. Essa é uma URL de solicitação das APIs do provedor do Azure Resource Manager. O ponto de extremidade para gerenciamento depende do ambiente. Por exemplo, para o Azure Global é https://management.azure.com/ e para o Azure US Government é https://management.usgovcloudapi.net/.
  - Sufixo de armazenamento: https://*.core.windows.net./. O (*) é um caractere curinga para o sufixo de armazenamento. Por exemplo, `https://demo.table.core.windows.net/`.

5. Depois de selecionar **Save**, você retornará à página **Connection Details**. Selecione **Next** para continuar na próxima página.
6. Configure recursos para a conexão. Os recursos compreendem a região e a rede.

   - Na página **Region**, selecione uma região.
   - Na página **Network**, faça o seguinte:
     - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco 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 fornecerá combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.

7. Na página **Summary**, exiba um resumo das configurações e selecione **Finish** para concluir a configuração.

Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager

Uma imagem pode ser um disco, um instantâneo ou a versão imagem de uma definição de imagem na Galeria de Computação do Azure que é usada para criar as VMs em um catálogo de máquinas. Antes de criar o catálogo de máquinas, crie uma imagem no Azure Resource Manager. Para obter informações gerais sobre imagens, consulte Criar catálogos de máquinas.

O uso de um perfil de máquina com início confiável como Security Type é obrigatório quando você seleciona uma imagem ou instantâneo com início confiável habilitado. Em seguida, você pode ativar ou desativar o SecureBoot e o vTPM especificando seus valores no Perfil de Máquina. Para obter informações sobre o início confiável do Azure, consulte Início confiável para máquinas virtuais do Azure.

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

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

Se essas propriedades personalizadas não forem definidas explicitamente, os valores da propriedade serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como o perfil da máquina. Além disso, se `ServiceOffering` não for especificado, ele será definido a partir do perfil da máquina.

> **Nota:**
>
> Se algumas das propriedades estiverem ausentes no perfil da máquina e não estiverem definidas nas propriedades personalizadas, os valores padrão das propriedades serão usados sempre que aplicável.

A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` tem todas as propriedades definidas ou os valores são derivados de MachineProfile.

Cenário New-ProvScheme

- MachineProfile tem todas as propriedades e CustomProperties não estão definidas. Exemplo:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
  machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance">
  3  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpA-value>"/>
  4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
        value>"/>
  5  <Property xsi:type="StringProperty" Name="LicenseType" Value="<
        mpA-value>"/>
  6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
        Value="<mpA-value>"/>
  7  <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
        Value="<mpA-value>"/>
  8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
        value>"/>
  9  </CustomProperties>
  10 <!--NeedCopy-->
  ```

- MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem somente LicenseType e OsType.

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
  machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance">
  3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
        value>"/>
  4  <Property xsi:type="StringProperty" Name="LicenseType" Value="<
        mpA-value>"/>
  5  </CustomProperties>
  6  <!--NeedCopy-->
  ```

- Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
  machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```


As propriedades personalizadas têm prioridade. Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
    CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value="<
    CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<
    CustomPropertiesA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Exemplo:

  - CustomProperties definem LicenseType e StorageAccountType
  - MachineProfile define LicenseType, OsType e Zones

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value="<
    CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não está definida. Exemplo:

  - CustomProperties definem StorageType
  - MachineProfile define LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
    machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\serviceoffering.
    folder<explicit-machine-size>.serviceoffering"
<!--NeedCopy-->
```

Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Se OsType não estiver em CustomProperties nem em MachineProfile, então:
  - O valor é lido a partir da imagem mestre.
  - Se a imagem mestre for um disco não gerenciado, OsType será definido como Windows.

  Exemplo:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
  machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
  "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.
  manageddisk"
  ```

  O valor da imagem mestre é gravado nas propriedades personalizadas, nesse caso, Linux.

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>
</CustomProperties>
<!--NeedCopy-->
```

Cenários Set-ProvScheme

- Um catálogo existente com:

  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define Zones

  Atualizações:

  - MachineProfile mpB.vm que define StorageAccountType
  - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define LicenseType e OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

  Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
      Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value="<
      CustomPropertiesB-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->
```

- Um catálogo existente com:

  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define StorageAccountType e LicenseType

  Atualizações:

  - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define StorageAccountType e OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

  Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
      Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
```



```
<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp
    -A-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Um catálogo existente com:
  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define Zones

  Atualizações:
  - Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  - `ServiceOffering` não está especificado

  ```
  Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\
  machineprofile.folder\azure.resourcegroup\mpB.vm"
  ```

  Os valores a seguir são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
    CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value="<
    mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma especificação de modelo ou uma VM como entrada para um perfil de máquina.

Esse método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta.

Restrições:

A criptografia de disco do Azure no host é:

- Incompatível com todos os tamanhos de máquinas do Azure
- Incompatível com a criptografia de disco do Azure

Para criar um catálogo de máquinas com capacidade de criptografia no host:

1. Verifique se a assinatura tem o recurso de criptografia no host ativado ou não. Para fazer isso, consulte https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Se não estiver ativado, você deve ativar o recurso para a assinatura. Para obter informações sobre como ativar o recurso para sua assinatura, consulte https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Verifique se um determinado tamanho de VM do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute uma destas opções:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Crie uma especificação de modelo ou uma VM como entrada para o perfil da máquina no portal do Azure com a criptografia no host ativada.

   - Se você quiser criar uma VM, selecione um tamanho de VM que suporte criptografia no host. Depois de criar a VM, a propriedade da VM **Encryption at host** é ativada.
   - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `securityProfile`.

4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina selecionando uma especificação de modelo ou VM.

   - Disco de SO/Disco de dados: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma
   - Disco de SO efêmero: é criptografado somente pela chave gerenciada pela plataforma
   - Disco de cache: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma

   Você pode criar o catálogo de máquinas usando a interface Full Configuration ou executando comandos do PowerShell.

   Se você quiser criar um catálogo de máquinas usando comandos do PowerShell, em que a chave de criptografia é uma chave gerenciada pelo cliente, faça o seguinte:

a) Abra uma janela do PowerShell.

b) Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.

c) Digite `cd xdhyp:/`.

d) Digite `cd .\HostingUnits\(your hosting unit)`.

e) Digite cd diskencryptionset.folder.

f) Digite dir para obter a lista de Conjuntos de Criptografia de Disco.

g) Copie o Id de um Conjunto de Criptografia de Disco.

h) Crie uma cadeia de caracteres de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www
    .w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"
    StorageAccountType`" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
    Value=`"False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
    Value=`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
     Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"
    DiskEncryptionSetId`" Value=`"/subscriptions/0xxx4xxx-xxb-4
    bxx-xxxx-xxxxxxxx/resourceGroups/abc/providers/Microsoft.
    Compute/diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

i) Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms
    ## -Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

j) Execute o comando New-ProvScheme. Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\
    def.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.
     folder\def.resourcegroup\def-vnet.virtualprivatecloud\
     subnet1.network" }

-ProvisioningSchemeName "name"
```



```
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\
   serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
   folder<def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

k) Conclua a criação do catálogo de máquinas.

Limitação do Azure

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

> **Dica:**
>
> Para obter mais informações, consulte Improving Azure performance with Machine Creation Services.

Para ajudar a mitigar esses problemas, você pode remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

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

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

Por padrão, o MCS oferece suporte a 500 operações simultâneas no máximo. Como alternativa, você pode usar o SDK remoto do PowerShell para definir o número máximo de operações simultâneas.

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

- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` por meio do comando do PowerShell `Set-item`.

Grupos de recursos do Azure

Os grupos de recursos de provisionamento do Azure fornecem uma maneira de provisionar as VMs que fornecem aplicativos e áreas de trabalho aos usuários. Você pode adicionar grupos de recursos do Azure vazios existentes ao criar um catálogo de máquinas do MCS ou criar novos grupos de recursos para você. Para obter informações sobre grupos de recursos do Azure, consulte a documentação da Microsoft.

Uso do grupo de recursos do Azure

Não há limite para o número de máquinas virtuais, discos gerenciados, instantâneos e imagens por Grupo de Recursos do Azure. (O limite de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure foi removido.)

- Ao usar uma entidade de serviço de escopo completo para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar uma entidade de serviço de escopo restrito para criar um catálogo de máquinas, você deve fornecer um Grupo de Recursos do Azure vazio e pré-criado para o catálogo.

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **Nota:**
>
> Se a propriedade personalizada `UseEphemeralOsDisk` estiver definida como **false** ou se não for especificado nenhum valor, todos os VDAs provisionados continuarão a usar um disco de SO provisionado.

Veja a seguir um exemplo de conjunto de propriedades personalizadas que devem ser usadas no esquema de provisionamento:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {
```



```
 9
10                  "Name": "StorageType",
11                  "Value": "Standard_LRS"
12               }
13   ,
14               {
15
16                  "Name": "UseSharedImageGallery",
17                  "Value": "true"
18               }
19   ,
20               {
21
22                  "Name": "SharedImageGalleryReplicaRatio",
23                  "Value": "40"
24               }
25   ,
26               {
27
28                  "Name": "SharedImageGalleryReplicaMaximum",
29                  "Value": "10"
30               }
31   ,
32               {
33
34                  "Name": "LicenseType",
35                  "Value": "Windows_Server"
36               }
37   ,
38               {
39
40                  "Name": "UseEphemeralOsDisk",
41                  "Value": "true"
42               }
43
44           ],
45   <!--NeedCopy-->
```

Como criar máquinas usando discos de SO efêmeros Os discos de SO efêmeros são controlados com base na propriedade `UseEphemeralOsDisk` do parâmetro `CustomProperties`.

Considerações importantes para discos efêmeros Para provisionar discos de sistema operacional efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve oferecer suporte a discos de SO efêmeros.
- O tamanho do cache ou disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco de SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também esses problemas nas seguintes situações:

- Criação do esquema de provisionamento.
- Modificação do esquema de provisionamento.
- Atualização da imagem.

Otimização de armazenamento de disco efêmero do Azure e do MCS (Machine Creation Services) (MCS I/O) O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Não é possível criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- Os parâmetros do PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) falham com uma mensagem de erro apropriada se você os definir como **true** em `New-ProvScheme` ou `Set-ProvScheme`.
- Para catálogos de máquinas existentes criados com os dois recursos ativados, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

Criptografia do servidor do Azure

O Citrix Virtual Apps and Desktops e o Citrix DaaS oferecem suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados de seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Server-side encryption of Azure Disk Storage.

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco está criptografado, altere a chave atual no `DiskEncryptionSet`. Todos os recursos associados a essa alteração de `DiskEncryptionSet` devem ser criptografados com a nova chave.
- Quando você desabilita ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja habilitada novamente ou você atribua uma nova chave. Qualquer catálogo usando a chave não pode ser ligado e você não pode adicionar VMs a ele.

Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente

Considere o seguinte ao usar esse recurso:

- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Depois de habilitar a chave de criptografia gerenciada pelo cliente, você não poderá desativá-la posteriormente. Se quiser desativar ou remover a chave de criptografia gerenciada pelo cliente, copie todos os dados para um disco gerenciado diferente que não esteja usando a chave de criptografia gerenciada pelo cliente.
- Os discos criados a partir de imagens personalizadas criptografadas usando criptografia no lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados usando as mesmas chaves gerenciadas pelo cliente. Esses discos devem estar na mesma assinatura.
- Os instantâneos criados a partir de discos criptografados com criptografia do lado do servidor e chaves gerenciadas pelo cliente devem ser criptografados com as mesmas chaves gerenciadas pelo cliente.
- Discos, instantâneos e imagens criptografados com chaves gerenciadas pelo cliente não podem ser movidos para outro grupo de recursos e assinatura.
- Os discos gerenciados criptografados atualmente ou anteriormente usando a Criptografia de Disco do Azure não podem ser criptografados usando chaves gerenciadas pelo cliente.
- Consulte o site da Microsoft para ver as limitações dos conjuntos de criptografia de disco por região.

> **Nota:**
>
> Consulte Quickstart: Create a Key Vault using the Azure portal para obter informações sobre como configurar a criptografia do lado do servidor do Azure.

Chave de criptografia gerenciada pelo cliente do Azure

Ao criar um catálogo de máquinas, você pode escolher se deseja criptografar dados nas máquinas provisionadas no catálogo. A criptografia no lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas no catálogo. Um Conjunto de Criptografia de Disco (DES) representa uma chave gerenciada pelo cliente. Para usar esse recurso, você deve primeiro criar seu DES no Azure. Um DES está no seguinte formato:

- /subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos. Se a imagem estiver criptografada com um DES, use o mesmo DES ao criar o catálogo da máquina. Você não pode alterar o DES depois de criar o catálogo.

Se você criar um catálogo com uma chave de criptografia e depois desabilitar o DES correspondente no Azure, não poderá mais ligar as máquinas no catálogo ou adicionar máquinas a ele.

Hosts dedicados do Azure

Você pode usar o MCS para provisionar VMs em hosts dedicados do Azure. Antes de provisionar VMs em hosts dedicados do Azure:

- Crie um grupo de hosts.
- Crie hosts nesse grupo de hosts.
- Verifique se há capacidade de host suficiente reservada para a criação de catálogos e máquinas virtuais.

Você pode criar um catálogo de máquinas com locação de host definida por meio do seguinte script do PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade de catálogo e não pode ser alterado depois que o catálogo é criado. Atualmente, a locação dedicada não é suportada no Azure.
- Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro HostGroupId.
- É necessário o posicionamento automático do Azure. Essa funcionalidade faz uma solicitação para integrar a assinatura associada ao grupo de hosts. Para obter mais informações, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview Se o posicionamento automático não estiver habilitado, o MCS emitirá um erro durante a criação do catálogo.

Galeria de Imagens Compartilhadas do Azure

Use a Galeria de Imagens Compartilhadas do Azure como um repositório de imagens publicadas para máquinas provisionadas do MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação dos discos de SO, melhorando os tempos de início e de inicialização do aplicativo para VMs não persistentes. A galeria de imagens compartilhadas contém os três elementos a seguir:

- *Galeria*: as imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de imagem na galeria*: esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- *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 só é compatível com discos gerenciados. Não está disponível para catálogos de máquinas legadas.

Para obter mais informações, consulte Azure shared image gallery overview.

Criar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure

Ao selecionar uma imagem a ser usada para criar um catálogo de máquina, você pode selecionar imagens criadas na Galeria de Computação do Azure.

Para que essas imagens apareçam, você deve:

1. Configurar um site do Citrix Virtual Apps and Desktops.
2. Conectar-se ao Azure Resource Manager.
3. No portal do Azure, criar um grupo de recursos. Para obter detalhes, consulte Criar uma Galeria de Imagens Compartilhadas do Azure usando o portal.
4. No grupo de recursos, crie uma Galeria de Computação do Azure.
5. Na Galeria de Computação do Azure, crie uma definição de imagem.
6. Na definição da imagem, crie uma versão da imagem.

Use os seguintes comandos do PowerShell para criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure:

1. Abra uma janela do PowerShell.

2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Selecione um grupo de recursos e liste todas as galerias do grupo de recursos.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
<!--NeedCopy-->
```

4. Selecione uma galeria e liste todas as definições de imagem da galeria.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
<!--NeedCopy-->
```

5. Selecione uma definição de imagem e liste todas as versões da definição de imagem.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
<!--NeedCopy-->
```

6. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Resource group
   - Gallery
   - Gallery image definition
   - Gallery image version

   Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurar a Galeria de Imagens Compartilhadas

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

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para dar suporte ao recurso Galeria de Imagens Compartilhadas:

`UseSharedImageGallery`

- Define se a Galeria de Imagens Compartilhadas deve ser usada para armazenar as imagens publicadas. Se definido como **True**, a imagem é armazenada como uma imagem da Galeria de Imagens Compartilhadas, caso contrário, a imagem é armazenada como um instantâneo.
- Os valores válidos são **true** e **false**.
- Se a propriedade não estiver definida, o valor padrão será **False**.

`SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas de versão de imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não estiver definida, os valores padrão serão usados. O valor padrão para discos de SO permanentes é 1000 e o valor padrão para discos de SO não persistentes é 40.

`SharedImageGalleryReplicaMaximum`

- Define o número máximo de réplicas para cada versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não estiver definida, o valor padrão será 10.
- Atualmente, o Azure oferece suporte a até 10 réplicas para uma versão única de imagem de galeria. Se a propriedade for definida com um valor maior do que o suportado pelo Azure, o MCS tentará usar o valor especificado. O Azure gera um erro, que registra o MCS deixa a contagem de réplicas atual inalterada.

> **Dica:**
>
> Ao usar a Galeria de Imagens Compartilhadas para armazenar uma imagem publicada para catálogos provisionados do MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na proporção de réplicas e no máximo de réplicas. A contagem de réplicas é calculada dividindo-se o número de máquinas no catálogo pela taxa de réplica (arredondando para o valor inteiro mais próximo) e, em seguida, limitando o valor à contagem máxima de réplicas. Por exemplo, com uma taxa de réplica de 20 e um máximo de 5, 0 a 20 máquinas têm uma réplica criada, 21 a 40 têm 2 réplicas, 41 a 60 têm 3 réplicas, 61 a 80 têm 4 réplicas, mais de 81 têm 5 réplicas.

Caso de uso: Atualizando a taxa de réplica da Galeria de Imagens Compartilhadas e o máximo de
O catálogo de máquinas existente usa a Galeria de Imagens Compartilhadas. Use o comando `Set-ProvScheme` para atualizar as propriedades personalizadas para todas as máquinas existentes no catálogo e quaisquer máquinas futuras:

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



```
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

Caso de uso: convertendo um catálogo de instantâneos em um catálogo da Galeria de Imagens Compartilhadas Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Dica:**
>
> Os parâmetros `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` não são necessários. Após a conclusão do comando `Set-ProvScheme`, a imagem da Galeria de Imagens Compartilhadas ainda não foi criada. Depois que o catálogo estiver configurado para usar a galeria, a próxima operação de atualização do catálogo armazenará a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. O ciclo de energia das máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Imagens Compartilhadas e todas as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente dentro de algumas horas.

Caso de uso: conversão de um catálogo da galeria de imagens compartilhadas em um catálogo de instantâneos Para esse caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

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

> **Dica:**
>
> Ao contrário da atualização de um instantâneo para um catálogo da Galeria de Imagens Compartilhadas, os dados personalizados de cada máquina ainda não foram atualizados para refletir as novas propriedades personalizadas. Execute o seguinte comando para ver as propriedades personalizadas originais da Galeria de Imagens Compartilhadas: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Depois que o comando `Set-ProvScheme` for concluído, o instantâneo da imagem ainda não foi criado. Depois que o catálogo estiver configurado para não usar a galeria, a próxima operação de atualização do catálogo armazenará a imagem publicada como um instantâneo. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o instantâneo e todas as máquinas recém-provisionadas são criadas a partir do instantâneo. O ciclo de energia das máquinas as atualiza, momento em que os dados personalizados da máquina são atualizados para refletir que `UseSharedImageGallery` está definido como **False**. Os ativos antigos da Galeria de Imagens Compartilhadas (galeria, imagem e versão) são limpos automaticamente em algumas horas.

Provisionar máquinas em zonas de disponibilidade especificadas

Você pode provisionar máquinas em zonas de disponibilidade específicas em ambientes do Azure. Você pode conseguir isso usando o PowerShell.

> **Nota:**
>
> Se nenhuma zona for especificada, o MCS permitirá que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribuirá aleatoriamente as máquinas entre elas.

Configuração de zonas de disponibilidade por meio do PowerShell

Com o PowerShell, você pode visualizar os itens de inventário oferecidos usando `Get-Item`. Por exemplo, para visualizar a oferta de serviços da *Eastern US region* `Standard_B1ls`:

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

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

```
$serviceOffering.AdditionalData
```

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

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

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

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

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

Disco efêmero do Azure

Os discos efêmeros do Azure permitem que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão.

> **Nota:**
>
> Os catálogos persistentes não oferecem suporte a discos de SO efêmeros.

Os discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Imagens Compartilhadas. Para obter mais informações, consulte Galeria de Imagens Compartilhadas do Azure.

Usando o PowerShell para configurar um disco efêmero

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

> **Nota:**
>
> Para usar esse recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

Por exemplo:

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

Armazenando um disco temporário do sistema operacional efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM ou em um disco de recursos. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não tenha um cache ou que tenha cache insuficiente. Essas VMs têm um disco temporário ou de recursos para armazenar um disco de SO efêmero, como `Ddv4`.

Considere o seguinte:

- Um disco efêmero é armazenado no disco de cache da VM ou no disco temporário (recurso) da VM. O disco de cache tem preferência em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco de SO.
- Para atualizações, uma nova imagem maior que o disco de cache, mas menor que o disco temporário, resulta na substituição do disco de SO efêmero pelo disco temporário da VM.

Preservação de uma máquina virtual provisionada durante o ciclo de energia

Escolha se deseja preservar uma máquina virtual provisionada durante o ciclo de energia. Use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. Esse parâmetro oferece suporte a uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provi-

sionada persiste quando a energia é desligada. Defina a propriedade `PersistVm` como **true** para manter uma máquina virtual quando desligada ou defina a propriedade como **false** para garantir que a máquina virtual não seja preservada quando desligada.

> **Nota:**
>
> A propriedade `PersistVm` só se aplica a um esquema de provisionamento com as propriedades `CleanOnBoot` e `UseWriteBackCache` habilitadas. Se a propriedade `PersistVm` não for especificada para máquinas virtuais não persistentes, elas serão excluídas do ambiente do Azure quando desligadas.

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` define a propriedade `PersistVm` como **true**:

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

No exemplo a seguir, o `New-ProvScheme CustomProperties` parâmetro preserva o cache de gravação `PersistVM` definindo como **true**:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
   Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
   false`" /><Property xsi:type=`"StringProperty`" Name=`"
   PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
   type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
   resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
   LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
```



```
6   -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
7   -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
       resourcegroup\demo-snapshot.snapshot"
8   -NetworkMapping @ {
9   "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
       region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
       .virtualprivatecloud\default.network" }
10
11 -ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
12  -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
       Standard_B2ms.serviceoffering" -UseWriteBackCache
13  -WriteBackCacheDiskSize 127
14  -WriteBackCacheMemorySize 256
15  <!--NeedCopy-->
```

> **Dica:**
>
> A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco de SO deve ser mantido. Para preservar uma máquina virtual provisionada, primeiro preserve o disco de SO. Não exclua o disco de SO sem primeiro excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem usar a especificação do parâmetro `PersistVm`.

Tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes do Azure que usam o MCS. Para VMs de destino, o MCS oferece suporte a:

- Disco de SO: SSD, SSD ou HDD premium
- Disco de cache de gravação: SSD, SSD ou HDD premium

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM oferece suporte ao tipo de armazenamento selecionado.
- Se sua configuração usar um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

> **Dica:**
>
> `StorageType` está configurado para um tipo de sistema operacional e uma conta de armazenamento. `WBCDiskStorageType` está configurado para o tipo de armazenamento em cache de write-back. Para um catálogo normal, é necessário `StorageType`. Se `WBCDiskStorageType` não estiver configurado, `StorageType` será usado como padrão para `WBCDiskStorageType`.

Se WBCDiskStorageType não estiver configurado, StorageType será usado como padrão para WBCDiskStorageType.

Configurando tipos de armazenamento

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

Veja a seguir um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>'
<!--NeedCopy-->
```

Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada

Você pode economizar nos custos de armazenamento mudando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade `StorageTypeAtShutdown` personalizada.

O tipo de armazenamento do disco muda para um nível inferior (conforme especificado na propriedade personalizada `StorageTypeAtShutdown`) quando você desliga a VM. Depois de ligar a VM, o tipo de armazenamento volta ao original (conforme especificado na propriedade `StorageType` personalizada ou na propriedade `WBCDiskStorageType` personalizada).

> **Importante:**
>
> O disco não existe até que a VM seja ligada pelo menos uma vez. Portanto, você não pode alterar o tipo de armazenamento ao ligar a VM pela primeira vez.

Requisitos

- Aplicável a um disco gerenciado. Isso implica que você defina a propriedade personalizada `UseManagedDisks` como true.
- Aplicável a um catálogo persistente e não persistente com um disco de sistema operacional permanente. Isso implica que você defina a propriedade personalizada `persistOsDisk` como true.

- Aplicável a um catálogo não persistente com um disco WBC persistente. Isso implica que você defina a propriedade personalizada `persistWBC` como true.

Restrição

- De acordo com a Microsoft, você só pode alterar o tipo de disco duas vezes por dia. Consulte o documento da Microsoft. De acordo com a Citrix, a atualização de `StorageType` acontece sempre que há uma ação de Iniciar ou Desalocar para a VM. Portanto, limite o número de ações de energia por VM a duas vezes por dia. Por exemplo, uma ação de energia pela manhã para iniciar a VM e outra à noite para desalocar a VM.

Alterar o tipo de armazenamento para um nível inferior Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

1. Adicione a propriedade personalizada `StorageTypeAtShutdown`, defina o valor como Standard_LRS (HDD) e crie um catálogo usando `New-ProvScheme`. Para obter informações sobre como criar um catálogo usando o PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Se `StorageTypeAtShutdown` tiver qualquer valor diferente de vazio ou Standard_LRS (HDD), a operação falhará.

   Exemplo de configuração de propriedades personalizadas ao criar um catálogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

   Exemplo de configuração de propriedades personalizadas ao criar um catálogo não persistente:


```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Quando você usa um perfil de máquina, a propriedade personalizada tem precedência sobre a propriedade definida em `MachineProfile`.

2. Desligue a VM e verifique o tipo de armazenamento da VM no portal do Azure. O tipo de armazenamento do disco muda para um nível inferior, conforme especificado na propriedade `StorageTypeAtShutdown` personalizada.
3. Ligue a VM. O tipo de armazenamento do disco volta para o tipo de armazenamento mencionado em:
   - Propriedade personalizada `StorageType` para disco do sistema operacional
   - Propriedade personalizada `WBCDiskStorageType` para o disco WBC somente se você especificar em `CustomProperties`. Caso contrário, ele volta para o tipo de armazenamento mencionado em `StorageType`.

Aplicar `StorageTypeAtShutdown` a um catálogo existente Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

Use `Set-ProvScheme` para adicionar uma VM a um catálogo existente. O recurso se aplica às novas VMs adicionadas após a execução de `Set-ProvScheme`. As máquinas existentes não são afe-

tadas.

Exemplo de configuração de propriedades personalizadas ao adicionar uma VM a um catálogo existente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

Alterar o tipo de armazenamento das VMs existentes para um nível inferior no desligamento
Antes de prosseguir com as etapas, consulte os Requisitos e a Restrição.

Você pode economizar custos de armazenamento alterando o tipo de armazenamento das VMs existentes para um nível inferior quando as VMs são desligadas. Para fazer isso, use a propriedade `StorageTypeAtShutdown` personalizada.

Para alterar o tipo de armazenamento das máquinas existentes em um catálogo para um nível inferior quando as VMs são desligadas:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Altere a cadeia de caracteres das propriedades personalizadas.


```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Atualize o esquema de provisionamento do catálogo existente. A atualização se aplica às novas VMs adicionadas após a execução de `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Atualize as VMs existentes para habilitar `StorageTypeAtShutdown`.

```
Request-ProvVMUpdate -ProvisioningSchemeName $CatalogName
<!--NeedCopy-->
```

7. Quando você ligar as máquinas na próxima vez, a propriedade `StorageTypeAtShutdown` das máquinas será atualizada. O tipo de armazenamento muda no próximo desligamento.

8. Execute o comando a seguir para visualizar o valor `StorageTypeAtShutdown` de cada VM em um catálogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $\_.VMName; $storageTypeAtShutdown = ($\_.CustomVmData
      | ConvertFrom-Json).StorageTypeAtShutdown.
    DiskStorageAccountType; return New-Object psobject -Property
    @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
    $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

Personalizar o comportamento de ativação em caso de falha na alteração do tipo de armazenamento Ao ligar, o tipo de armazenamento de um disco gerenciado pode apresentar falha ao mudar para o tipo desejado devido a uma falha no Azure. Nesses cenários, a VM permanece desligada e uma mensagem de falha é enviada a você. No entanto, você pode optar por ligar a VM, mesmo quando o armazenamento não pode ser restaurado para o tipo configurado, ou optar por manter a VM desligada.

- Se você configurar a propriedade personalizada `FailSafeStorageType` como **true** (configuração padrão) ou não a especificar nos comandos `New-ProvScheme` ou `Set-ProvScheme`:

  - Na ativação, a VM é ligada com o tipo de armazenamento incorreto.
  - Na desativação, a VM permanece desligada com o tipo de armazenamento incorreto.

- Se você configurar a propriedade personalizada `FailSafeStorageType` como **false** nos comandos `New-ProvScheme` ou `Set-ProvScheme`:

  - Na ativação, a VM permanece desligada com o tipo de armazenamento incorreto.
  - Na desativação, a VM permanece desligada com o tipo de armazenamento incorreto.

Para criar um catálogo de máquinas:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Crie um pool de identidades se ainda não tiver sido criado.
4. Adicione a propriedade personalizada em `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Crie o catálogo de máquinas. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Para atualizar um catálogo de máquinas existente que inclua a propriedade personalizada `FailSafeStorageType`. Essa atualização não afeta as VMs existentes.

1. Atualize a propriedade personalizada no comando `Set-ProvScheme`. Por exemplo:


```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
<!--NeedCopy-->
```

Para aplicar a alteração feita em Set-ProvScheme às VMs existentes, execute o comando `Request-ProvVMUpdate`.

1. Execute o comando Request-ProvVMUpdate. Por exemplo:

   ```
   Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
       List-Of-Vm-Names>
   <!--NeedCopy-->
   ```

2. Reinicie as VMs.

Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, isso não afeta as máquinas existentes. Usando o comando `Request-ProvVMUpdate` do PowerShell, você pode aplicar o esquema de provisionamento atual a uma máquina persistente ou não persistente existente ou a um conjunto de máquinas. Atualmente, no Azure, você pode atualizar `ServiceOffering`, `MachineProfile` e as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> Você só pode atualizar as propriedades personalizadas `StorageType`, `WBCDiskStorageType`

> e `IdentityDiskStorageType` de um catálogo usando o disco gerenciado em ambientes do Azure.
> Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento (nome do catálogo de máquinas)

Depois de fazer as seguintes alterações no esquema de provisionamento, a instância de VM é recriada para catálogos persistentes no Azure:

- Altere o `MachineProfile`
- Remova `LicenseType`
- Remova `DedicatedHostGroupId`

> **Nota:**
>
> O disco do sistema operacional das máquinas existentes, juntamente com todos os seus dados, permanece como está e uma nova VM é anexada ao disco.
> Para atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Atualize o esquema de provisionamento. Por exemplo,

   - Com a VM como entrada do perfil da máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
<!--NeedCopy-->
```

   - Com a especificação do modelo como entrada do perfil da máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    template-spec>.templatespec<template-spec-version>.
    templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```


- Com apenas a oferta do serviço:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Atualize as máquinas existentes.

- Para atualizar todas as máquinas existentes. Por exemplo,

```
Request-ProvVMUpdate  – ProvisioningSchemeName "my-catalog"
<!--NeedCopy-->
```

- Para atualizar uma lista de máquinas específicas. Por exemplo,

```
Request-ProvVMUpdate -ProvisioningSchemeName "my-catalog" -
    VMName "vm1","vm2"
<!--NeedCopy-->
```

- Para atualizar máquinas com base na saída de Get-ProvVM. Por exemplo,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Request-
    ProvVMUpdate
<!--NeedCopy-->
```

5. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Reinicialize as máquinas. Na próxima vez que forem ligadas, as alterações às propriedades serão aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```



```
<!--NeedCopy-->
```

Agendar atualizações de configuração

Você pode agendar um intervalo de tempo para as atualizações de configuração das máquinas existentes provisionadas pelo MCS usando o comando PowerShell `Schedule-ProvVMUpdate`. Qualquer ativação ou reinicialização durante o horário programado aplica uma atualização programada do esquema de provisionamento a uma máquina.

Se você executar o comando `Request-ProvVMUpdate` e `Schedule-ProvVMUpdate`, o comando mais recente entrará em vigor.

> **Nota:**
>
> `Schedule-ProvVMUpdate` tem todas as funcionalidades de `Request-ProvVMUpdate` e muito mais. Posteriormente, `Schedule-ProvVMUpdate` substituirá `Request-ProvVMUpdate`.

Você também pode cancelar a atualização da configuração antes do horário agendado usando `Cancel-ProvVMUpdate`.

Você pode agendar a atualização da configuração de:

- Uma única VM
- Várias VMs associadas a um ID de esquema de provisionamento ou a um nome de esquema de provisionamento
- Um catálogo inteiro associado a um ID de esquema de provisionamento ou a um nome de esquema de provisionamento

Para agendar a atualização da configuração:

1. Crie um catálogo usando a interface Full Configuration ou o PowerShell.
2. Abra uma janela do **PowerShell**.
3. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
4. Verifique a configuração das máquinas existentes. Por exemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

5. Atualize o esquema de provisionamento para atualizar uma propriedade personalizada, um perfil de máquina ou uma oferta de serviço. Por exemplo,


```
Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
    MachineProfile"XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

6. Verifique se:

   - a propriedade atual da VM corresponde ao esquema de provisionamento atual e
   - há alguma ação de atualização pendente na VM.

   Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

7. Execute `Schedule-ProvVMUpdate` para programar a atualização de uma VM para as configurações de provisionamento mais recentes na próxima vez que ela for iniciada na janela do horário agendado. Por exemplo,

   - Para agendar uma atualização com a hora de início como a hora atual

```
Schedule-ProvVMUpdate -ProvisioningSchemeName " my-catalog "
    -VMName "vm1" -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - Para agendar uma atualização em um fim de semana

```
Schedule-ProvVMUpdate -ProvisioningSchemeName " my-catalog "
    -VMName "vm1" -StartTimeInUTC "10/15/2022 9:00am" -
    DurationInMinutes (New –TimeSpan –Days 2).TotalMinutes
<!--NeedCopy-->
```

> **Nota:**
>
> - `VMName` é opcional. Se não for especificada, a atualização será agendada para todo o catálogo.
> - Em vez de `StartTimeInUTC`, use `StartsNow` para indicar que a hora de início do agendamento é a hora atual.
> - `DurationInMinutes` é opcional. O padrão é 120 minutos. Um número negativo (por exemplo, —1) indica que não há limite superior na janela de tempo do cronograma.

8. Verifique o status da atualização.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```


9. Ligue a VM. Se você ligar a máquina após o horário programado, a atualização da configuração não será aplicada. Se você ligar a máquina dentro do horário programado,

    - Se a máquina estiver desligada, e
        - você não ligar a máquina, a atualização de configuração não é aplicada
        - você ligar a máquina, a atualização de configuração é aplicada
    - Se a máquina estiver ligada, e
        - você não reiniciar a máquina, a atualização de configuração não é aplicada
        - você reiniciar a máquina, a atualização de configuração é aplicada

Você também pode cancelar uma atualização de configuração de uma única VM, várias VMs ou um catálogo inteiro. Para cancelar uma atualização de configuração:

1. Execute `Cancel-ProvVMUpdate`. Por exemplo,

    - Para cancelar a atualização de configuração agendada de uma única VM:

    ```
    1  Cancel-ProvVMUpdate -ProvisioningSchemeName " my-catalog " -
          VMName "vm1"
    2  <!--NeedCopy-->
    ```

    - Para cancelar a atualização de configuração agendada para várias VMs.

    ```
    1  Cancel-ProvVMUpdate -ProvisioningSchemeName "my-catalog" -
          VMName "vm1","vm2"
    2  <!--NeedCopy-->
    ```

    > **Nota:**
    >
    > As VMs devem ser do mesmo catálogo.

Recuperar informações para VMs do Azure, instantâneos, disco de SO e definição de imagem da galeria

Você pode exibir informações para uma VM do Azure, incluindo disco de SO e tipo, instantâneo e definição de imagem da galeria. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Use essa funcionalidade para exibir e selecionar uma imagem do Linux ou do Windows. Uma propriedade do PowerShell, `TemplateIsWindowsTemplate`, foi adicionada ao parâmetro `AdditionDatafield`. Esse campo contém informações específicas do Azure: tipo de VM, disco de SO, informações da imagem da galeria e informações do tipo do sistema operacional. Se `TemplateIsWindowsTemplate` for definido como **True**, isso indica que o tipo de sistema operacional é Windows; se `TemplateIsWindowsTemplat` for definido como **False**, isso indica que o tipo de sistema operacional é Linux.

> **Dica:**
>
> As informações exibidas pela propriedade do `TemplateIsWindowsTemplate` PowerShell são derivadas da API do Azure. Em alguns casos, esse campo pode estar vazio. Por exemplo, um instantâneo de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de sistema operacional não pode ser recuperado de um instantâneo.

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

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

Catálogos de máquinas com início confiável

Para criar com êxito um catálogo de máquinas com início confiável, use:

- Um perfil de máquina com início confiável
- Um tamanho de VM que ofereça suporte ao início confiável
- Uma versão de Windows VM que ofereça suporte ao início confiável Atualmente, o Windows 10, 2016, 2019 e 2022 oferecem suporte ao início confiável.

> **Importante:**
>
> O início confiável requer a criação de novas VMs. Você não pode ativar o início confiável em VMs existentes que foram inicialmente criadas sem ele.

Para exibir os itens de inventário da oferta do Citrix DaaS e determinar se o tamanho da VM suporta o início confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
3. Execute o seguinte comando:


```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
    - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM é compatível com o início confiável.
    - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não é compatível com o início confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que suportam o início confiável:

```
(Get-AzComputeResourceSku | where {
 $\_.Locations.Contains($region) -and ($\_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Veja a seguir exemplos que descrevem se o tamanho da VM oferece ou não suporte ao início confiável após a execução do comando do Azure PowerShell.

- *Exemplo 1*: se a VM do Azure oferecer suporte somente à Geração 1, a VM não é compatível com o início confiável. Portanto, o recurso `TrustedLaunchDisabled` não é exibido depois que você executa o comando do Azure PowerShell.
- *Exemplo 2*: se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` for **True**, o tamanho da VM de Geração 2 não é compatível com o início confiável.
- *Exemplo 3*: se a VM do Azure oferecer suporte somente à Geração 2 e o recurso `TrustedLaunchDisabled` não for exibido após a execução do comando PowerShell, o tamanho da VM de Geração 2 não é compatível com o início confiável.

Para obter mais informações sobre o início confiável de máquinas virtuais do Azure, consulte o documento da Microsoft Início confiável para máquinas virtuais do Azure.

Erros ao criar catálogos de máquinas com o início confiável

Você verá os erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com início confiável:

Cenário	Erro
Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado	`MachineProfileNotSupportedForUnmanagedCata`
Se você selecionar um perfil de máquina compatível com início confiável ao criar um catálogo com disco não gerenciado como imagem mestre	`SecurityTypeNotSupportedForUnmanagedDisk`
Se você não selecionar um perfil de máquina ao criar um catálogo gerenciado com a origem de uma imagem mestre com início confiável como o tipo de segurança	`MachineProfileNotFoundForTrustedLaunchMaste`
Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre	`SecurityTypeConflictBetweenMasterImageAndMa`
Se você selecionar um tamanho de VM que não ofereça suporte ao início confiável, mas usar uma imagem mestre compatível com início confiável ao criar um catálogo	`MachineSizeNotSupportTrustedLaunch`

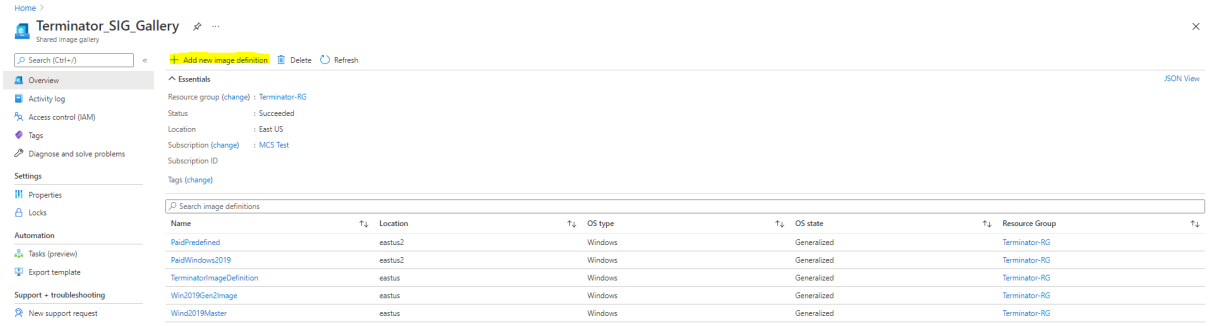
Azure Marketplace

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

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

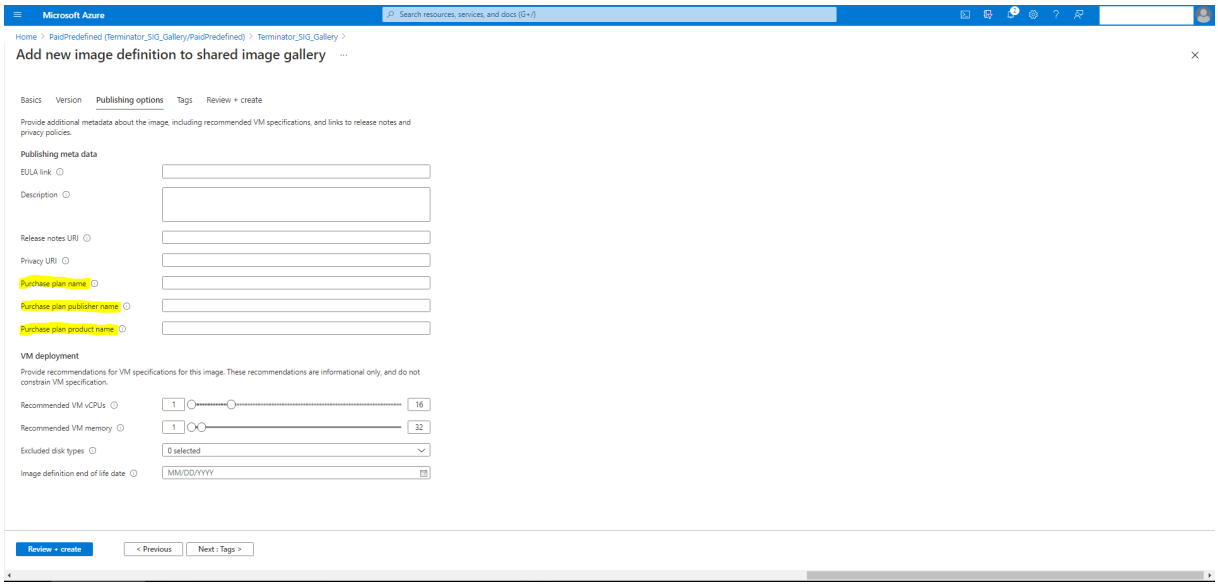
Verifique se a imagem criada na Galeria de Imagens Compartilhadas contém informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Opcionalmente, essas imagens podem ser usadas para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.

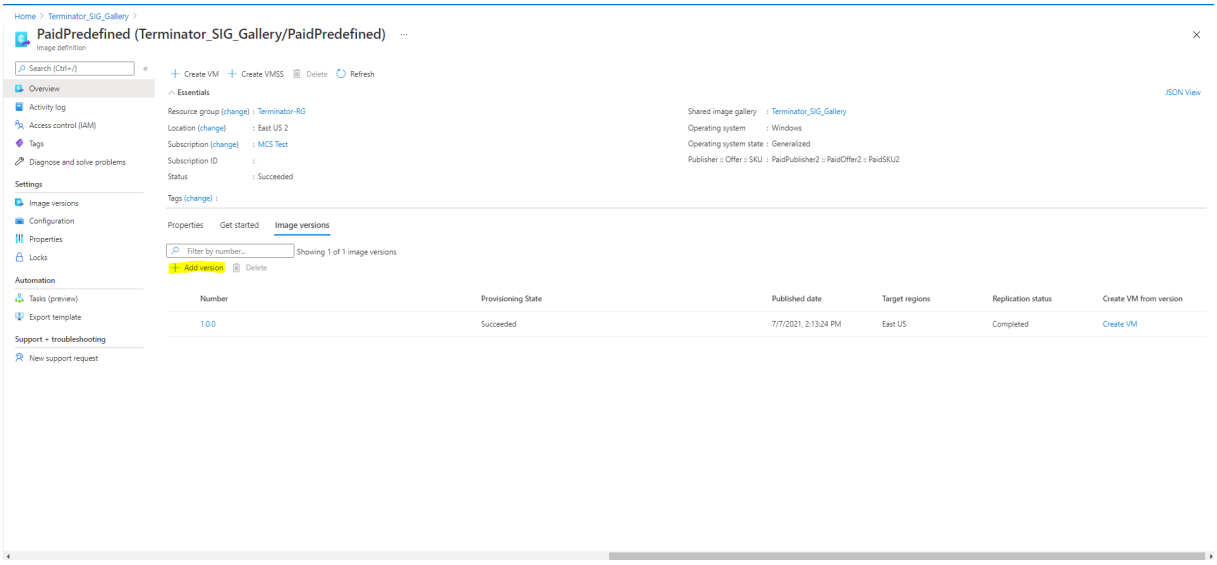


Na página **Publishing options**, verifique as informações do plano de compra.

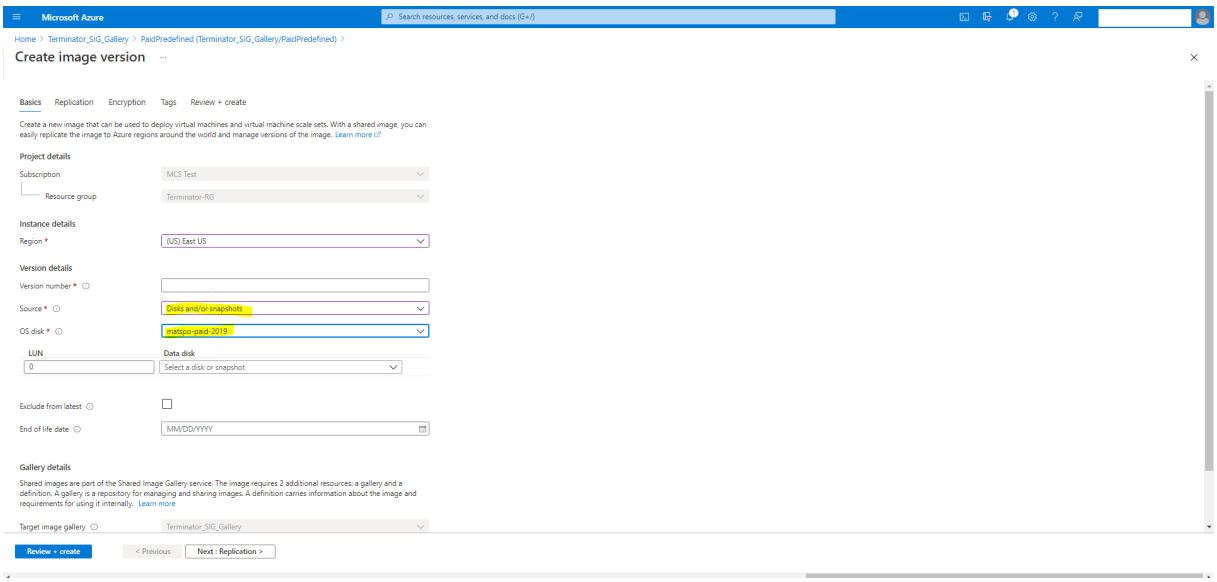
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. Se você deixar de preencher as informações do plano de compra, isso pode causar falha no processo do catálogo de máquinas.



Depois de verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Isso é usado como a imagem mestre. Clique em **Add version**:



Na seção **Version details**, selecione o instantâneo da imagem ou o disco gerenciado como 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 de permissões mínimas.

Criar 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",
<!--NeedCopy-->
```

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

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
<!--NeedCopy-->
```

Criar, atualizar ou excluir VMs Crie um catálogo de máquinas e, em seguida, adicione, exclua, atualize máquinas e exclua o catálogo de máquinas.

A seguir está a lista de permissões mínimas necessárias quando 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",
```



```
<!--NeedCopy-->
```

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

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

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

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

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Se a imagem mestre for um disco gerenciado. Instantâneos, ou VHD, está em uma região diferente da região da conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
<!--NeedCopy-->
```

- Se você usar o grupo de recursos gerenciados pela Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

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

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
<!--NeedCopy-->
```

- Se você usar o suporte a host dedicado do Azure:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```



```
<!--NeedCopy-->
```

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

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

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

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
<!--NeedCopy-->
```

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

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

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

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
<!--NeedCopy-->
```


Permissão geral

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

O conjunto de permissões a seguir fornece a melhor compatibilidade 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",
```



```
46 "Microsoft.Resources/subscriptions/resourceGroups/read",
47 "Microsoft.Resources/subscriptions/resourceGroups/write",
48 "Microsoft.Resources/subscriptions/resourceGroups/delete",
49 "Microsoft.Storage/storageAccounts/delete",
50 "Microsoft.Storage/storageAccounts/listKeys/action",
51 "Microsoft.Storage/storageAccounts/read",
52 "Microsoft.Storage/storageAccounts/write",
53 "Microsoft.Resources/templateSpecs/read",
54 "Microsoft.Resources/templateSpecs/versions/read",
55 <!--NeedCopy-->
```

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas
- CTX219211: Set up a Microsoft Azure Active Directory account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Ambientes de virtualização do Microsoft System Center Virtual Machine Manager

October 19, 2023

Siga estas instruções se você usa o Hyper-V com Microsoft System Center Virtual Machine Manager (VMM) para fornecer máquinas virtuais.

Esta versão oferece suporte às versões do VMM listadas em Requisitos do sistema.

> **Nota:**
>
> Clusters Hyper-V mistos (contendo servidores executando versões diferentes do Hyper-V) não são suportados.

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

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

Instalar e configurar um hipervisor

> **Importante:**
>
> Todos os Delivery Controllers devem estar na mesma floresta que os servidores VMM.

1. Instale o servidor Microsoft Hyper-V e o VMM em seus servidores.
2. Instale o console System Center Virtual Machine Manager em todos os Controllers. A versão do console deve corresponder à versão do servidor de gerenciamento. Embora um console anterior possa se conectar ao servidor de gerenciamento, o provisionamento de VDAs falhará se as versões forem diferentes.
3. Verifique as seguintes informações da conta:

   A conta que você usa para especificar hosts no Studio é um administrador do VMM ou administrador delegado do VMM para as máquinas Hyper-V relevantes. Se esta conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados no Studio durante o processo de criação do host.

   A conta de usuário usada para a integração do Studio também deve ser membro do grupo de segurança local de administradores em cada servidor Hyper-V. Essa configuração dá suporte ao gerenciamento do ciclo de vida da VM, como criação, atualização e exclusão de VM.

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

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

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

1. Em **Create User Roles Wizard**, selecione Fabric Administrator (Delegated Administrator) como a função do usuário.
2. Em **Members**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Scope**, selecione os grupos de hosts aos quais deseja que o administrador delegado tenha acesso.
4. Crie uma nova **Run As Account** usando credenciais de usuário administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

Criar uma VM mestre

1. Instale um VDA na VM mestre e selecione a opção para otimizar a área de trabalho para melhorar o desempenho.
2. Tire um instantâneo da VM mestre para usar como backup.

Criar áreas de trabalho virtuais

Se você estiver usando o MCS para criar VMs, ao criar um site ou uma conexão:

1. Selecione o tipo de host de virtualização da Microsoft.
2. Digite o endereço como o nome de domínio totalmente qualificado do servidor host.
3. Insira as credenciais da conta de administrador que você configurou anteriormente que tem permissões para criar VMs.
4. Em **Host Details**, selecione o cluster ou o host autônomo para usar ao criar VMs.

   Procure e selecione um cluster ou host autônomo mesmo se você estiver usando uma única implantação de host Hyper-V.

MCS em compartilhamentos de arquivo SMB 3

Para catálogos de máquinas criados com MCS em compartilhamentos de arquivo SMB 3 para armazenamento na VM, certifique-se de que as credenciais atendam aos seguintes requisitos. Esses requisitos asseguram que as chamadas a partir da Hypervisor Communications Library (HCL) do Controller estabeleçam a conexão com o armazenamento SMB:

- As credenciais de usuário do VMM devem incluir acesso completo de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante os eventos de ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Quando usar o armazenamento SMB, ative o Authentication Credential Security Support Provider (CredSSP) do Controller para as máquinas Hyper-V individualmente. Use esse processo para VMM 2012 SP1 com Hyper-V no Windows Server 2012. Para obter mais informações, consulte CTX137465.

O HCL usa `CredSSP` para abrir uma conexão com a máquina Hyper-V. Esse recurso passa as credenciais de usuário criptografadas pelo Kerberos para a máquina Hyper-V. Os comandos do **PowerShell** na sessão na máquina Hyper-V remota são executados com as credenciais fornecidas. Nesse caso, as credenciais do usuário do VMM, para que os comandos de comunicação de armazenamento funcionem corretamente.

As tarefas a seguir usam scripts do PowerShell que se originam no HCL e que são 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). Ele clona e deixa a VM mestre pronta para criar VMs a partir do novo disco criado (e remove a dependência da VM mestre original).

  ConvertVirtualHardDisk on the root\virtualization\v2 namespace

Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

- **Criar disco de diferença:** cria um disco de diferença a partir da imagem mestre gerada pela consolidação da imagem mestre. Depois, o disco de diferença é anexado a uma nova VM.

  CreateVirtualHardDisk on the root\virtualization\v2 namespace

  Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

- **Carregar discos de identidade:** o HCL não pode carregar o disco de identidade diretamente para o armazenamento SMB. Portanto, a máquina Hyper-V deve carregar e copiar o disco de identidade para o armazenamento. Como a máquina Hyper-V não pode ler o disco no Controller, o 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 de administrador.

  A máquina Hyper-V copia o disco para o armazenamento SMB por meio de um script do PowerShell em execução na sessão remota do PowerShell. Uma pasta é criada na máquina Hyper-V e as permissões nessa pasta são bloqueadas apenas para o usuário do VMM (por meio da conexão remota do PowerShell).

  O HCL exclui o arquivo do compartilhamento de 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:** tal como acontece com os carregamentos, os discos de identidade passam pela máquina Hyper-V para o HCL. O processo a seguir cria uma pasta que só tem permissões de usuário do VMM no servidor Hyper-V se ela não existir.

  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 de administrador da máquina Hyper-V na memória.

O HCL exclui o arquivo do compartilhamento de administrador.

Provisionamento do Azure Stack HCI por meio do SCVMM

Azure Stack HCI é uma solução de cluster de infraestrutura hiperconvergente (HCI) que hospeda cargas de trabalho virtualizadas do Windows e do Linux e o seu armazenamento em um ambiente híbrido local.

Os serviços híbridos do Azure aprimoram o cluster com recursos como monitoramento baseado em nuvem, recuperação de site e backups de VM. Você também pode ter uma visão centralizada de todas as suas implantações de do Azure Stack HCI no portal do Azure.

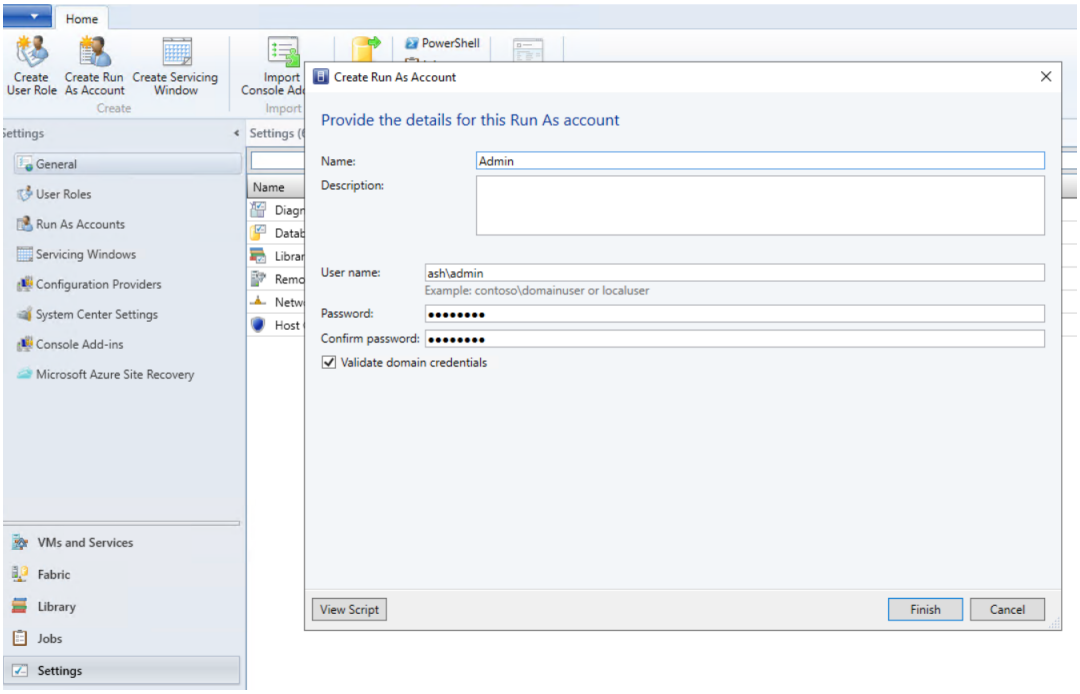
Integrar o Azure Stack HCI ao SCVMM

Para integrar o Azure Stack HCI ao SCVMM, você precisa primeiro criar um cluster do Azure Stack HCI e, em seguida, integrar esse cluster ao SCVMM.

1. Para criar o cluster do Azure Stack HCI, consulte o documento da Microsoft Conectar o Azure Stack HCI ao Azure.
2. Para integrar o cluster do Azure Stack HCI ao SCVMM, faça o seguinte:
   a) Faça login na máquina que está preparada para hospedar o servidor SCVMM e instale o SCVMM 2019 UR3 ou posterior.

      > **Nota:**
      >
      > Instale o console do administrador SCVMM 2019 UR3 ou posterior em todos os controladores.

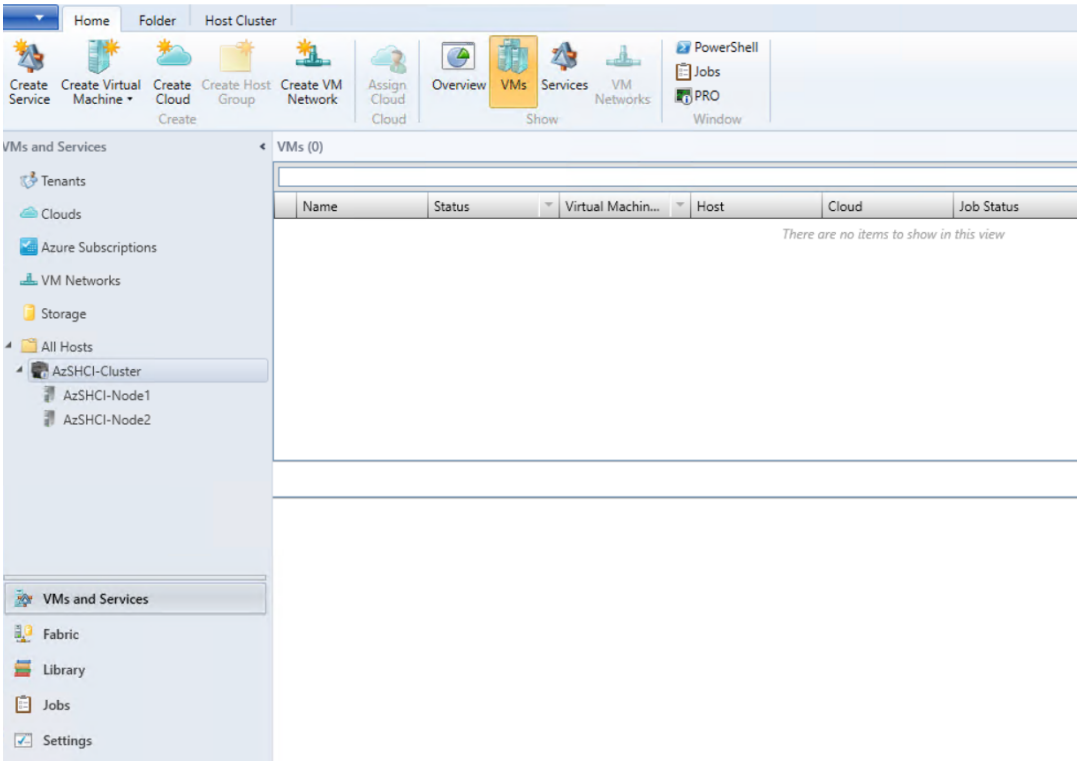
   b) Na página **Settings** do console do VMM, crie uma conta Executar como.



c) Execute os seguintes comandos do PowerShell com privilégios administrativos no servidor SCVMM para adicionar o cluster do Azure Stack HCI como um host:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

d) Agora você pode ver o cluster do Azure Stack HCI juntamente com os nós no console do VMM.



e) Crie a conexão de hospedagem do SCVMM na interface **Full Configuration**.

Ambientes de virtualização do Citrix Hypervisor

June 28, 2023

Criar uma conexão ao Citrix Hypervisor

Ao criar uma conexão com o Citrix Hypervisor (anteriormente XenServer), você deve fornecer as credenciais para um usuário VM Power Admin ou de nível superior.

A Citrix recomenda o uso de HTTPS para proteger as comunicações com o Citrix Hypervisor. Para usar HTTPS, você deve substituir o certificado SSL padrão instalado no Citrix Hypervisor; consulte CTX128656.

Você pode configurar a alta disponibilidade se ela estiver ativada no servidor Citrix Hypervisor. A Citrix recomenda que você selecione todos os servidores no pool (em Edit High Availability) para permitir a comunicação com o servidor Citrix Hypervisor se o mestre do pool falhar.

Você pode selecionar um tipo e um grupo de GPU, ou Passthrough, se o Citrix Hypervisor oferecer suporte a vGPU. A exibição indica se a seleção possui recursos de GPU dedicados.

Ao usar o armazenamento local em um ou mais hosts Citrix Hypervisor para armazenamento de dados temporário, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

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

- BIOS legado para VMs com SO de área de trabalho ou servidor compatíveis.
- UEFI para VMs com SO de área de trabalho ou servidor compatíveis, incluindo Inicialização Segura.

> **Nota:**
>
> Permissões de operador de pool ou superiores são necessárias ao configurar o MCS.

Usar o IntelliCache para conexões do Citrix Hypervisor

Usando o IntelliCache, as implantações de VDI hospedadas são mais econômicas porque você pode usar uma combinação de armazenamento compartilhado e armazenamento local. Isso melhora o desempenho e reduz o tráfego de rede. O armazenamento local armazena em cache a imagem mestre do armazenamento compartilhado, o que reduz o número de leituras no armazenamento compartilhado. Para áreas de trabalho compartilhadas, as gravações nos discos diferenciais são gravadas no armazenamento local no host e não no armazenamento compartilhado.

- O armazenamento compartilhado deve ser NFS quando usar o IntelliCache.
- A Citrix recomenda que você use um dispositivo de armazenamento local de alto desempenho para garantir a transferência de dados mais rápida possível.

Para usar o IntelliCache, você deve ativá-lo no produto e no Citrix Hypervisor.

- Quando instalar o Citrix Hypervisor, selecione **Enable thin provisioning (Optimized storage for Virtual Desktops)**. O Citrix não oferece suporte a pools mistos de servidores que têm o IntelliCache ativado e os que não têm. Para obter mais informações, consulte a documentação do Citrix Hypervisor.
- No Citrix Virtual Apps and Desktops, o IntelliCache é desativado por padrão. Você pode alterar a configuração somente ao criar uma conexão Citrix Hypervisor; não é possível desativar o IntelliCache posteriormente. Quando você adiciona uma conexão Citrix Hypervisor:
  - Selecione **Shared** como o tipo de armazenamento.
  - Selecione a caixa de seleção **Use IntelliCache**.

Criar um catálogo de máquina usando uma conexão do Citrix Hypervisor

As máquinas com capacidade para GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure máquinas compatíveis com GPU para permitir que a VM opere com o software que usa a GPU para operações.

1. No XenCenter, crie uma VM com VGA padrão, redes e vCPU.
2. Atualize a configuração da VM para habilitar o uso de GPU (Passthrough ou vGPU).
3. Instale um sistema operacional suportado e ative o RDP.
4. Instale os drivers Citrix VM Tools e NVIDIA.
5. Limpe o console de administração do Virtual Network Computing (VNC) para otimizar o desempenho e reinicie a VM.
6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e reinicialize a VM.
7. Opcionalmente, crie um instantâneo para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente configurados no XenCenter e use recursos de GPU.

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes do Microsoft System Center Configuration Manager

June 28, 2023

Sites que usam o Microsoft System Center Configuration Manager (Configuration Manager) para gerenciar o acesso a aplicativos e áreas de trabalho podem estender o uso para o Citrix Virtual Apps and Desktops usando estas opções:

- Instalar VDAs usando SCCM.
- **Recurso Configuration Manager Wake Proxy :** o recurso Remote PC Access Wake on LAN é suportado com o Configuration Manager. Para obter detalhes, consulte Wake on LAN - SCCM integrado.
- **Propriedades do Citrix Virtual Apps and Desktops:** as Propriedades permitem que você identifique o Citrix Virtual Desktops para gerenciamento por meio do Configuration Manager. (Em algumas versões, o Configuration Manager usa o nome anterior do Citrix Virtual Apps and Desktops: XenApp e XenDesktop.)

Propriedades

As propriedades estão disponíveis para o Microsoft System Center Configuration Manager para gerenciar áreas de trabalho virtuais.

As propriedades booleanas exibidas no Configuration Manager aparecem como `1` ou `0`, não true ou false.

As propriedades estão disponíveis para a classe `Citrix_virtualDesktopInfo` no espaço de nome `Root\Citrix\DesktopInformation`. O nome das propriedades vem do provedor de Instrumentação de Gerenciamento do Windows (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 a área de trabalho a um usuário; defina como `False` para uma área de trabalho aleatória
`IsMasterImage`	Permite decisões sobre o ambiente. Por exemplo, instale aplicativos na imagem e não nas máquinas provisionadas. Os valores válidos são: `True` em uma VM que é usada como uma imagem. Esse valor é definido durante a instalação com base em uma seleção, ou limpo em uma VM que é provisionada a partir dessa imagem.
`IsVirtualMachine`	`True` para uma máquina virtual, **`false`** para uma máquina física.
`OSChangesPersist`	`False` se a imagem do sistema operacional da área de trabalho for redefinida para um estado limpo sempre que for reiniciada; caso contrário, **`true`**.

Propriedade	Descrição
`PersistentDataLocation`	O local onde o Configuration Manager armazena dados persistentes. Isso não é acessível aos usuários.
`BrokerSiteName`, `DesktopCatalogName`, `DesktopGroupName`, `HostIdentifier`	Determinados quando a área de trabalho se registra no Controller. Eles são nulos para uma área de trabalho que não foi totalmente registrada.

Para coletar as propriedades, execute um inventário de hardware no Configuration Manager. Para exibir as propriedades, use o Configuration Manager Resource Explorer. Nessas instâncias, os nomes incluem espaços ou variam ligeiramente do nome das propriedades. Por exemplo, `BrokerSiteName` aparece como `Broker Site Name`.

- Configurar o Configuration Manager para coletar propriedades Citrix WMI a partir do Citrix VDA
- Criar coleções de dispositivos baseadas em consulta usando as propriedades Citrix WMI
- Criar condições globais com base nas propriedades Citrix WMI
- Usar condições globais para definir requisitos de tipo de implantação de aplicativo

Você também pode usar as propriedades Microsoft na classe Microsoft `CCM_DesktopMachine` no espaço de nome `Root\ccm_vdi`. Para obter mais informações, consulte a documentação da Microsoft.

Ambientes de virtualização do VMware

October 19, 2023

Siga estas instruções se você usa VMware para fornecer máquinas virtuais.

Instale o vCenter Server e as ferramentas de gerenciamento apropriadas. (Não há suporte para a operação Linked Mode do vSphere vCenter.)

Se você planeja usar o MCS, não desative o recurso Datastore Browser no vCenter Server (descrito em https://kb.vmware.com/s/article/2101567). Quando você desativa esse recurso, o MCS não trabalha corretamente.

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

- BIOS legado para VMs com SO de área de trabalho ou servidor compatíveis.

- UEFI para VMs com SO de área de trabalho ou servidor compatíveis, incluindo Inicialização Segura.

Privilégios necessários

Crie uma conta de usuário da VMware e uma ou mais funções de VMware. Baseie a criação dessas funções no nível de granularidade de que precisa para atribuir permissões de usuários. Defina os privilégios para cada função, usando a lista de permissões do vCenter que o Citrix Virtual Apps and Desktops precisa para realizar as operações.

Para conceder permissões a um usuário, associe o usuário à função no nível do data center. Para obter mais informações sobre como definir permissões no vCenter, consulte a documentação do VMware.

As tabelas a seguir mostram os mapeamentos entre as operações do Citrix Virtual Apps and Desktops e os privilégios mínimos necessários do VMware.

> **Nota:**
>
> O nome de exibição da lista de permissões, especificamente *User Interface*, é diferente em algumas versões do vSphere. Por exemplo, no vSphere 6.7 a permissão *User Interface* é **Change Memory** e **Change Settings**, em lugar de **Settings** e **Memory** conforme descrito nos privilégios necessários observados nesta página.

Adicionar conexões e recursos

SDK	Interface de usuário
System. Anonymous, System. Read e System.View	Adicionada automaticamente. Pode usar a função somente leitura interna.

Gerenciamento de energia

SDK	Interface de usuário
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

Provisionar máquinas (Machine Creation Services)

Para provisionar máquinas usando o MCS, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

SDK	Interface de usuário
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Atualização e reversão da imagem

SDK	Interface de usuário
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Excluir máquinas provisionadas

SDK	Interface de usuário
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Perfil de armazenamento (vSAN)

Para exibir, criar ou excluir políticas de armazenamento durante a criação de catálogos em um armazenamento de dados vSAN, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
storage.Profile-driven storage update	PROFILE-DRIVEN STORAGE > Profile-driven storage update
storage.Profile-driven storage view	PROFILE-DRIVEN STORAGE > Profile-driven storage view

Marcas e atributos personalizados

As marcas e os atributos personalizados permitem que você anexe metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e a filtragem desses objetos. Para criar, editar, atribuir e excluir marcas ou categorias, as seguintes permissões são obrigatórias:

SDK	Interface de usuário
Tagging.Create	vSphere Tagging > Create vSphere Tag
Tagging.Create	vSphere Tagging > Create vSphere Tag Category
Tagging.Edit	vSphere Tagging > Edit vSphere Tag
Tagging.Edit	vSphere Tagging > Edit vSphere Tag Category
Tagging.Delete	vSphere Tagging > Delete vSphere Tag
Tagging.Delete	vSphere Tagging > Delete vSphere Tag Category

SDK	Interface de usuário
Tagging.Assign	vSphere Tagging > Assign ou Unassign vSphere Tag
Tagging.Assign	vSphere Tagging > Assign ou Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Nota:**
>
> Quando o MCS cria um catálogo de máquinas, ele marca as VMs de destino com marcas de nomes especiais. Essas marcas diferenciam a imagem mestre das VMs criadas pelo MCS e evitam o uso de VMs criadas pelo MCS para preparação de imagens. Você pode identificar a diferença pelo valor do atributo `XdProvisioned` no vCenter. O atributo é definido como **True** se o MCS criar VMs.

Operações criptográficas

Os privilégios de operações criptográficas controlam quem pode realizar qual tipo de operação criptográfica e em qual tipo de objeto. O vSphere Native Key Provider usa os privilégios `Cryptographer.*`. As seguintes permissões mínimas são necessárias para operações criptográficas:

> **Nota:**
>
> Essas permissões são necessárias para criar catálogos de máquinas MCS com VM equipada com vTPM.

SDK	Interface de usuário
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt

SDK	Interface de usuário
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographic operations.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographic operations.Read KMS information	Privileges > All Privileges > Cryptographic operations > Read KMS information

Provisionar máquinas (Citrix Provisioning)

Todos os privilégios de **Provisionar máquinas (Machine Creation Services)** e o seguinte.

SDK	Interface de usuário
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template

> **Nota:**
>
> As permissões para clonar e implantar um modelo são necessárias para provisionar VMs usando o Assistente de Instalação do Citrix Virtual Apps and Desktops e o Assistente de Exportação de Dispositivos por meio do console Citrix Provisioning.

Obter e importar um certificado

Para proteger as comunicações do vSphere, a Citrix recomenda que você use HTTPS em vez de HTTP.

HTTPS requer certificados digitais. Use um certificado digital emitido por uma autoridade de certificação que atenda à política de segurança da sua organização.

Se você não conseguir usar um certificado digital emitido por uma autoridade de certificação, poderá usar o certificado autoassinado instalado pelo VMware. Use esse método somente se a política de segurança da sua organização o permitir. Adicione o certificado VMware vCenter a cada Delivery Controller.

1. Adicione o nome de domínio totalmente qualificado (FQDN) do computador executando o vCenter Server ao arquivo hosts nesse servidor, em `%SystemRoot%/WINDOWS/system32/Drivers/etc/`. Essa etapa só é necessária se o FQDN do computador que executa o vCenter Server ainda não estiver presente no sistema de nomes de domínio.
2. Obtenha o certificado do vCenter usando qualquer um dos três métodos a seguir:

   Do servidor vCenter.

   a) Copie o arquivo rui.crt do servidor vCenter para um local acessível em seus Delivery Controllers.
   b) No Controller, navegue até o local do certificado exportado e abra o arquivo rui.crt.

   Baixe o certificado usando um navegador da Web. Se você estiver usando o Internet Explorer, 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 estabeleça uma conexão da Web segura com o servidor vCenter (por exemplo, https://server1.domain1.com).
   b) Aceite os avisos de segurança.
   c) Clique na barra de endereços que exibe o erro do certificado.
   d) Examine o certificado e clique na guia Detalhes.
   e) Selecione **Copiar para arquivo e exportar no formato .CER**, fornecendo um nome quando solicitado.
   f) Salve o certificado exportado.
   g) Navegue até o local do certificado exportado e abra o arquivo .CER.

   Importe-o diretamente do Internet Explorer executado como administrador.

   - Abra seu navegador da Web e estabeleça uma conexão da Web segura com o servidor vCenter (por exemplo, https://server1.domain1.com).
   - Aceite os avisos de segurança.
   - Clique na barra de endereços que exibe o erro do certificado.
   - Examine o certificado.

3. Importe o certificado para o repositório de certificados em cada um dos seus Controllers.

   a) Clique na opção **Instalar certificado**, selecione **Máquina local** e clique em **Avançar**.

b) Selecione **Colocar todos os certificados no repositório a seguir** e clique em **Procurar**. Selecione **Pessoas confiáveis** e clique em **OK**. Clique em **Avançar** e, em seguida, clique **Concluir**.

Se você alterar o nome do servidor vSphere após a instalação, será necessário gerar um novo certificado autoassinado no servidor antes de importar o novo certificado.

Considerações de configuração

Criar uma VM mestre:

Use uma VM mestre para fornecer áreas de trabalho e aplicativos de usuário em um catálogo de máquinas. No seu hipervisor:

1. Instale um VDA na VM mestre, selecionando a opção para otimizar a área de trabalho, 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 vCenter SDK.
- Especifique as credenciais de uma conta de usuário do VMware que você configurou anteriormente que tenha permissões para criar VMs. Especifique o nome do 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 a 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 seja pelos Controllers.

Ao criar uma conexão de host do vSphere no Studio, uma caixa de diálogo permite visualizar o certificado da máquina à qual você está se conectando. Você pode então escolher se deve confiar nele.

Redefinir disco do sistema operacional

Use o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do sistema operacional de uma VM persistente em um catálogo de máquinas criado pelo MCS.

Para executar com êxito o comando PowerShell, certifique-se de que:

- As VMs de destino estão em um catálogo persistente do MCS.
- O catálogo de máquinas MCS está funcionando corretamente.
- Isso implica que o esquema de provisionamento e o host existem e que o esquema de provisionamento tem entradas corretas.
- O VMware vCenter não está no modo de manutenção.
- As VMs de destino estão desligadas e no modo de manutenção.

Execute as seguintes etapas para redefinir o disco do sistema operacional:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
3. Execute o comando `Reset-ProvVMDisk` do PowerShell de qualquer uma das seguintes formas:

    - Especifique a lista de VMs como uma lista separada por vírgulas e execute a redefinição em cada VM:

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
        ,"def") -OS
    <!--NeedCopy-->
    ```

    - Especifique a lista de VMs como saída do comando `Get-ProvVM` e execute a redefinição em cada VM:

    ```
    (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
        "abc" -OS
    <!--NeedCopy-->
    ```

    - Especifique uma única VM pelo nome:

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
        -OS
    <!--NeedCopy-->
    ```

    - Crie tarefas de redefinição separadas para cada uma das VMs retornadas pelo comando `Get-ProvVM`. Isso é menos eficiente porque cada tarefa executará as mesmas verificações redundantes, como a verificação da capacidade do hipervisor e verificação de conexão para cada VM.


```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. É exibido um prompt de confirmação que lista as VMs a serem redefinidas juntamente com uma mensagem de aviso de que essa é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma ação é executada.

   > **Nota:**
   >
   > Não retire as VMs do modo de manutenção nem as ligue até a conclusão do processo de redefinição.

   Você pode executar o comando do PowerShell `-WhatIf` para imprimir a ação que ele tomaria e sair sem realizar a ação.

   Você também pode ignorar a solicitação de confirmação usando um dos seguintes métodos:

   - Forneça o parâmetro `-Force`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     <!--NeedCopy-->
     ```

   - Forneça o parâmetro `-Confirm:$false`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Confirm:$false
     <!--NeedCopy-->
     ```

   - Antes de executar o `Reset-ProvVMDisk`, mude `$ConfirmPreference` para **None**:

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'
     PS C:\Windows\system32> $ConfirmPreference
     None
     PS C:\Windows\system32> Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -VMName "abc" -OS
     <!--NeedCopy-->
     ```

5. Execute `Get-ProvTask` para obter o status das tarefas retornadas pelo comando `Reset-ProvVMDisk`.

Atualizar o ID da pasta de um catálogo de máquinas

Você pode atualizar o ID da pasta de um catálogo de máquinas MCS especificando o `FolderId` nas propriedades personalizadas do comando `Set-ProvScheme`. As VMs criadas após a atualização

do ID da pasta são criadas com esse novo ID de pasta. Se essa propriedade não for especificada no `CustomProperties`, as VMs serão criadas na pasta em que a imagem mestre está localizada.

Execute as etapas a seguir para atualizar o ID da pasta de um catálogo de máquinas.

1. Abra um navegador da Web e insira a URL do **vSphere Web Client**.
2. Insira as credenciais e clique em **Login**.
3. Crie uma pasta de posicionamento de VM no **vSphere Web Client**.
4. Abra uma janela do PowerShell.
5. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
6. Especifique `FolderID` em `CustomProperties` de `Set-ProvScheme`. Neste exemplo, o valor do ID da pasta é `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
     f630687372" -CustomProperties "<CustomProperties xmlns=""http
     ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
     http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
     ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
     CustomProperties>"
2 <!--NeedCopy-->
```

7. Adicione uma VM ao catálogo de máquinas usando o Studio.
8. Verifique a nova VM no vSphere Web Client. A nova VM é criada na nova pasta.

Encontrar o ID da pasta no vSphere

Acesse o Managed Object Browser (MOB) em qualquer sistema de servidor ESXi ou vCenter para encontrar o ID da pasta das VMs.

O MOB é um aplicativo de servidor baseado na Web, disponível em todos os sistemas de servidor ESX/ESXi e vCenter. Esse utilitário do vSphere permite que você visualize informações detalhadas sobre objetos como VMs, armazenamentos de dados e pools de recursos.

1. Abra um navegador da Web e digite `http://x.x.x.x/mob`, onde x.x.x.x é o endereço IP do vCenter Server ou o host ESX/ESXi. Por exemplo, https://10.60.4.70/mob.
2. Na **página inicial** do MOB, clique no valor da propriedade **content**.
3. Clique no valor de **rootFolder**.
4. Clique no valor de **childEntity**.
5. Clique no valor de **vmFolder**.
6. Você pode encontrar o ID da pasta no valor de **childEntity**.

Solução de problemas

Se houver falha ao criar o catálogo, consulte CTX294978.

Soluções de nuvem e de parceiros da VMware

April 3, 2024

O Citrix Virtual Apps and Desktops oferece suporte às seguintes soluções de nuvem e parceiros do VMware:

- Solução VMware no Azure (AVS)
- Google Cloud VMware Engine
- Nuvem VMware na Amazon Web Services (AWS)

Integração do Azure VMware Solution (AVS)

O serviço Citrix Virtual Apps and Desktop oferece suporte ao AVS. O AVS fornece infraestrutura de nuvem contendo clusters do vSphere criados pela infraestrutura do Azure. Aproveite o Citrix Virtual Apps and Desktop Service para usar o AVS para provisionar sua carga de trabalho do VDA da mesma forma que você usaria o vSphere em ambientes locais.

Configuração do cluster AVS

Para permitir que o Citrix Virtual Apps and Desktop Service use o AVS, execute as seguintes etapas no Azure:

- Solicite uma cota de host
- Registre o provedor de recursos Microsoft.AVS
- Lista de verificação de rede
- Crie uma nuvem privada do Azure VMware Solution
- Acesse uma nuvem privada do Azure VMware Solution
- Configure a rede para sua nuvem privada VMware no Azure
- Configure o DHCP para a solução VMware do Azure
- Adicione um segmento de rede no Azure VMware Solution
- Verifique o ambiente do Azure VMware Solution

Solicitar cota de host para clientes do Azure Enterprise Agreement Na página **Help + Support** do portal do Azure, selecione **New support request** e inclua as seguintes informações:

- Issue type:Technical
- Subscription:Select your subscription
- Service:All services > Azure VMware Solution
- Resource:General question
- Summary:Need capacity
- Problem type:Capacity Management Issues
- Problem subtype:Customer Request for Additional Host Quota/Capacity

Na **Description** do ticket de suporte, inclua as seguintes informações na guia **Details** :

- POC or Production
- Region Name
- Number of hosts
- Any other details

> **Nota:**
>
> O AVS requer um mínimo de três hosts e recomenda que você use redundância de hosts N+1.

Depois de especificar os detalhes do ticket de suporte, selecione **Review + Create** para enviar a solicitação ao Azure.

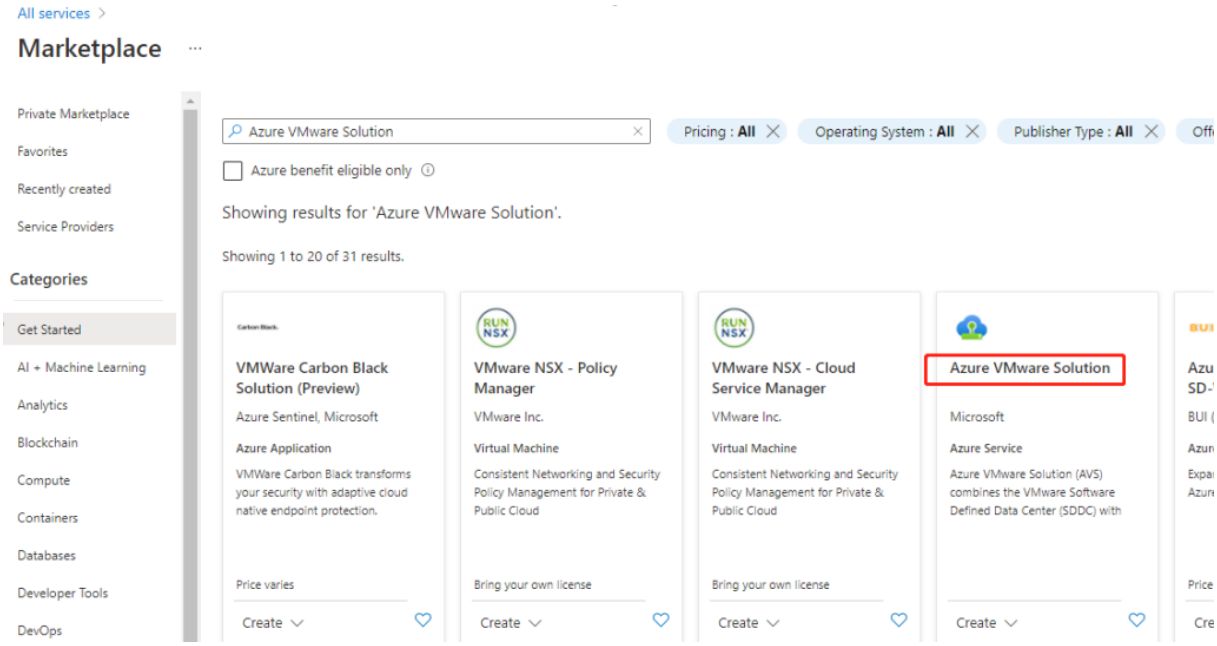
Registre o provedor de recursos Microsoft.AVS Depois de solicitar a cota do host, registre o provedor de recursos:

1. Faça login no portal do Azure.
2. No menu do portal do Azure, selecione **All services**.
3. No menu **All services**, insira a assinatura e selecione **Subscriptions**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Resource providers** e insira **Microsoft.AVS** na barra de pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

Considerações sobre rede O AVS oferece serviços de rede que exigem intervalos de endereços de rede e portas de firewall específicos. Consulte Lista de verificação de planejamento de rede da Solução VMware no Azure para obter mais informações.

Crie uma nuvem privada do Azure VMware Solution Depois de considerar os requisitos de rede para o seu ambiente, crie uma nuvem privada ASV:

1. Faça login no portal do Azure.
2. Selecione **Create a new resource**.
3. Na caixa de texto **Search the Marketplace**, digite *Azure VMware Solution* e selecione **Azure VMware Solution** na lista.



imagem

Na janela **Solução VMware do Azure**:

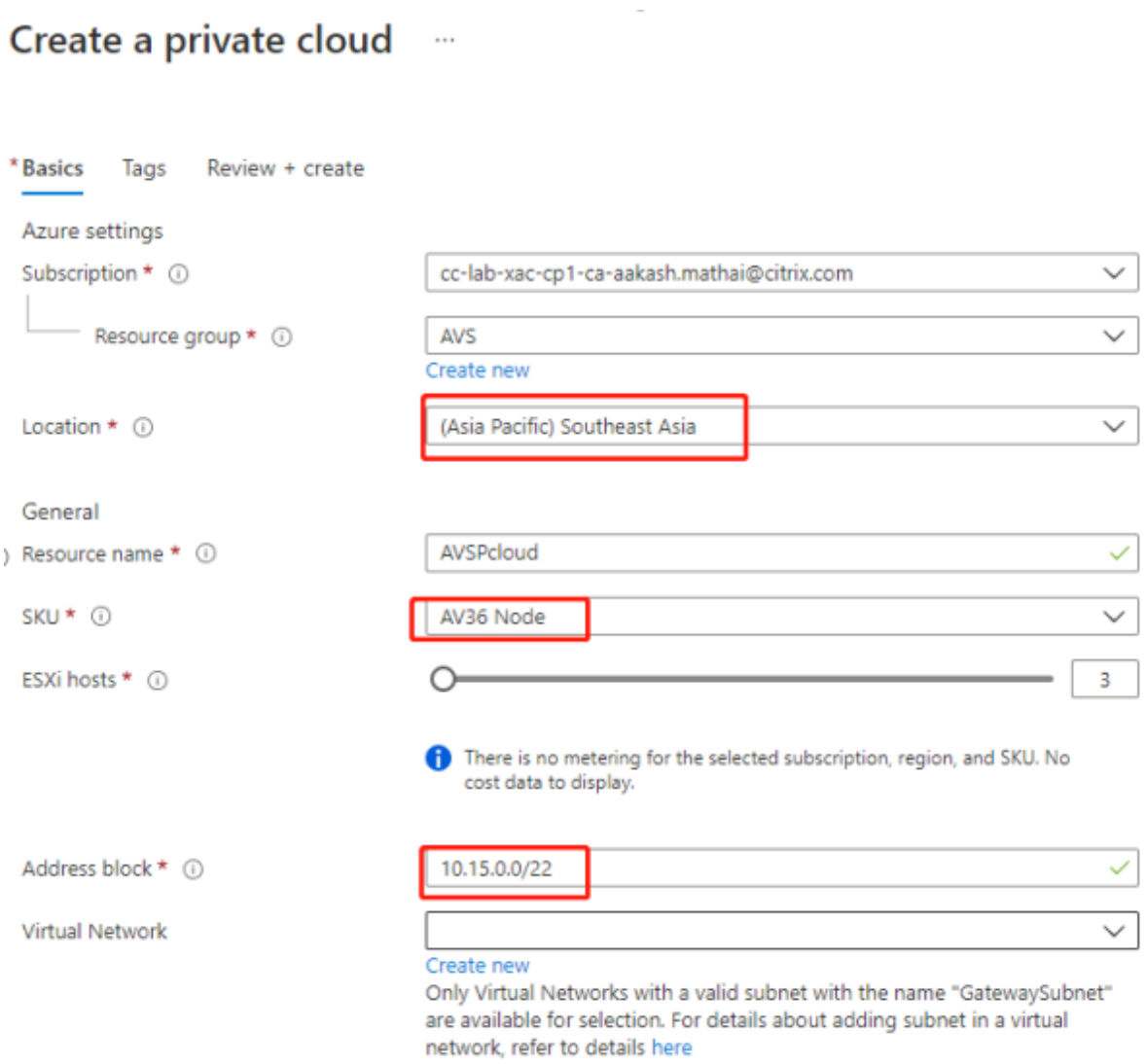
1. Selecione **Create**.
2. Click the **Basics** tab.
3. Insira valores para os campos, usando as informações da tabela abaixo:

Campo	Valor
Subscription	Selecione a assinatura que você planeja usar para a implantação. Todos os recursos em uma assinatura do Azure são cobrados juntos.
Resource group	Selecione o grupo de recursos para sua nuvem privada. Um grupo de recursos do Azure é um contêiner lógico no qual os recursos do Azure são implantados e gerenciados. Como alternativa, você pode criar um novo grupo de recursos para sua nuvem privada.

Campo	Valor
Localização	Selecione um local, como east us. Essa é a região que você definiu durante a fase de planejamento.
Nome do recurso	Forneça o nome da nuvem privada do Azure VMware Solution.
SKU	Selecione AV36.
Hosts	Mostra o número de hosts alocados para o cluster de nuvem privada. O valor padrão é 3, que pode ser aumentado ou diminuído após a implantação.
Bloco de endereço	Forneça um bloco de endereço IP para a nuvem privada. O CIDR representa a rede de gerenciamento de nuvem privada e será usado para os serviços de gerenciamento de cluster, como o vCenter Server e o NSX-T Manager. Use o espaço de endereçamento /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure, nem a redes locais.
Rede virtual	Deixe isso em branco porque o circuito do Azure VMware Solution ExpressRoute é estabelecido como uma etapa pós-implantação.

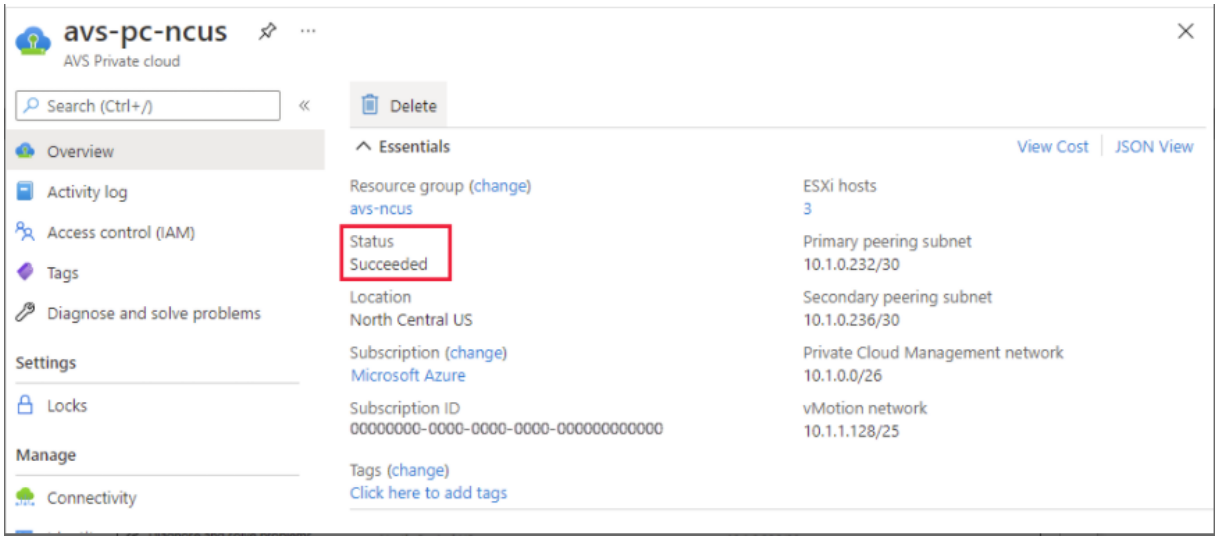
Na tela **Create a private cloud** :

1. No campo **Location**, selecione a região que tem o AVS; a região do grupo de recursos é a mesma que a região AVS.
2. No campo **SKU**, selecione **AV36 Node**.
3. Especifique um endereço IP no campo **Address Block**. Por exemplo, 10.15.0.0/22.
4. Selecione **Review + Create**.
5. Depois de analisar as informações, clique em **Create**.



> **Dica:**
>
> A criação de uma nuvem privada pode levar de 3 a 4 horas. A adição de um único host ao cluster pode levar de 30 a 45 minutos.

Verifique se a implantação foi bem-sucedida. Navegue até o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Succeeded**, a implantação estará concluída.



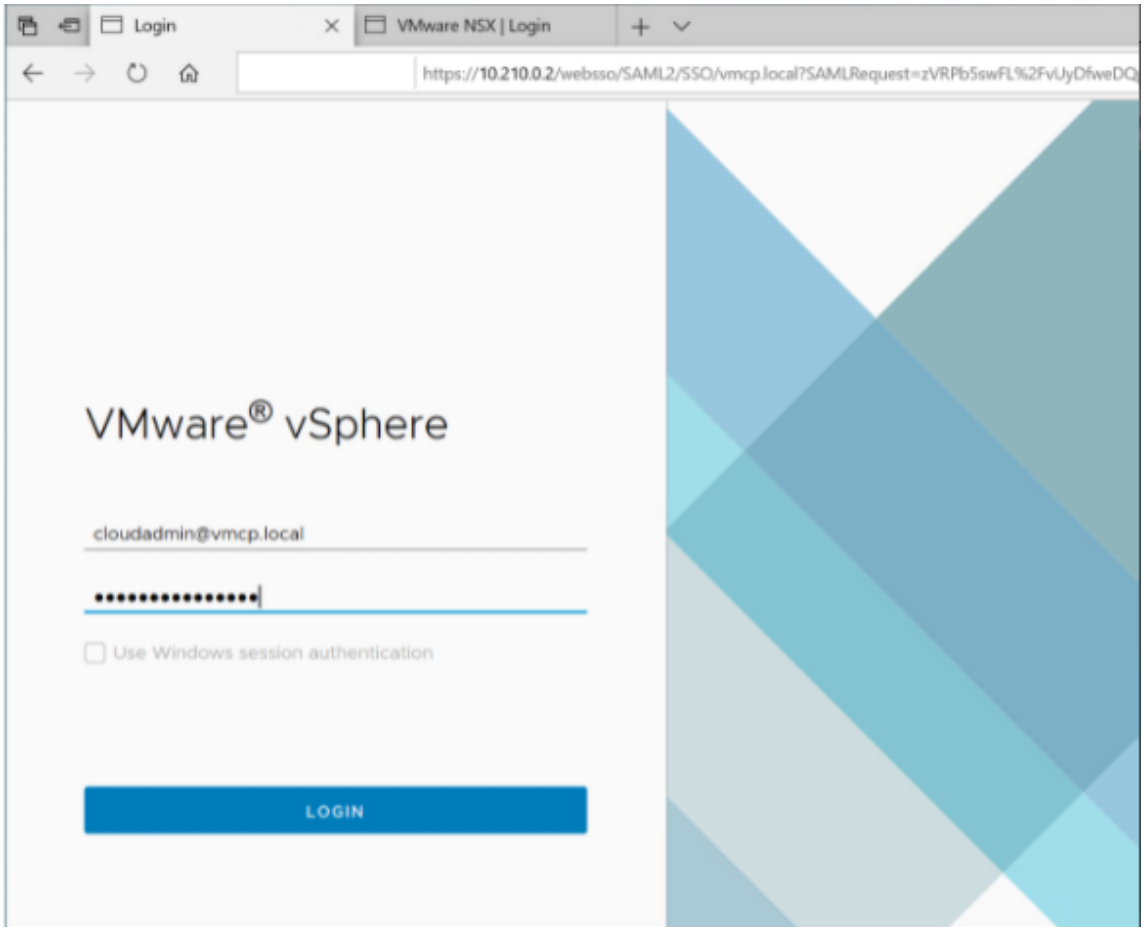
Acesse uma nuvem privada do Azure VMware Solution Depois de criar uma nuvem privada, crie uma VM do Windows e conecte-se ao vCenter local da sua nuvem privada.

Crie uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar** e, em seguida, pesquise e selecione **Microsoft Windows 10/2016/2019**.
2. Clique em **Create**.
3. Insira as informações necessárias e selecione **Review + Create**.
4. Depois que a validação for aprovada, selecione **Create** para iniciar o processo de criação da máquina virtual.

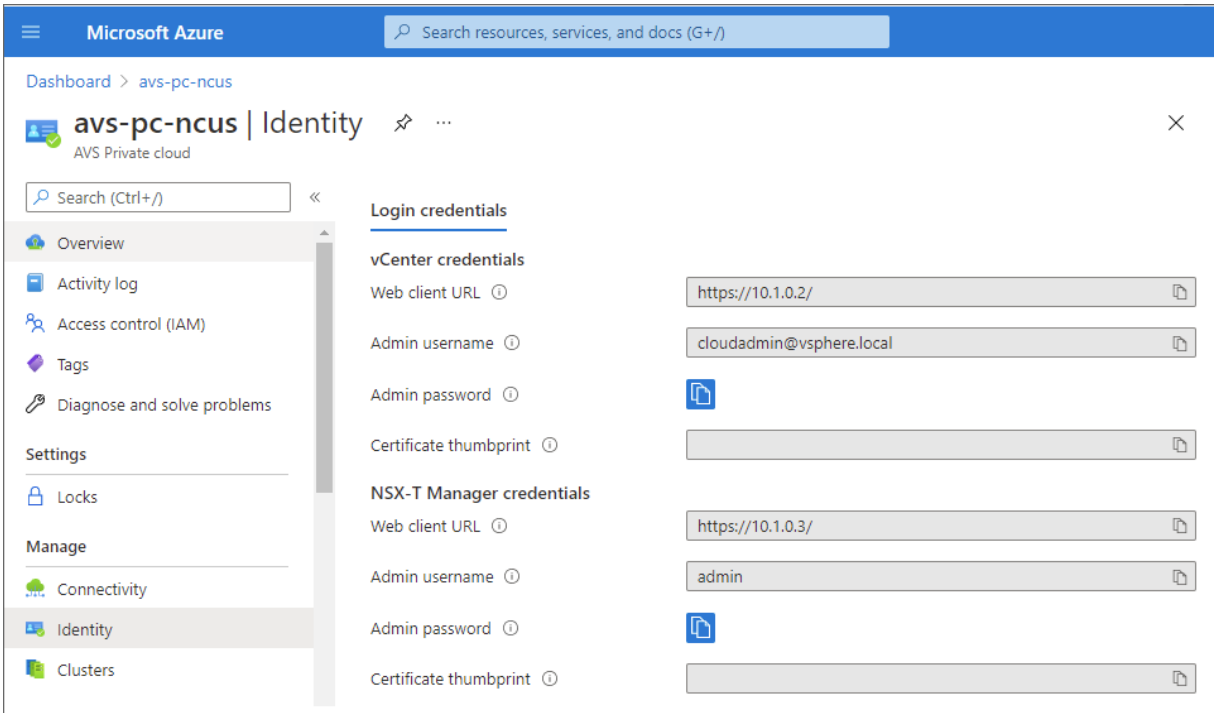
Conecte-se ao vCenter local da sua nuvem privada

1. Faça login em **vSphere Client with VMware vCenter SSO** como administrador de nuvem.



2. No portal do Azure, selecione sua nuvem privada e, em seguida, **Manage> Identity**.

Os URLs e credenciais de usuário para o vCenter de nuvem privada e o NSX-T Manager são exibidos:



Display private cloud vCenter and NSX Manager URLs and credentials.

Depois de confirmar URLs e credenciais do usuário:

1. Navegue até a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegue até os URLs do vCenter e do NSX-T Manager em duas guias do navegador. Na guia vCenter, insira as credenciais de usuário *cloudadmin@vmcp.local* da etapa anterior.

Configure a rede para sua nuvem privada VMware no Azure Depois de acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.

Crie uma rede virtual

1. Faça login no portal do Azure.
2. Navegue até o grupo de recursos criado anteriormente.
3. Selecione **+ Add** para definir um novo recurso.
4. Na caixa de texto **Search the Marketplace**, digite *virtual network*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Virtual Network**, selecione **Create** para configurar a rede virtual para sua nuvem privada.
6. Na página **Create Virtual Network**, insira os detalhes da sua rede virtual.
7. Na guia **Basics**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Next : IP Addresses.**

8. Na guia **IP Addresses**, no espaço de endereço IPv4, insira o endereço criado anteriormente.

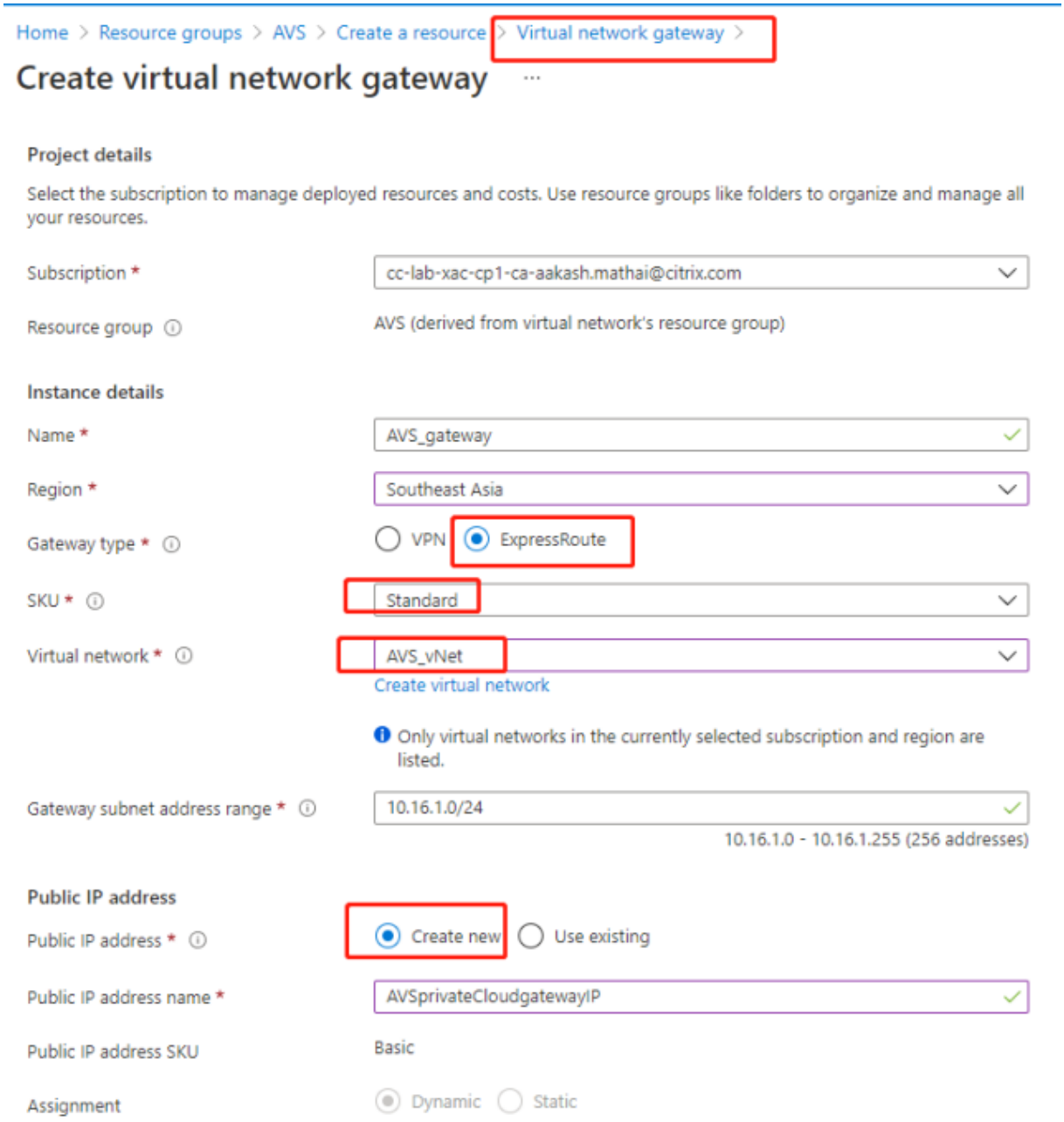
> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço usado ao criar sua nuvem privada.

Depois de entrar no espaço de endereço:

1. Selecione **+ Add subnet**.
2. Na página **Add subnet**, dê à sub-rede um nome e um intervalo de endereços apropriado.
3. Clique em **Add**.
4. Selecione **Review + create**.
5. Verifique as informações e clique em **Create**. Quando a implantação estiver concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual Depois de criar uma rede virtual, crie um gateway de rede virtual.

1. No grupo de recursos, selecione **+ Add** para adicionar um novo recurso.
2. Na caixa de texto **Search the Marketplace**, digite *virtual network gateway*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Virtual Network gateway**, clique em **Create**.
4. Na guia **Basics** da página **Create virtual network gateway**, forneça valores para os campos.
5. Clique em **Review + create**.



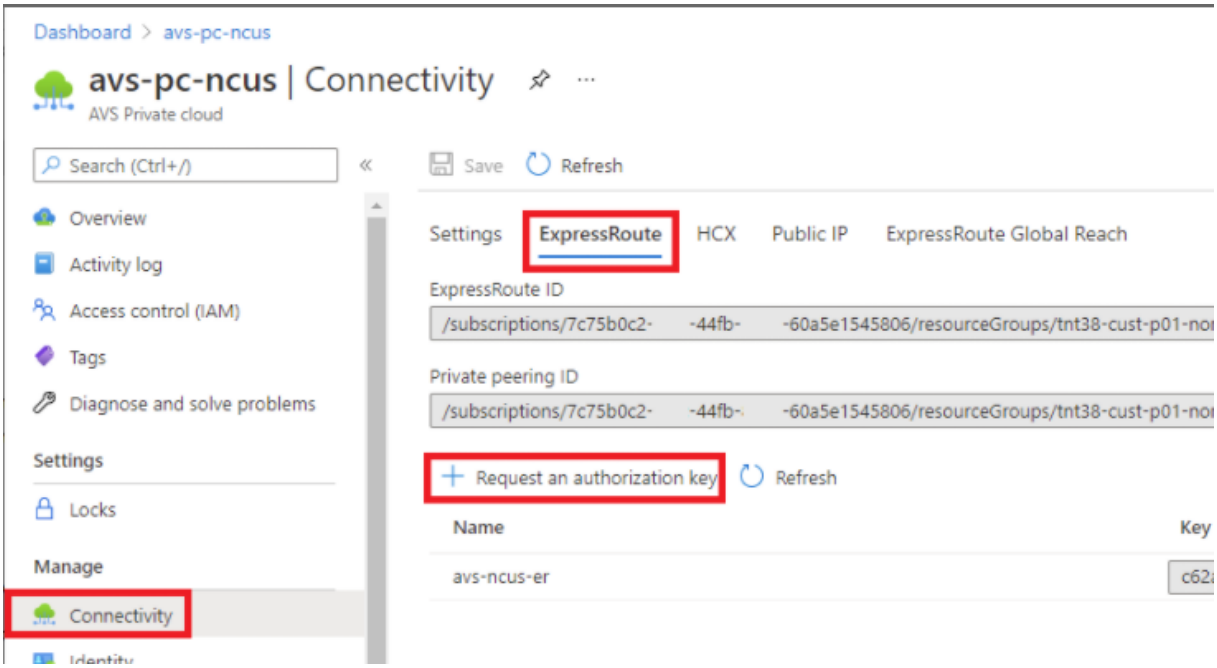
Depois de analisar a configuração do gateway de rede virtual, clique em **Create** para implantar o gateway de rede virtual.

Após a conclusão da implantação, conecte sua conexão do **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada do Azure AVS.

Conectar o ExpressRoute ao gateway de rede virtual Depois de implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada do Azure AVS:

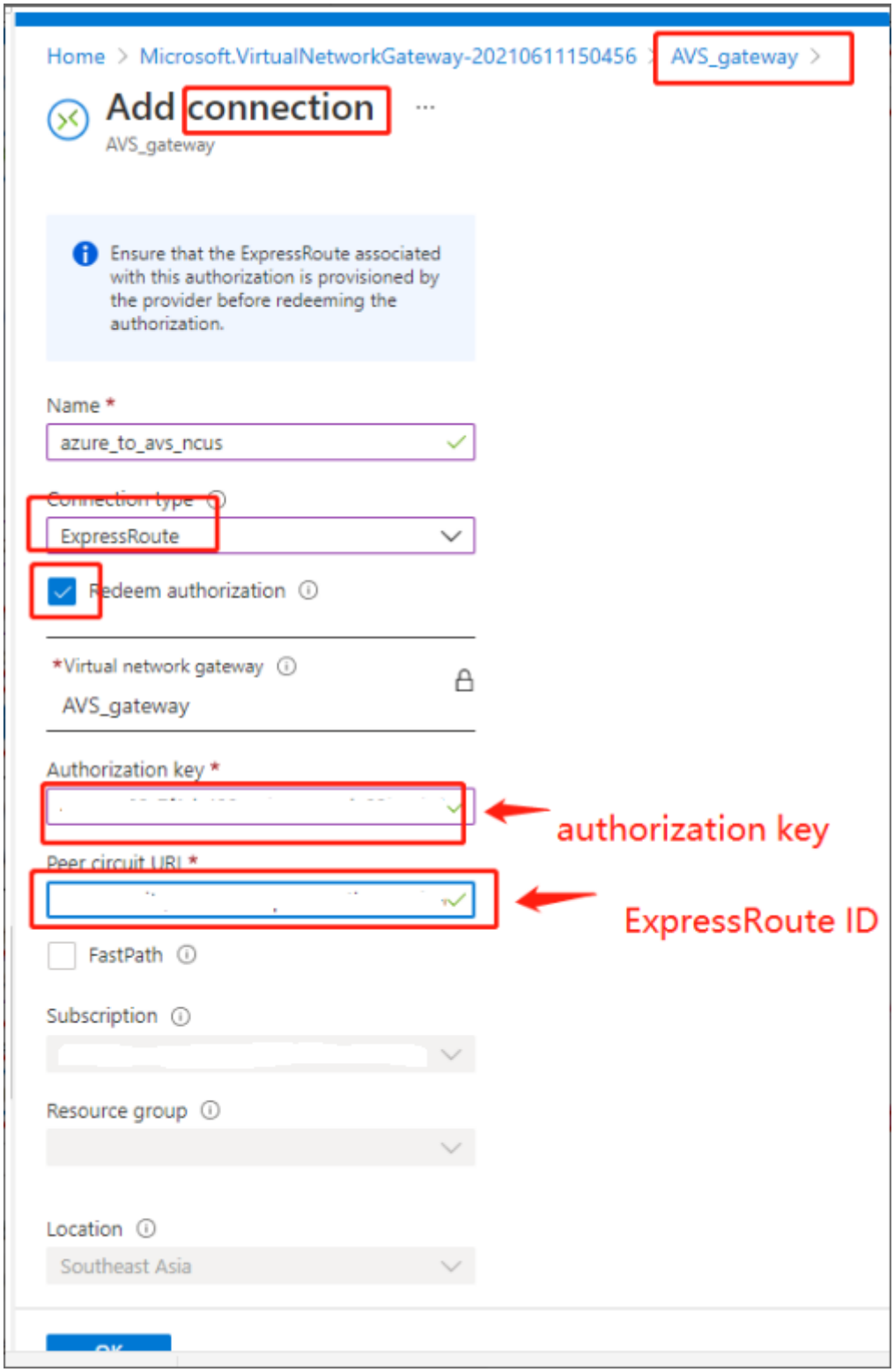
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegue até a **nuvem privada do Azure VMware Solution**. Selecione **Manage> Connectivity > ExpressRoute** e, em seguida, selecione **+ Request an authorization key.**

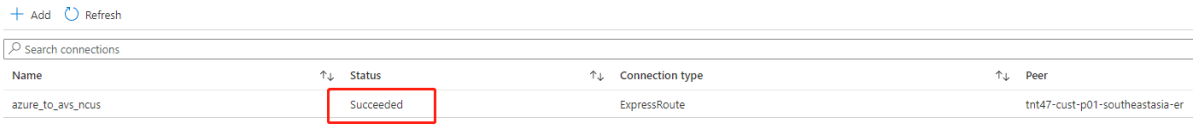


Depois de solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Create**. Pode levar cerca de 30 segundos para criar a chave. Depois de criada, a nova chave aparece na lista de chaves de autorização para a nuvem privada.
2. Copie a **chave de autorização** e o **ID do ExpressRoute**. Você precisará deles para concluir o processo de peering. A chave de autorização desaparece após algum tempo, então copie-a assim que ela aparecer.
3. Navegue até o **gateway de rede virtual** que você planeja usar e selecione **Connections> + Add**.
4. Na página **Add connection**, forneça valores para os campos e selecione **OK.**



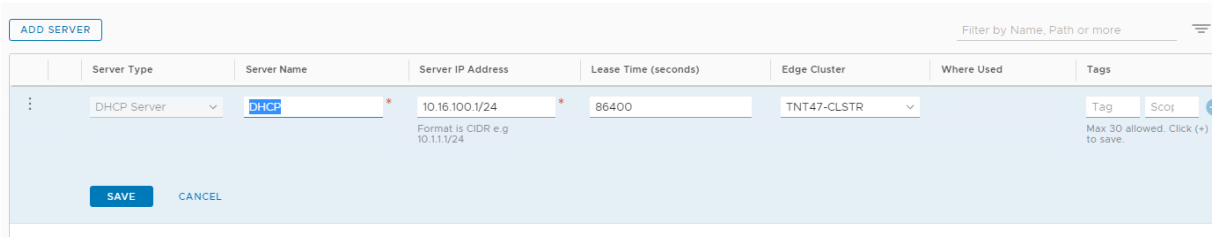
A conexão é estabelecida entre o circuito do ExpressRoute e sua rede virtual:



Configure o DHCP para a solução VMware do Azure Depois de conectar o ExpressRoute ao gateway virtual, configure o DHCP.

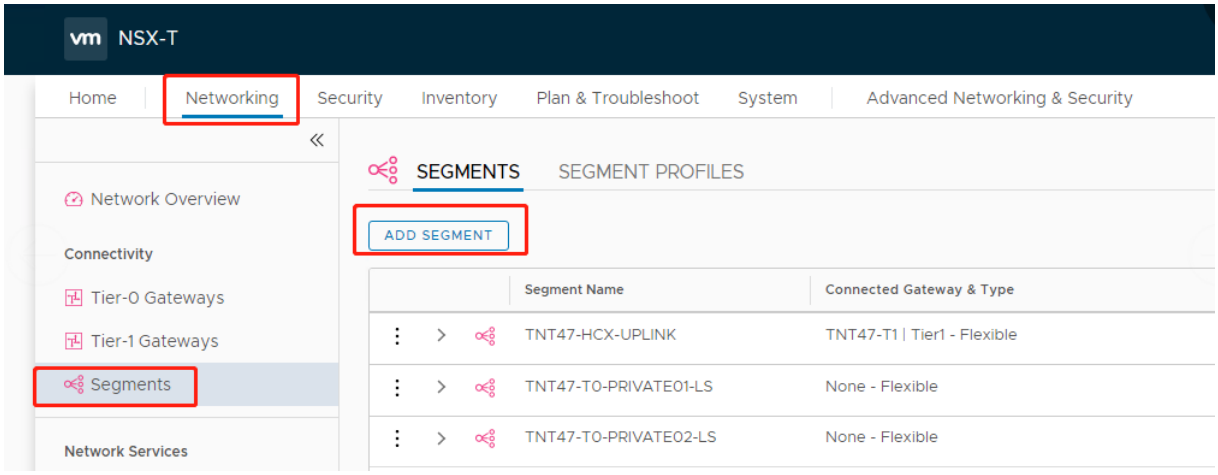
Usar o NSX-T para hospedar seu servidor DHCP No NSX-T Manager:

1. Selecione **Networking> DHCP** e, em seguida, selecione **Add Server**.
2. Selecione **DHCP** para o **Server Type**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Tier 1 Gateways**, selecione as reticências verticais no gateway de camada 1 e, em seguida, selecione **Edit**.
5. Selecione **No IP Allocation Set** para adicionar uma sub-rede.
6. Selecione **DHCP Local Server** para o **Type**.
7. Para o **DHCP Server**, selecione **Default DHCP** e clique em **Save**.
8. Clique em **Save** novamente e selecione **Close Editing**.



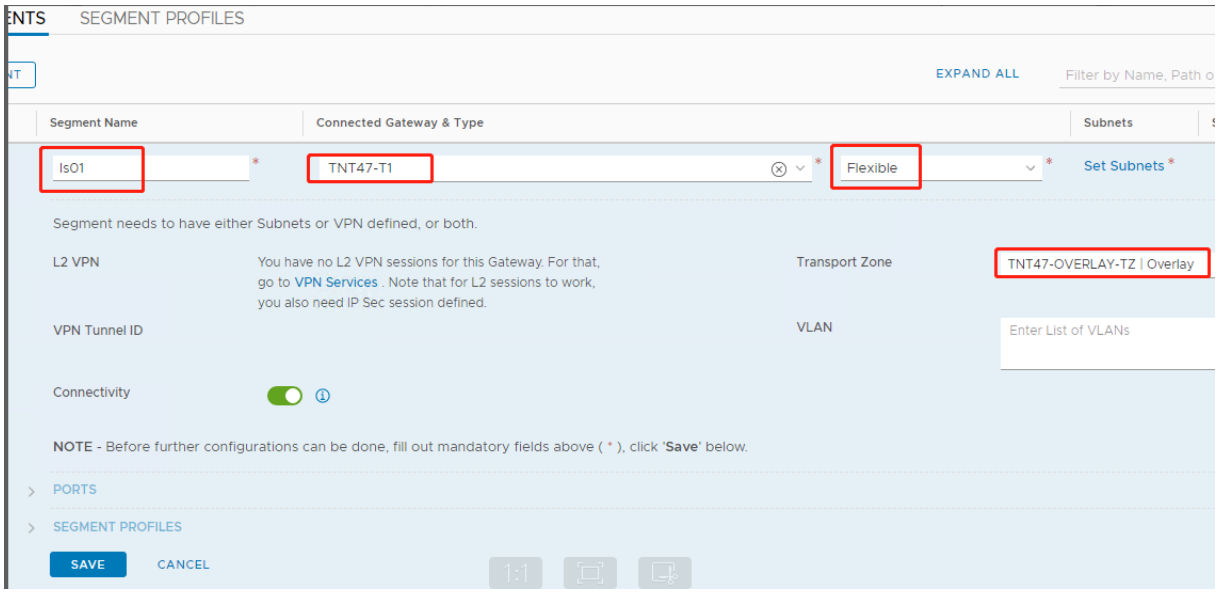
Adicione um segmento de rede no Azure VMware Solution Depois de configurar o DHCP, adicione um segmento de rede.

Para adicionar um segmento de rede, no NSX-T Manager, selecione **Networking> Segments** e clique em **Add Segment**.



Na tela **Segments profile**:

1. Insira um **nome** para o segmento.
2. Selecione o **Tier-1 Gateway (TNTxx-T1)** como o **Connected Gateway** e deixe o **Type** como **Flexible**.
3. Selecione a **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Clique em **Set Subnets**.



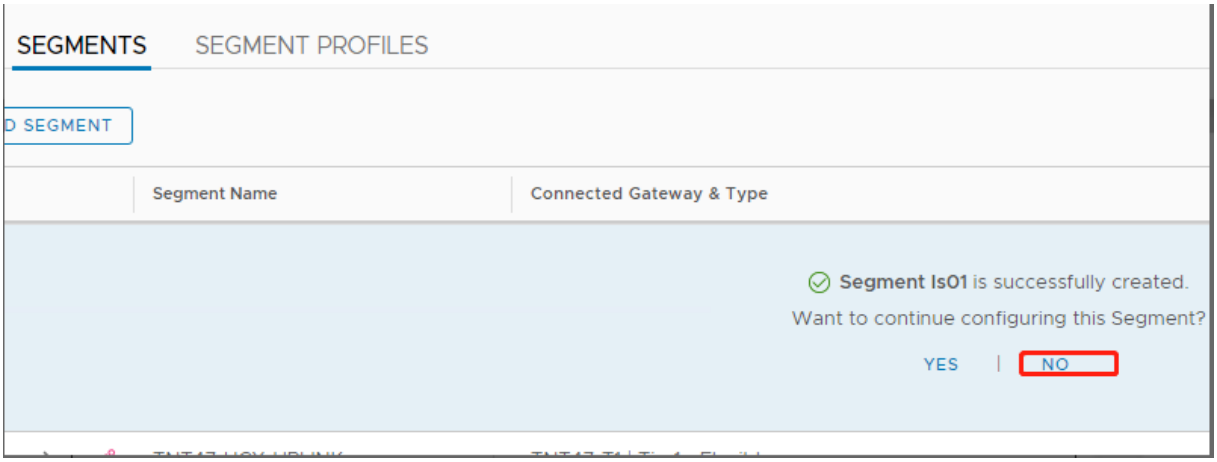
Na seção **Subnets** :

1. Digite o endereço IP do gateway.
2. Selecione **Add**.

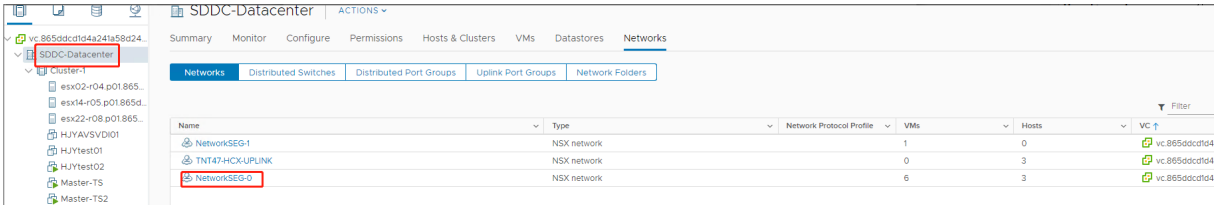
> **Importante:**
>
> O endereço IP desse segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.

O intervalo DHCP deve pertencer ao endereço IP do segmento:

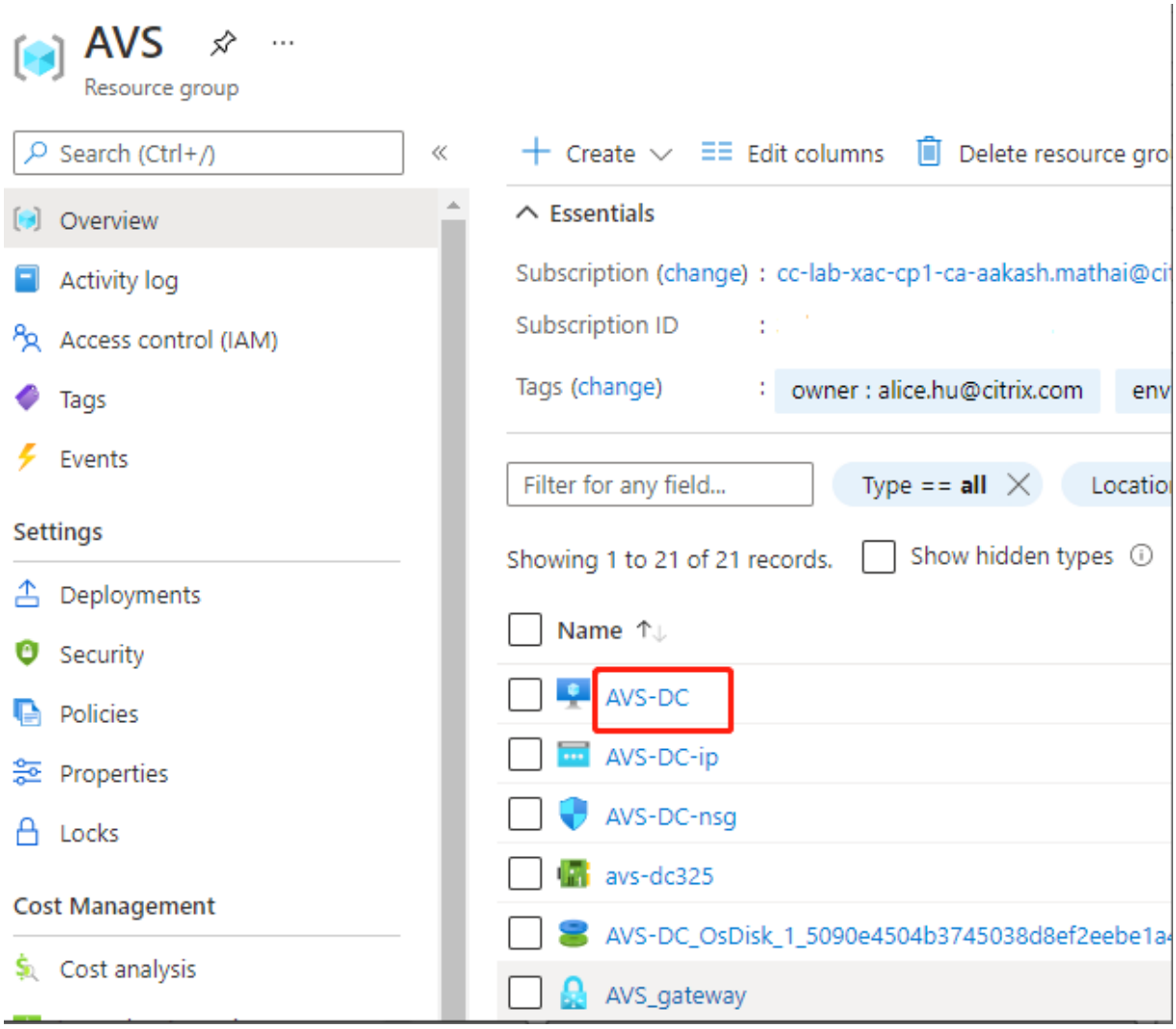
Selecione **No** para recusar a opção de continuar configurando o segmento:



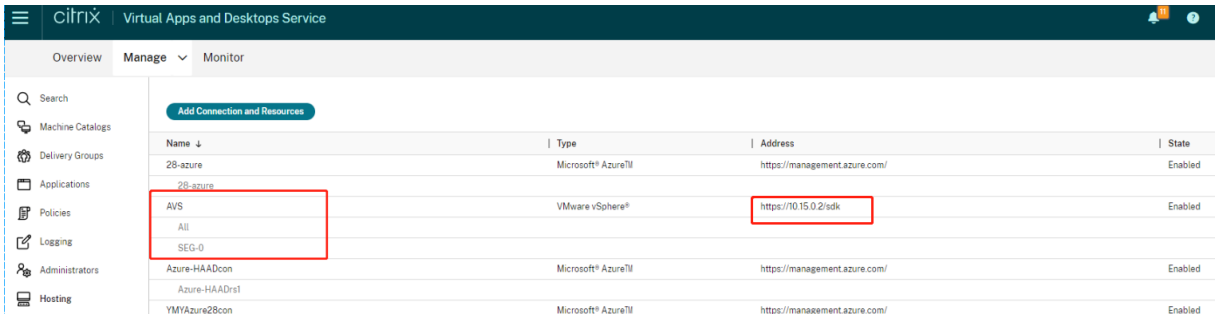
No vCenter, selecione **Rede > Datacenter SDDC**:



Verificar o ambiente do Azure AVS Configure uma conexão direta e um conector no grupo de recursos do Azure:



Verifique a conexão com as credenciais do vCenter:



Google Cloud VMware Engine

O Citrix Virtual Apps and Desktops permite migrar cargas de trabalho Citrix locais baseadas em VMware para o Google Cloud VMware Engine.

Configurar o Google Cloud VMware Engine

O procedimento a seguir descreve como adquirir e configurar um cluster no Google Cloud VMware Engine.

Acessar o portal do VMware Engine

1. No **Google Cloud Console**, clique no menu de navegação.
2. Na seção **Compute**, clique em **VMware Engine** para abrir o VMware Engine em uma nova guia do navegador.

Requisitos para criar a primeira nuvem privada Você precisa ter acesso ao Google Cloud VMware Engine, à cota de nós disponível do VMware Engine e a uma função do IAM apropriada. Prepare os seguintes requisitos antes de continuar a criar a sua nuvem privada:

1. Solicite acesso à API e cota de nós. Para obter mais informações, consulte Como solicitar acesso e cota da API.
2. Anote os intervalos de endereços que você deseja usar para os dispositivos de gerenciamento VMware e a rede de implantação HCX. Para obter mais informações, consulte Requisitos de rede.
3. Obtenha a função do IAM de VMware Engine Service Admin.

Criar a sua primeira nuvem privada

1. Acesse o portal do VMware Engine.
2. Na página inicial do VMware Engine, clique em **Create a private cloud**. O local de hospedagem e os tipos de nó de hardware são listados.
3. Selecione o número de nós para a nuvem privada. Pelo menos três nós são necessários.
4. Insira um intervalo CIDR (Classless Inter-Domain Routing) para a rede de gerenciamento VMware.
5. Insira um intervalo CIDR para a rede de implantação HCX.

   > **Importante:**
   >
   > O intervalo CIDR não deve se sobrepor a nenhuma de suas sub-redes locais ou na nuvem. O intervalo CIDR deve ser /27 ou superior.

6. Selecione **Review and create**.
7. Revise as configurações. Para alterar a configuração, clique em **Back**.
8. Clique em **Create** para começar a criar a nuvem privada.

À medida que o VMware Engine cria a sua nova nuvem privada, ele implanta vários componentes do VMware e define políticas de Autoscale iniciais para clusters na nuvem privada. A criação da nuvem privada pode levar de 30 minutos a 2 horas. Depois que o provisionamento é concluído, você recebe um e-mail.

Configurar o gateway VPN do Google Cloud VMware Engine Para estabelecer a conectividade inicial com o Google Cloud VMware Engine, você pode usar um gateway VPN. Essa é uma VPN cliente baseada em OpenVPN com a qual você pode se conectar ao seu vCenter SDDC (VMware Software Defined Data Center) e fazer qualquer configuração inicial necessária.

Antes de implantar um gateway VPN, configure o intervalo de **Edge Services** para a região onde o seu SDDC está implantado. Para isso:

1. Faça logon no portal do **Google Cloud VMware Engine** e acesse **Network > Regional Settings**. Clique em **Add Region**.
2. Escolha a região em que o seu SDDC está implantado e ative **Internet Access** e **Public IP Service**.
3. Forneça o intervalo dos Edge Services anotado durante o planejamento e clique em **Submit**. A ativação desses serviços leva de 10 a 15 minutos.

   Depois de concluídos, os Edge Services são exibidos como **Enabled** na página Regional Settings. A ativação dessas configurações permite que IPs públicos sejam alocados para o seu SDDC, o que é um requisito para a implantação de um gateway VPN.

Para implantar um gateway VPN:

1. No portal do **Google Cloud VMware Engine**, acesse **Network > VPN Gateways**. Clique em **Create New VPN Gateway**.
2. Forneça o nome do gateway VPN e da sub-rede cliente reservados durante o planejamento. Clique em **Avançar**.
3. Selecione os usuários para conceder acesso à VPN. Clique em **Avançar**.
4. Especifique as redes que devem ser acessíveis por VPN. Clique em **Avançar**.
5. Uma tela de resumo é exibida. Verifique as seleções e clique em **Submit** para criar o gateway VPN. A página VPN Gateways é exibida com o status do novo gateway VPN como **Creating**.
6. Depois que o status mudar para **Operational**, clique no novo gateway VPN.
7. Clique em **Download my VPN configuration** para baixar um arquivo ZIP contendo perfis OpenVPN pré-configurados para o gateway VPN. Perfis para conexão por meio de UDP/1194 e TCP/443 estão disponíveis. Escolha a sua preferência e importe-a para o Open VPN; depois conecte-se.
8. Vá para **Resources** e selecione o seu SDDC.

Conectar a VPN

1. Estabeleça uma conexão ponto a site entre sua rede local e a nuvem privada por meio da configuração do VPN Gateway. Consulte Configurar o gateway VPN do Google Cloud VMware Engine.
2. Carregue a configuração da VPN baixada em Configurar o gateway VPN do Google Cloud VMware Engine.
3. Importe para a sua VPN cliente, por exemplo, OpenVPN Connect.

Para obter mais informações, consulte Como se conectar usando uma VPN.

Criar a primeira sub-rede

Acessar o NSX-T Manager no portal do VMware Engine O processo de criação de uma sub-rede acontece no NSX-T, que você acessa por meio do VMware Engine. Faça o seguinte para acessar o NSX-T Manager.

1. Faça logon no portal do **Google Cloud VMware Engine**.
2. Na navegação principal, vá para **Resources**.
3. Clique no **nome da nuvem privada** correspondente à nuvem privada em que você deseja criar a sub-rede.
4. Na página de detalhes da sua nuvem privada, clique na guia **vSphere Management Network**.
5. Clique no **FQDN** correspondente ao NSX-T Manager.
6. Quando solicitado, insira suas credenciais de login. Se você configurou o vIDM e o conectou a uma origem de identidade, como o Active Directory, use as suas credenciais de origem de identidade.

> **Lembrete:**
>
> Você pode recuperar as credenciais geradas na página de detalhes da nuvem privada.

Configurar o serviço DHCP para a sub-rede Antes de criar uma sub-rede, configure um serviço DHCP:

No NSX-T Manager:

1. Vá para **Networking > DHCP**. O painel de rede mostra que o serviço DHCP cria um gateway Tier-0 e outro Tier-1.
2. Para começar a provisionar um servidor DHCP, clique em **Add Server**.
3. Selecione **DHCP** para o **Server Type**, forneça o nome do servidor e o endereço IP.
4. Clique em **Save** para criar o serviço DHCP.

Faça o seguinte para anexar esse serviço DHCP ao gateway Tier-1 relevante. Um gateway padrão Tier-1 já está provisionado pelo serviço DHCP :

1. Selecione **Tier 1 Gateways**, selecione as reticências verticais no gateway de camada 1 e, em seguida, selecione **Edit**.
2. No campo **IP Address Management**, selecione **No IP Allocation Set**.
3. Selecione **DHCP Local Server** para o **Type**.
4. Selecione o servidor DHCP que você criou para o **DHCP Server**.
5. Clique em **Salvar**.
6. Clique em **Close Editing**.

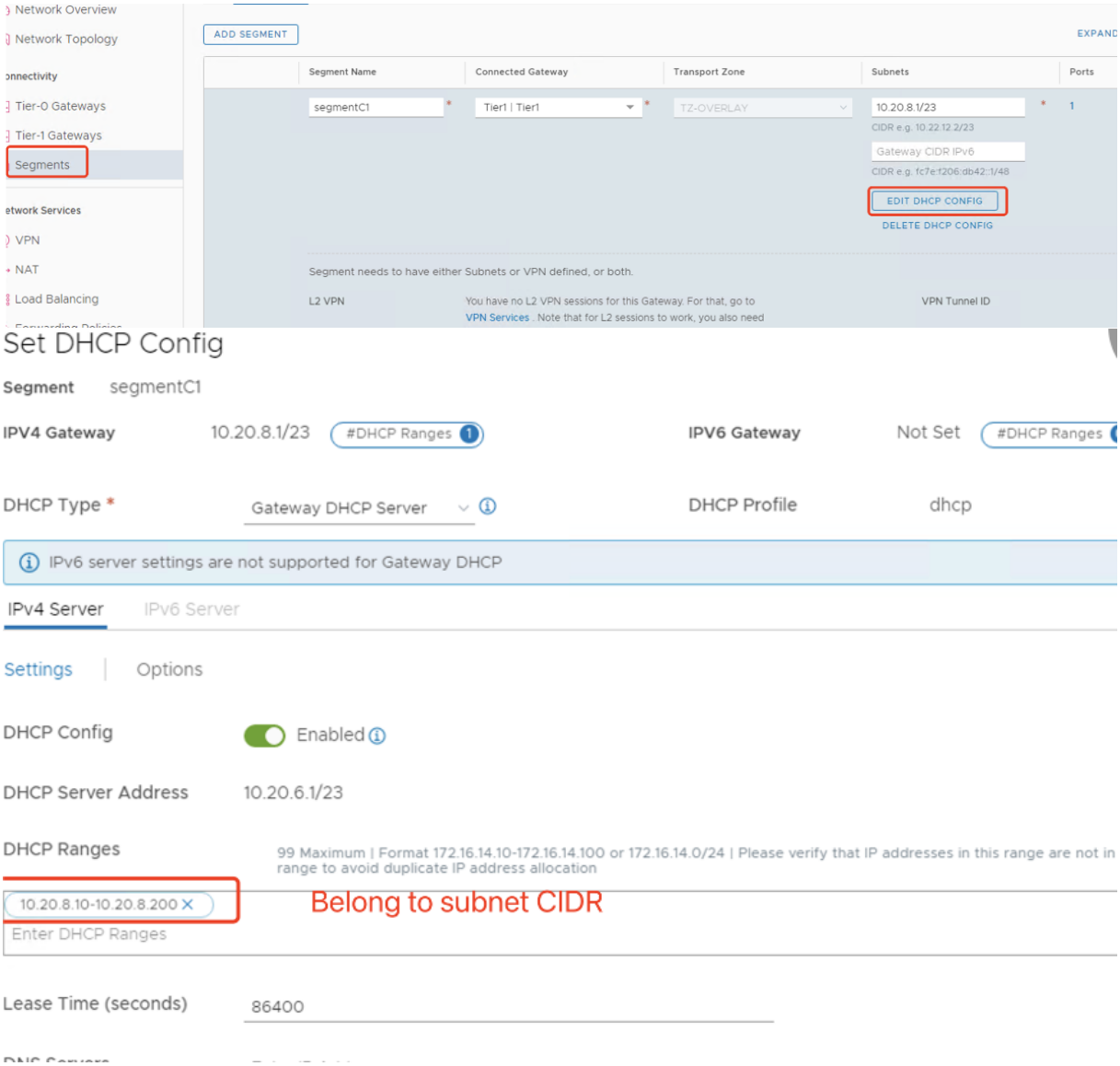
Agora você pode criar um segmento de rede no NSX-T. Para obter mais informações sobre DHCP no NSX-T, consulte a documentação do VMware para DHCP.

Criar um segmento de rede no NSX-T Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede do NSX-T para a sua nuvem privada:

1. No NSX-T Manager, vá para **Networking > Segments**.
2. Clique em **Add Segment**.
3. Insira um nome para o segmento.
4. Selecione **Tier-1** como **Connected Gateway** e deixe Type como **Flexible**.
5. Clique em **Set Subnets**.
6. Clique em **Add Subnets**.
7. Insira o intervalo de sub-rede em **Gateway IP/Prefix Length**. Especifique o intervalo de sub-rede com **.1** como o último octeto. Por exemplo, **10.12.2.1/24**.
8. Especifique os intervalos de DHCP e clique em **ADD**.
9. Em **Transport Zone**, selecione **TZ-OVERLAY** na lista suspensa.
10. Clique em **Salvar**. Agora você pode selecionar esse segmento de rede no vCenter quando criar uma VM.

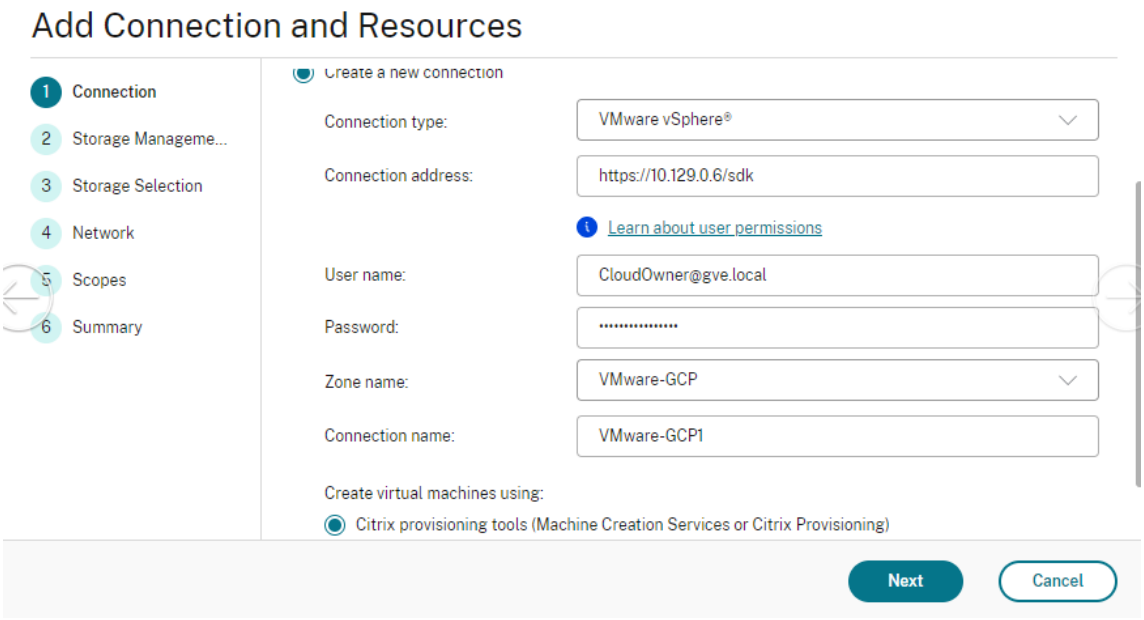
Em uma determinada região, você pode configurar no máximo 100 rotas exclusivas do VMware Engine para a sua rede VPC usando o acesso a serviços privados. Isso inclui, por exemplo, intervalos de endereços IP de gerenciamento de nuvem privada, segmentos de rede de carga de trabalho NSX-T e intervalos de endereços IP de rede HCX. Esse limite inclui todas as nuvens privadas na região.

> **Nota:**
>
> Há um problema de configuração do Google Cloud, por isso você precisa definir a configuração do intervalo DHCP várias vezes. Portanto, certifique-se de definir a configuração do intervalo DHCP após a configuração do Google Cloud. Clique em **EDIT DHCP CONFIG** para configurar os intervalos de DHCP.



Criar a conexão do Google Cloud VMware no Citrix Studio

1. Crie uma máquina no vCenter.
2. Inicie o Citrix Studio.
3. Selecione o nó de hospedagem e clique em **Add Connection and Resources**.
4. Na tela **Connection**, selecione **Create a new Connection** e os seguintes detalhes:



a) Selecione **Connection type** como **VMware vSphere**.
b) Em **Connection address**, insira o endereço IP privado de vCenter.
c) Insira as credenciais do vCenter.
d) Digite um nome para a conexão.
e) Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Network**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

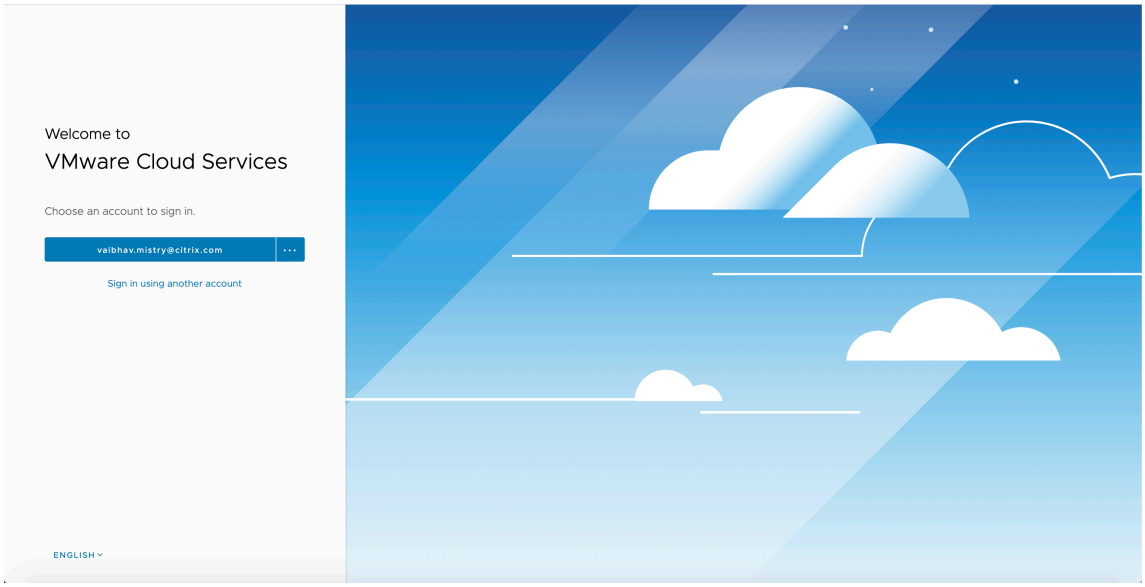
Nuvem VMware na Amazon Web Services (AWS)

A nuvem VMware na Amazon Web Services (AWS) permite que você migre cargas de trabalho locais da Citrix baseadas em VMware para a Nuvem AWS.

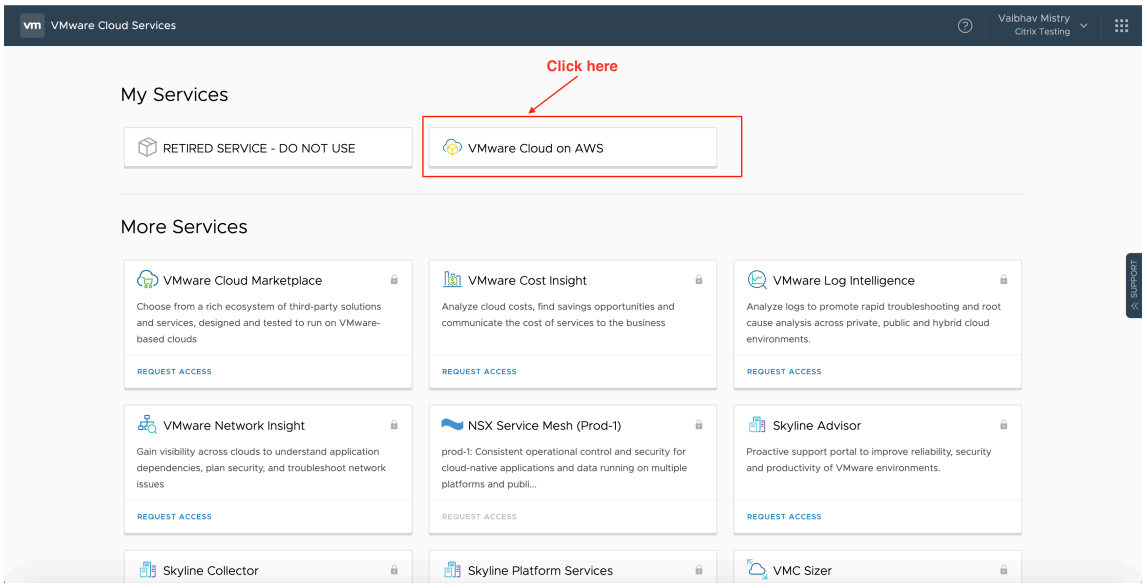
Este artigo descreve o procedimento para configurar uma nuvem VMware na AWS.

Acesse o ambiente de nuvem VMware

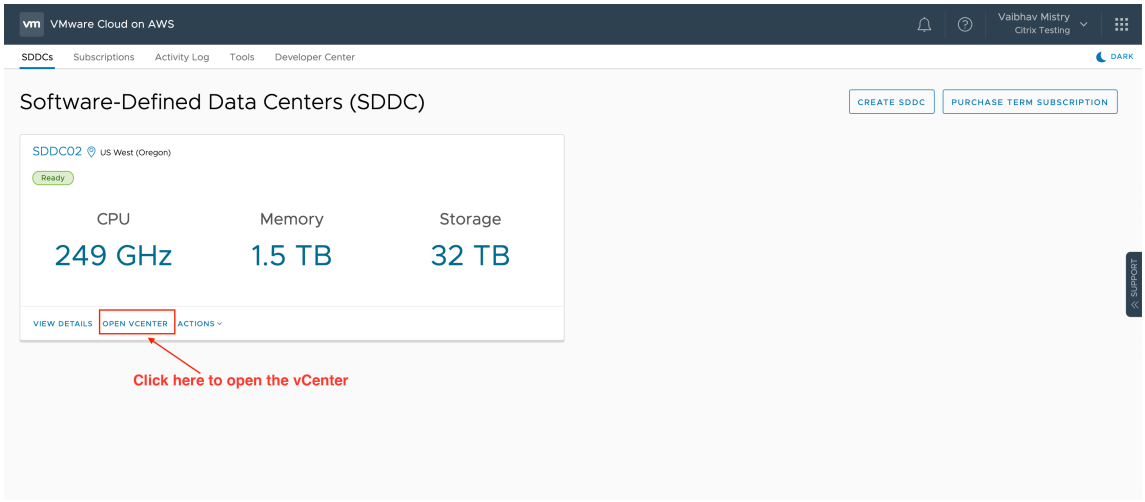
1. Faça login nos serviços de nuvem da VMware usando o URL https://console.cloud.vmware.com/.

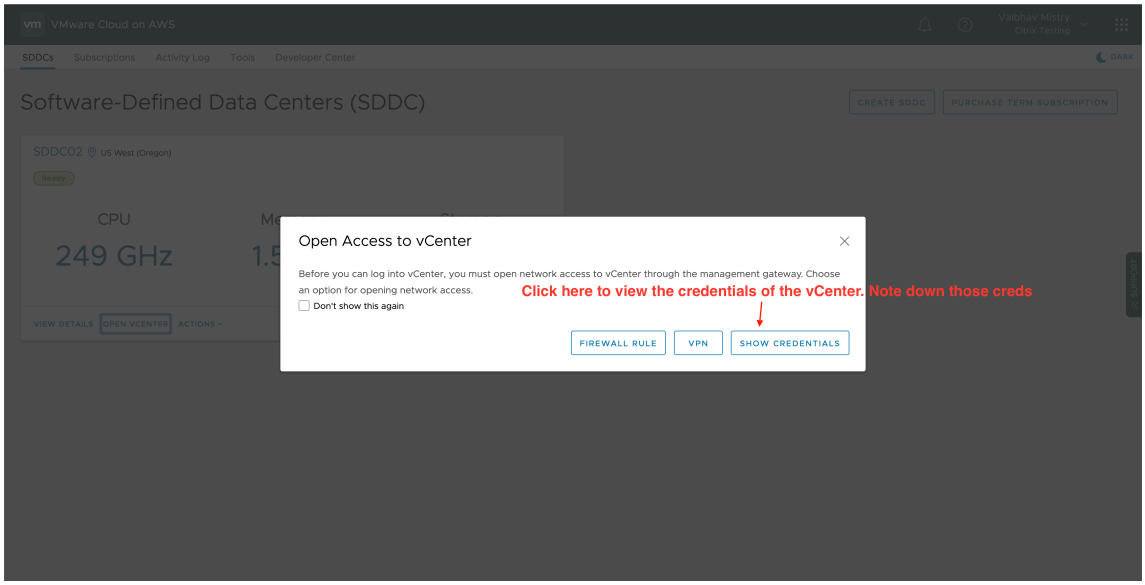


2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

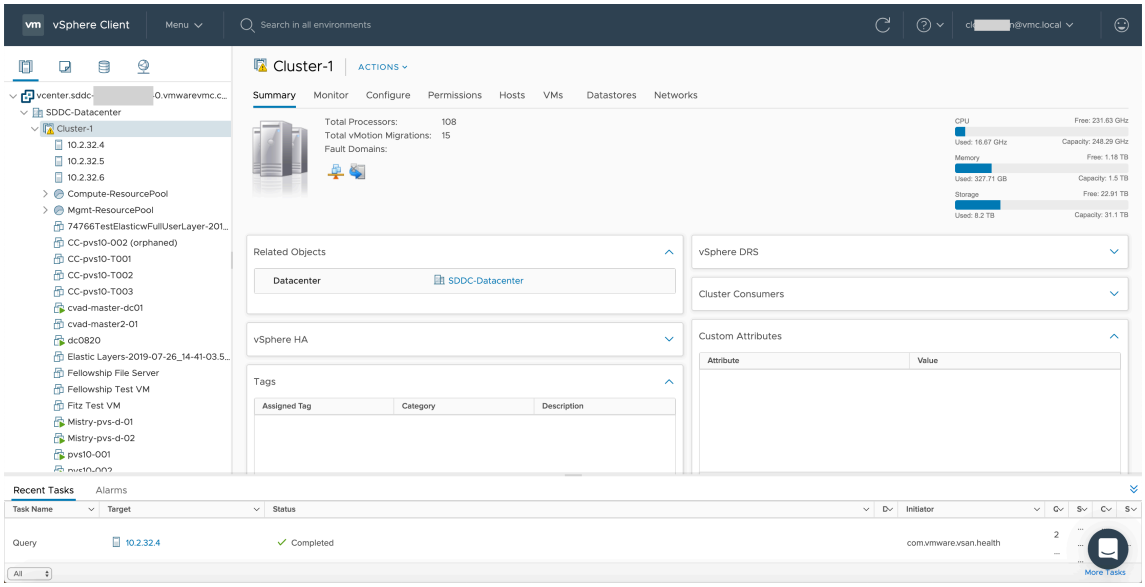


3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Observe as credenciais para uso posterior.





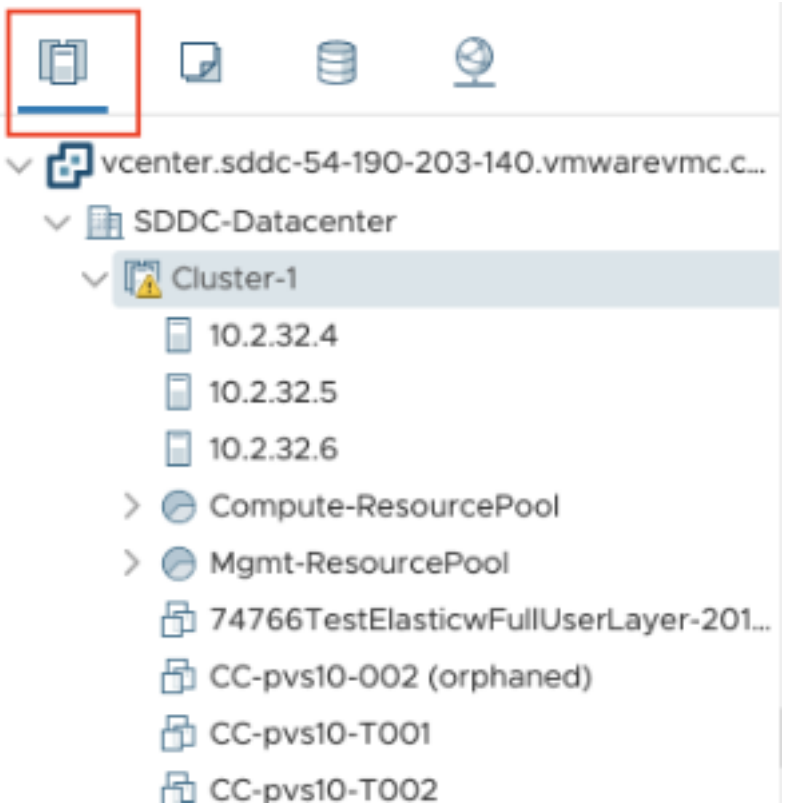
4. Abra um navegador da Web e insira a URL do vSphere Web Client.
5. Insira as credenciais conforme indicado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



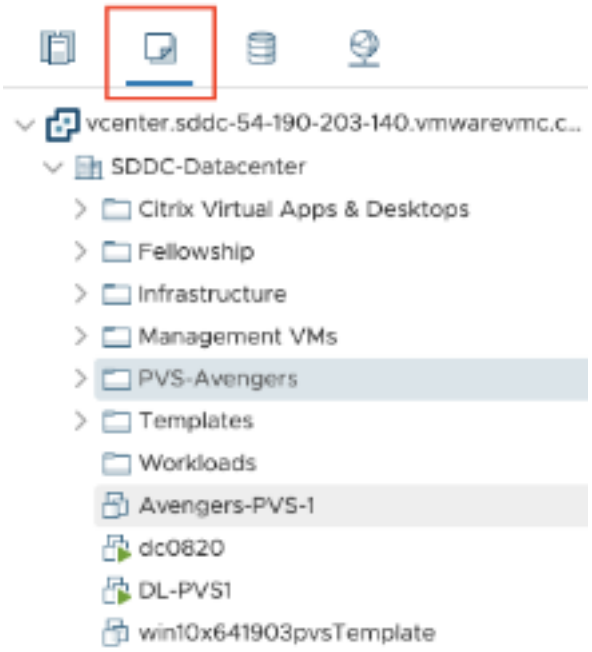
Sobre o ambiente de nuvem VMware

Há quatro visualizações na página da Web do cliente vSphere.

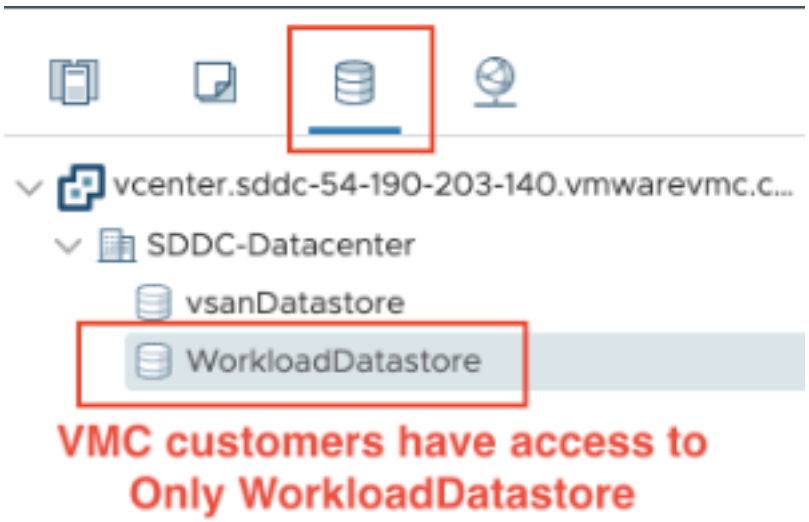
- Visualização de host e cluster: você não pode criar um novo cluster, mas o administrador da nuvem pode criar vários pools de recursos.



- Visualização de VM e modelo: o administrador da nuvem pode criar várias pastas.



- Exibição de armazenamento: selecione **WorkloadDatastore** storage ao adicionar a unidade de hospedagem no Citrix Studio porque você tem acesso somente ao Workload Datastore.



- Exibição de rede: os ícones são diferentes para redes em nuvem VMware e redes opacas.

Depois de configurar o cluster, consulte Ambientes de virtualização VMware para adicionar conexões e recursos.

Ambientes de nuvem da AWS

April 3, 2024

Este artigo o orienta na configuração de sua conta da AWS como um local de recursos que você pode usar com o Citrix Virtual Apps and Desktops. O local de recursos inclui um conjunto básico de componentes, ideal para uma prova de conceito ou outra implantação que não exija recursos distribuídos por várias zonas de disponibilidade. Depois de concluir essas tarefas, você pode instalar VDAs, provisionar máquinas, criar catálogos de máquinas e criar grupos de entrega.

Quando concluir as tarefas deste artigo, o local de recursos incluirá os seguintes componentes:

- Uma nuvem privada virtual (VPC) com sub-redes públicas e privadas dentro de uma única zona de disponibilidade.
- Uma instância que é executada como um Controlador de Domínio do Active Directory e um servidor DNS, localizada na sub-rede privada da VPC.
- Uma instância que atua como um host bastion na sub-rede pública da sua VPC. Essa instância é usada para iniciar conexões RDP com as instâncias na sub-rede privada para fins administrativos. Depois de concluir a configuração do local de recursos, você pode encerrar a instância para que ela não fique mais prontamente acessível. Quando for necessário gerenciar outras instâncias na sub-rede privada, como as instâncias do VDA, você pode reiniciar a instância do host bastion.

Visão geral da tarefa

Configure uma nuvem privada virtual (VPC) com sub-redes pública e privada. Quando você concluir essa tarefa, a AWS implantará um gateway NAT com um endereço Elastic IP na sub-rede pública. Essa ação permite que instâncias na sub-rede privada acessem a Internet. As instâncias na sub-rede pública são acessíveis ao tráfego público de entrada, enquanto as instâncias na sub-rede privada não são.

Configure grupos de segurança. Os grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também associa esses grupos de segurança a cada instância na sua VPC.

Crie um conjunto de opções de DHCP. Com uma Amazon VPC, os serviços DHCP e DNS são fornecidos por padrão, o que afeta a forma como você configura o DNS no seu Controlador de Domínio do Active Directory. O DHCP da Amazon não pode ser desativado e o DNS da Amazon pode ser usado apenas para resolução de DNS público, não para resolução de nomes do Active Directory. Para especificar os servidores de domínio e nome entregues às instâncias por meio do DHCP, crie um conjunto de opções DHCP. O conjunto atribui o sufixo de domínio do Active Directory e especifica o servidor DNS para todas as instâncias na sua VPC. Para garantir que os registros Host (A) e de Pesquisa inversa (PTR) sejam registrados automaticamente quando as instâncias ingressarem no domínio, configure as propriedades do adaptador de rede para cada instância adicionada à sub-rede privada.

Adicione um bastion host e um Controlador de Domínio à VPC. Por meio do bastion host, você pode fazer login 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 VPC Dashboard, selecione **Create VPC**.
3. Selecione **VPC and more**.
4. Em NAT gateways ($) selecione **In 1 AZ** ou **1 per AZ**.
5. Nas opções de DNS, deixe **Enable DNS hostnames** selecionada.
6. Selecione **Create VPC**. A AWS cria as sub-redes pública e privada, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

Tarefa 2: Configurar grupos de segurança

Essa tarefa cria e configura os seguintes grupos de segurança para a sua VPC:

- Um grupo de segurança público a ser associado às instâncias em sua sub-rede pública.
- Um grupo de segurança privado a ser associado às instâncias em sua sub-rede privada.

Para criar os grupos de segurança:

1. No VPC Dashboard, selecione **Security Groups**.
2. Crie um grupo de segurança para o grupo de segurança pública. Selecione **Create Security Group** e insira uma marca de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Yes, Create**.

Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Origem
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	Selecione o grupo de segurança público.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0

Tipo	Origem
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Quando tiver terminado, selecione **Save**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Destino
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Quando tiver terminado, selecione **Save**.

Configurar o grupo de segurança privado

1. Na lista de grupos de segurança, selecione o grupo de segurança privado.
2. Se você não configurou o tráfego do grupo de segurança público, é necessário definir portas TCP; selecionar a guia **Inbound Rules** e selecionar **Edit** para criar as seguintes regras:

Tipo	Origem
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	Selecione o grupo de segurança público.
ICMP	Selecione o grupo de segurança público.
TCP 53 (DNS)	Selecione o grupo de segurança público.
UDP 53 (DNS)	Selecione o grupo de segurança público.
80 (HTTP)	Selecione o grupo de segurança público.
TCP 135	Selecione o grupo de segurança público.

Tipo	Origem
TCP 389	Selecione o grupo de segurança público.
UDP 389	Selecione o grupo de segurança público.
443 (HTTPS)	Selecione o grupo de segurança público.
TCP 1494 (ICA/HDX)	Selecione o grupo de segurança público.
TCP 2598 (Session Reliability)	Selecione o grupo de segurança público.
3389 (RDP)	Selecione o grupo de segurança público.
TCP 49152–65535	Selecione o grupo de segurança público.

3. Quando tiver terminado, selecione **Save**.
4. Selecione a guia **Outbound Rules** e selecione **Edit** para criar as seguintes regras:

Tipo	Destino
ALL Traffic	Selecione o grupo de segurança privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Quando tiver terminado, selecione **Save**.

Tarefa 3: Executar instâncias

Siga as etapas a seguir para criar duas instâncias do EC2 e descriptografar a senha de administrador padrão gerada pela Amazon:

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No EC2 Dashboard, selecione **Launch Instance**.
3. Selecione uma imagem de máquina do Windows Server e um tipo de instância.
4. Na página **Configure Instance Details**, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Subnet**, faça as seguintes seleções para cada instância:
    - Bastion host: selecione a sub-rede pública

- Domain Controller: selecione a sub-rede privada

6. Em **Auto-assign Public IP address**, faça as seguintes seleções para cada instância:
   - Bastion host: selecione **Enable.**
   - Domain Controller: selecione **Use default setting** ou **Disable**.
7. Em **Network Interfaces**, insira um endereço IP primário dentro do intervalo de IP da sub-rede privada para o Controlador de Domínio.
8. Se necessário, na página **Add Storage**, modifique o tamanho do disco.
9. Na página **Tag Instance**, insira um nome amigável para cada instância.
10. Na página **Configure Security Groups**, selecione **Select an existing security group** e faça as seguintes seleções para cada instância:
    - Bastion host: selecione o grupo de segurança público.
    - Domain Controller: selecione o grupo de segurança privado.
11. Revise suas escolhas e selecione **Launch**.
12. Crie um novo par de chaves ou selecione um par existente. Se você criar um novo par de chaves, baixe seu arquivo de chave privada (.pem) e mantenha-o em um local seguro. Você deve fornecer sua chave privada ao adquirir a senha de administrador padrão para a instância.
13. Selecione **Launch Instances**. Selecione **View Instances** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-executada tenha passado por todas as verificações de status antes de acessá-la.
14. Adquira a senha de administrador padrão para cada instância:
    a) Na lista de instâncias, selecione a instância e, em seguida, selecione **Connect**.
    b) Vá até a guia **RDP client**, selecione **Get Password** e carregue seu arquivo de chave privada (`.pem`) quando solicitado.
    c) Selecione **Decrypt Password** para obter a senha legível por humanos. A AWS exibe a senha padrão.
15. Repita as etapas da etapa 2 até criar duas instâncias:
    - Uma instância do bastion host em sua sub-rede pública
    - Uma instância em sua sub-rede privada que deve ser usada como Controlador de Domínio.

Tarefa 4: Criar um conjunto de opções de DHCP

1. No VPC Dashboard, selecione **DHCP Options Sets**.
2. Insira as seguintes informações:

- Name tag: insira um nome amigável para o conjunto.
- Domain name: insira o nome de domínio totalmente qualificado que você usa ao configurar a instância do Controlador de Domínio.
- Domain name servers: insira o endereço IP privado que você atribuiu à instância do Controlador de Domínio e a cadeia de caracteres **AmazonProvidedDNS**, separados por vírgula.
- NTP servers: deixe este campo em branco.
- NetBIOS name servers: insira o endereço IP privado da instância do Controlador de Domínio.
- NetBIOS node type: insira **2**.

3. Selecione **Yes, Create.**
4. Associe o novo conjunto à sua VPC:

   a) No VPC Dashboard, selecione **Your VPCs** e, em seguida, selecione a VPC que você configurou anteriormente.
   b) Selecione **Actions > Edit DHCP Options Set**.
   c) Quando solicitado, selecione o novo conjunto que você criou e, em seguida, selecione **Save**.

Tarefa 5: Configurar as instâncias

1. Usando um cliente RDP, conecte-se ao endereço IP público da instância do host bastion. Quando solicitado, insira as credenciais para a conta de administrador.
2. Na instância do host bastion, inicie a Conexão de Área de Trabalho Remota e conecte-se ao endereço IP privado da instância que deseja configurar. Quando solicitado, insira as credenciais de administrador para a instância.
3. Para todas as instâncias na sub-rede privada, defina as configurações de DNS:

   a) Selecione **Iniciar > Painel de controle > Rede e Internet > Central de Rede e Compartilhamento > Alterar as configurações do adaptador**. Clique duas vezes na conexão de rede exibida.
   b) Selecione **Propriedades > Protocolo de Internet versão 4 (TCP/IPv4) > Propriedades**.
   c) Selecione **Avançado > DNS**. Certifique-se de que as seguintes configurações estejam ativadas e selecione **OK**:

      - Registre os endereços desta conexão no DNS
      - Use o sufixo DNS desta conexão no registro de DNS

4. Para configurar o Controlador de Domínio:

a) Usando o Server Manager, adicione a função Active Directory Domain Services com todos os recursos padrão.
b) Promova a instância a um Controlador de Domínio. Durante a promoção, habilite o DNS e use o nome de domínio especificado ao criar o conjunto de opções de DHCP. Reinicie a instância quando solicitado.

Criar uma conexão

Quando você cria 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 chaves que contém esses valores da AWS e depois importá-los. Você também deve fornecer a região, a zona de disponibilidade, o nome da VPC, os endereços de sub-rede, o nome do domínio, o nome dos grupos de segurança e as credenciais.
- O arquivo de credenciais para a conta raiz da AWS (recuperado do console da AWS) não está formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão da AWS. Portanto, o gerenciamento do Citrix Virtual Apps and Desktops não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Verifique se você está usando os arquivos de credenciais do AWS Identity Access Management (IAM).

> **Nota:**
>
> Depois de criar uma conexão, as tentativas de atualizar a chave de API e a chave secreta podem falhar. Para resolver o problema, verifique as restrições do seu servidor proxy ou do firewall e confirme que o seguinte endereço pode ser contatado: `https://*.amazonaws.com`.

Valores padrão de conexão do host

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

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

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

URL do ponto de extremidade de serviço

URL do ponto de extremidade do serviço de zona padrão

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

Locação da AWS

A AWS oferece as seguintes opções de locação: locação compartilhada (o tipo padrão) e locação dedicada. Locação compartilhada significa que várias instâncias do Amazon EC2 de clientes diferentes podem residir no mesmo equipamento de hardware físico. Locação dedicada significa que suas instâncias do EC2 são executadas somente no hardware com as outras instâncias que você implantou. Outros clientes não usam o mesmo equipamento de hardware.

Você pode usar o MCS para provisionar hosts dedicados da AWS usando o PowerShell.

Configurar a locação de host dedicada da AWS usando o PowerShell

Você pode criar um catálogo de máquinas com a locação de host definida por meio do PowerShell.

Um host dedicado [EC2] da Amazon é um servidor físico com capacidade de instância [EC2] totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM.

Os hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado dos tipos de instância C4 Large é limitado à execução de 16 instâncias. Consulte o site da AWS para obter mais informações.

Os requisitos de provisionamento para os hosts da AWS incluem:

- Uma imagem (AMI) importada da BYOL (traga sua própria licença). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para atender às solicitações de provisionamento.
- Ativar o **posicionamento automático**.

Para provisionar a um host dedicado na AWS usando o PowerShell, use o cmdlet **New-ProvScheme** com o parâmetro TenancyType definido como *Host*.

Consulte a Documentação do Citrix Developer para obter mais informações.

Captura de propriedade de instâncias da AWS

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, você seleciona uma AMI para representar a imagem mestre/de ouro do catálogo. A partir dessa AMI, o MCS usa um instantâneo do disco. Em versões anteriores, se você quisesse funções ou marcações em suas máquinas, usaria o console da AWS para defini-las individualmente. Essa funcionalidade é ativada por padrão.

> **Dica:**
>
> Para usar a captura de propriedade da instância da AWS, você deve ter uma VM associada à AMI.

Para melhorar esse processo, o **MCS lê** as propriedades da instância a partir da qual a AMI foi obtida e aplica a função de Identity Access Management (IAM) e as marcas da máquina às máquinas provisionadas de um determinado catálogo. Ao usar esse recurso opcional, o processo de criação do catálogo localiza a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são armazenadas em um Launch Template da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturada.

As propriedades capturadas incluem:

- Funções de IAM –aplicadas a instâncias provisionadas.
- Marcações –aplicadas a instâncias provisionadas, seus discos e NICs. Essas marcações são aplicadas a recursos temporários da Citrix, incluindo: objetos e bucket S3, recursos de volume e worker, e AMIs, instantâneos e modelos de execução.

> **Dica:**
>
> A marcação de recursos temporários da Citrix é opcional e pode ser configurada usando a propriedade personalizada `AwsOperationalResourcesTagging`.

Captura da propriedade da instância da AWS

Você pode usar este recurso especificando uma propriedade personalizada, `AwsCaptureInstanceProperti`, ao criar um esquema de provisionamento para uma conexão de hospedagem da AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```


Consulte a Documentação do Citrix Developer para obter mais informações.

Aplicação de propriedades de instâncias da AWS e marcação de recursos operacionais

Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode controlar se as propriedades de função e marcação com tag do IAM devem ser aplicadas a essas máquinas. Você também pode controlar se as marcas de máquina devem ser aplicadas aos recursos operacionais.

Marcação de recursos operacionais da AWS

Uma Amazon Machine Image (AMI) representa um tipo de dispositivo virtual usado para criar uma máquina virtual dentro do ambiente de nuvem Amazon Cloud, comumente chamado de EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Quando cria um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem de ouro do catálogo.

> **Importante:**
>
> A criação de catálogos por meio da captura de uma propriedade de instância e um modelo de execução é necessária para usar a marcação de recursos operacionais.

Para criar um catálogo da AWS, você deve primeiro criar uma AMI para a instância que você quer que seja a imagem de ouro. O MCS lê as marcas dessa instância e as incorpora ao modelo de execução. As marcas do modelo de execução são então aplicadas a todos os recursos da Citrix criados no seu ambiente da AWS, incluindo:

- Máquinas virtuais
- Discos VM
- Interfaces de rede VM
- Buckets do S3
- Objetos do S3
- Modelos de execução
- AMIs

Marcação de um recurso operacional

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell no host DDC.
2. Execute o comando `asnp citrix` para carregar módulos PowerShell específicos da Citrix.

Para marcar um recurso para uma VM provisionada, use a nova propriedade personalizada `AwsOperationalResourcesTagging`. A sintaxe dessa propriedade é:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"...<standard provscheme parameters
>
```

Definição de permissões do IAM

Use as informações nesta seção para definir as permissões do IAM para o Citrix DaaS na AWS. O serviço IAM da Amazon permite contas com vários usuários, que podem ser organizados em grupos. Os usuários podem ter permissões diferentes para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões do IAM, consulte Referência de política JSON do IAM.

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

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

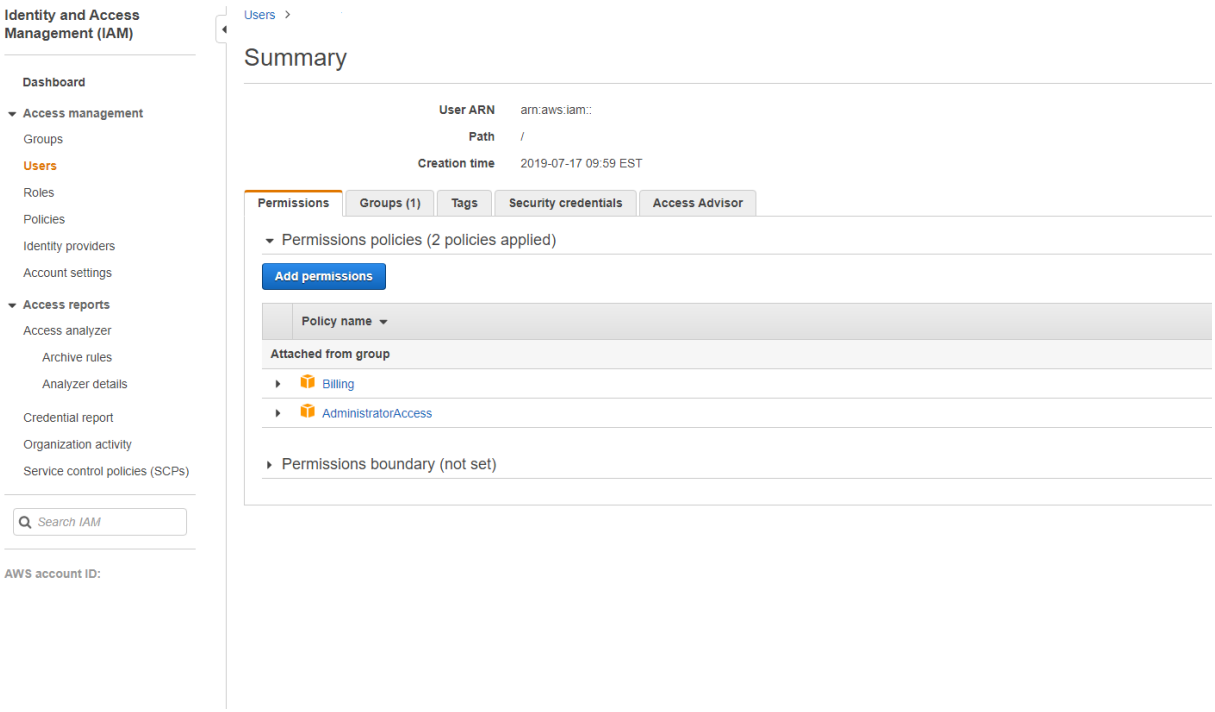
Depois de inserir as informações da política, selecione **Continue** para concluir o grupo de usuários. Os usuários do grupo recebem permissões para executar somente as ações necessárias para o Citrix DaaS.

> **Importante:**
>
> Use o texto de política fornecido no exemplo acima para listar as ações que um Citrix DaaS usa para executar ações em uma conta da AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar mais restrições aos recursos.

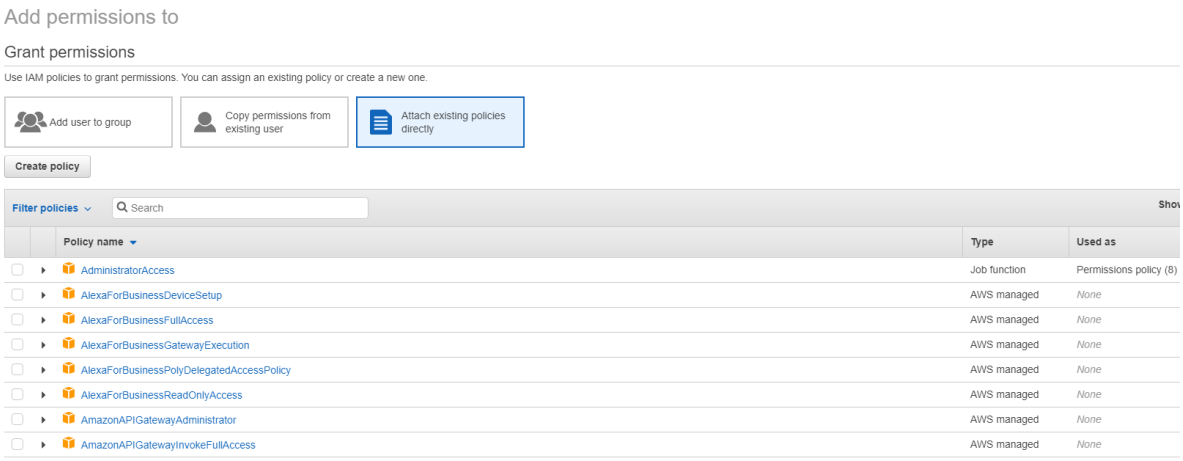
Adicionar permissões do IAM

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

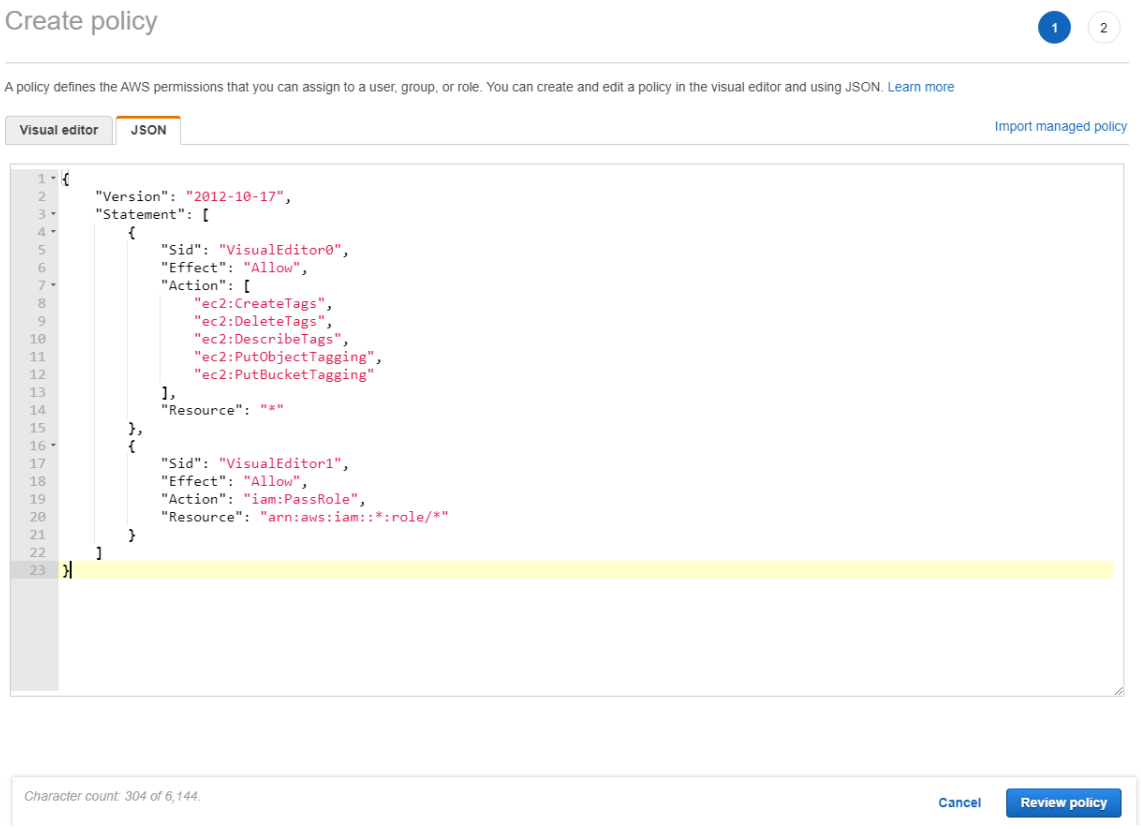
1. No painel **Summary**, selecione a guia **Permissions**.
2. Selecione **Add permissions.**



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



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



> **Dica:**
>
> O exemplo de JSON observado talvez não inclua todas as permissões para o seu ambiente. Consulte How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS para obter mais informações.

Sobre as permissões da AWS

Esta seção contém a lista completa de permissões da AWS.

> **Nota:**
>
> A permissão *iam:PassRole* é necessária somente para **role_based_auth**.

Criar uma conexão de host

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

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
22
23  <!--NeedCopy-->
```

Gerenciamento de energia de VMs

As instâncias de máquina estão ligadas ou desligadas.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22  }
23
24  <!--NeedCopy-->
```


Criar, atualizar ou excluir VMs

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

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2: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": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> **Nota:**
>
> A seção do EC2 relacionada a SecurityGroups só será necessária se um grupo de segurança de isolamento precisar ser criado para a VM de preparação durante a criação do catálogo. Feito isso, essas permissões não serão necessárias.

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

As seguintes permissões devem ser adicionadas à política:

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

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

Criptografia do EBS dos volumes criados

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

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }
```



```
18
19      ]
20   }
21
22  <!--NeedCopy-->
```

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

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": [
9                   "kms:CreateGrant",
10                  "kms:Decrypt",
11                  "kms:DescribeKey",
12                  "kms:GenerateDataKeyWithoutPlainText",
13                  "kms:ReEncryptTo",
14                  "kms:ReEncryptFrom"
15             ],
16             "Resource": [
17                 "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                      -456d-a12b-a123b4cd56ef"
18             ],
19             "Condition": {
20
21                 "Bool": {
22
23                     "kms:GrantIsForAWSResource": true
24                  }
25
26              }
27
28          }
29
30      ]
31   }
32
33  <!--NeedCopy-->
```

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

```
1  {
2
```



```
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

Para obter mais informações, consulte a documentação oficial do AWS Key Management Service.

Autenticação baseada na função do IAM

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

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```

Política de permissões mínimas do IAM

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

> **Importante:**
>
> Para usar **role_based_auth**, primeiro configure a função do IAM desejada em todos os Delivery

> Controllers em nosso site. Usando o Web Studio, adicione a conexão de hospedagem e forneça o role_based_auth para a chave de autenticação e o segredo. Uma conexão de hospedagem com essas configurações usa a autenticação baseada em função.

```
{

    "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:GenerateDataKey",
                    "kms:ReEncryptTo",
                    "kms:ReEncryptFrom"
                ],
                "Resource": "*"
            }
    ,
           {

                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::*:role/*"
            }

        ]
    }

<!--NeedCopy-->
```

Nota:

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

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes do Google Cloud

April 3, 2024

O Citrix Virtual Apps and Desktops permite provisionar e gerenciar máquinas no Google Cloud. Este artigo orienta você no uso do Machine Creation Services (MCS) para provisionar máquinas virtuais na

implantação do serviço Citrix Virtual Apps ou Citrix Virtual Desktops.

Requisitos

- Conta do Citrix Cloud. O recurso descrito neste artigo está disponível somente no Citrix Cloud.
- Assinatura do Citrix DaaS. Para obter detalhes, consulte Introdução.
- Um projeto do Google Cloud. O projeto armazena todos os recursos de computação associados ao catálogo de máquinas. Pode ser um projeto existente ou um projeto novo.
- Habilite quatro APIs no seu projeto do Google Cloud. Para obter detalhes, consulte Habilitar as APIs do Google Cloud.
- Conta de serviço do Google Cloud. A conta de serviço é autenticada no Google Cloud para permitir o acesso ao projeto. Para obter detalhes, consulte Configurar e atualizar contas de serviço.
- Ative o acesso privado do Google. Para obter detalhes, consulte Ativar o acesso privado do Google.

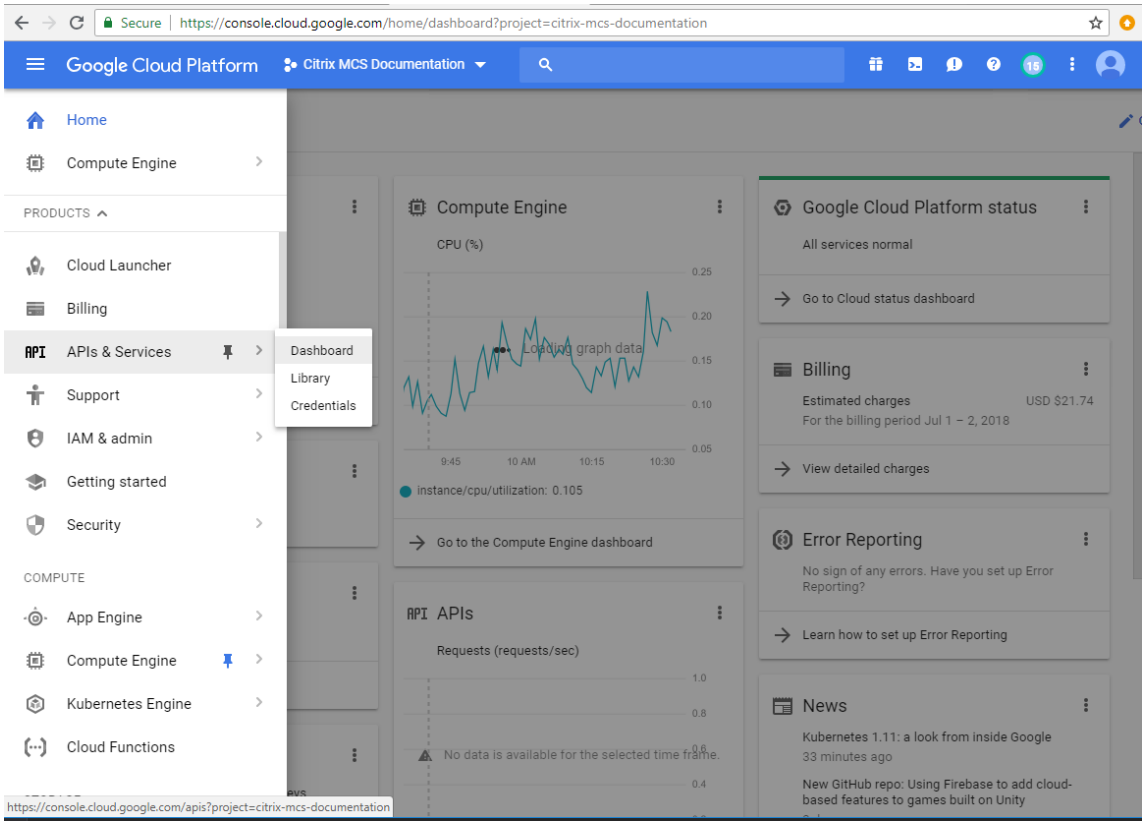
Habilitar as APIs do Google Cloud

Para usar a funcionalidade do Google Cloud por meio da interface Full Configuration do Citrix Virtual Apps and Desktops, ative estas APIs no seu projeto do Google Cloud:

- API do Compute Engine
- API do Cloud Resource Manager
- API do Identity and Access Management (IAM)
- API do Cloud Build
- Cloud Key Management Service (KMS)

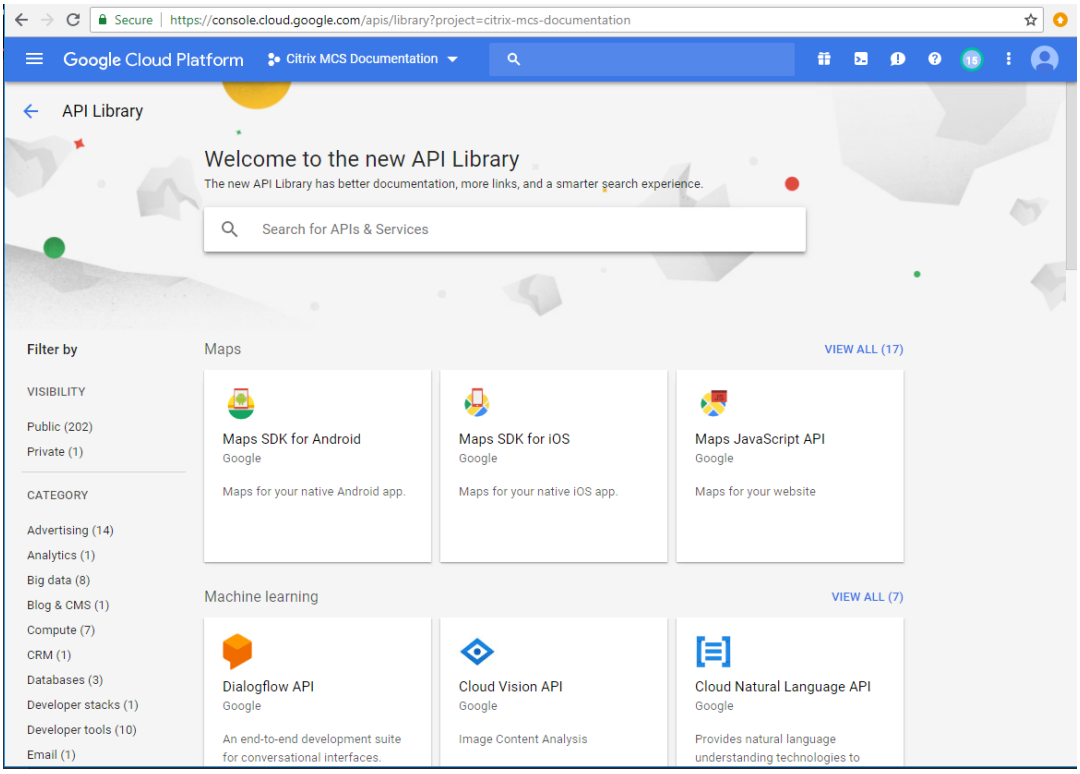
No console do Google Cloud, conclua estas etapas:

1. No menu superior esquerdo, selecione **APIs and Services > Dashboard**.



2. Na tela **Dashboard**, confirme que a API de Compute Engine está ativada. Caso contrário, siga estes passos:

    a) Navegue para **APIs and Services > Library**.



b) Na caixa de pesquisa, digite *Compute Engine*.

c) Nos resultados da pesquisa, selecione **Compute Engine API**.

d) Na página **Compute Engine API**, selecione **Enable**.

3. Ative a API do Cloud Resource Manager.

a) Navegue para **APIs and Services > Library**.

b) Na caixa de pesquisa, digite *Cloud Resource Manager*.

c) Nos resultados da pesquisa, selecione **Cloud Resource Manager API**.

d) Na página **Cloud Resource Manager API**, selecione **Enable**. O status da API é exibido.

4. Da mesma forma, ative **Identity and Access Management (IAM) API** e **Cloud Build API**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para isso:

1. Abra o Google Console e carregue o Cloud Shell.
2. Execute os quatro comandos a seguir no Cloud Shell:

- gcloud services enable compute.googleapis.com
- gcloud services enable cloudresourcemanager.googleapis.com
- gcloud services enable iam.googleapis.com
- gcloud services enable cloudbuild.googleapis.com

3. Clique em **Authorize** se o Cloud Shell solicitar.

Configurar e atualizar contas de serviço

O Citrix Cloud usa três contas de serviço separadas no projeto do Google Cloud:

- *Conta de serviço do Citrix Cloud*: essa conta de serviço permite que o Citrix Cloud acesse o projeto do Google, provisione e gerencie máquinas. A conta do Google Cloud é autenticada no Citrix Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar essa conta de serviço manualmente.

  Você pode identificar essa conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

  Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a essa conta de serviço:

  - Compute Admin
  - Storage Admin
  - Cloud Build Editor
  - Service Account User
  - Cloud Datastore User

- *Conta de serviço Cloud Build*: essa conta de serviço é provisionada automaticamente depois que você ativa todas as APIs mencionadas em Habilitar as APIs do Google Cloud.

  Você pode identificar essa conta de serviço pelo endereço de e-mail que começa com **ID do projeto** e a palavra **cloudbuild**. Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

  Conceda as seguintes funções a essa conta de serviço:

  - Cloud Build Service Account
  - Compute Instance Admin
  - Service Account User

- *Conta de serviço do Cloud Compute*: essa conta de serviço é adicionada pelo Google Cloud às instâncias criadas no Google Cloud quando a API do Compute é ativada. Essa conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar a função **Storage Admin** que exige as seguintes permissões:

  - resourcemanager.projects.get
  - storage.objects.create

- storage.objects.get
- storage.objects.list

Você pode identificar essa conta de serviço pelo endereço de e-mail que começa com ID do projeto e a palavra compute. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`.

Criar uma conta de serviço do Citrix Cloud

Para criar uma conta de serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegue para **IAM & Admin > Service accounts**.
2. Na página **Service accounts**, selecione **CREATE SERVICE ACCOUNT**.
3. Na página **Create service account**, insira as informações necessárias e selecione **CREATE AND CONTINUE**.
4. Na página **Grant this service account access to project**, clique no menu suspenso **Select a role** e selecione as funções necessárias. Clique em **+ADD ANOTHER ROLE** se quiser adicionar mais funções.

   > **Nota:**
   >
   > Ative todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUE**.
6. Na página **Grant users access to this service account**, adicione usuários ou grupos para conceder acesso para realizarem ações na conta de serviço.
7. Clique em **DONE**.
8. Navegue até o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Confirme que as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Grant this service account access to project** e **Grant users access to this service account** são opcionais. Se você optar por ignorar essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM & Admin > IAM**.

- Para exibir funções associadas a uma conta de serviço, adicione as funções sem ignorar as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

Chave da conta de serviço do Citrix Cloud Ao criar uma conta de serviço, existe a opção de criar uma chave para a conta. Você precisa dessa chave ao criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credencial (.json). O arquivo é baixado automaticamente e salvo na pasta **Downloads** depois que você cria a chave. Ao criar a chave, certifique-se de definir o tipo de chave como JSON. Caso contrário, a interface Full Configuration do Citrix não pode analisá-la.

> **Dica:**
>
> Crie chaves usando a página **Service accounts** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

Adicionar funções à conta de serviço do Citrix Cloud

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegue para **IAM & Admin > IAM**.
2. Na página **IAM > PERMISSIONS**, localize a conta de serviço que você criou, identificável pelo endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso à entidade de segurança da conta de serviço.
4. Na página **Edit access to "project-id"** da opção de entidade de segurança selecionada, selecione **ADD ANOTHER ROLE** para adicionar as funções necessárias à sua conta de serviço, uma por uma, e selecione **SAVE**.

Adicionar funções à conta de serviço do Cloud Build

Para adicionar funções à conta de serviço do Cloud Build:

1. No console do Google Cloud, navegue para **IAM & Admin > IAM**.
2. Na página do **IAM**, localize a conta de serviço do Cloud Build, identificável pelo endereço de e-mail que começa com **ID do projeto** e a palavra **cloudbuild**.

   Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Edit access to "project-id"** da opção de entidade de segurança selecionada, selecione **ADD ANOTHER ROLE** para adicionar as funções necessárias à sua conta de serviço Cloud Build, uma por uma, e selecione **SAVE**.

   > **Nota:**
   >
   > Habilite todas as APIs para obter a lista completa de funções.

Gerenciamento do bucket e permissões de armazenamento

O Citrix DaaS melhora o processo de relatar falhas de compilação na nuvem do serviço Google Cloud. Esse serviço executa compilações no Google Cloud. O Citrix DaaS cria um intervalo de armazenamento chamado `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` onde os serviços do Google Cloud capturam informações de registro de compilação. Uma opção é definida nesse bucket que exclui o conteúdo após um período de 30 dias. Esse processo exige que a conta de serviço usada para a conexão tenha as permissões do Google Cloud definidas como `storage.buckets.update`. Se a conta de serviço não tiver essa permissão, o Citrix DaaS ignorará os erros e prosseguirá com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de compilação aumenta e exigem limpeza manual.

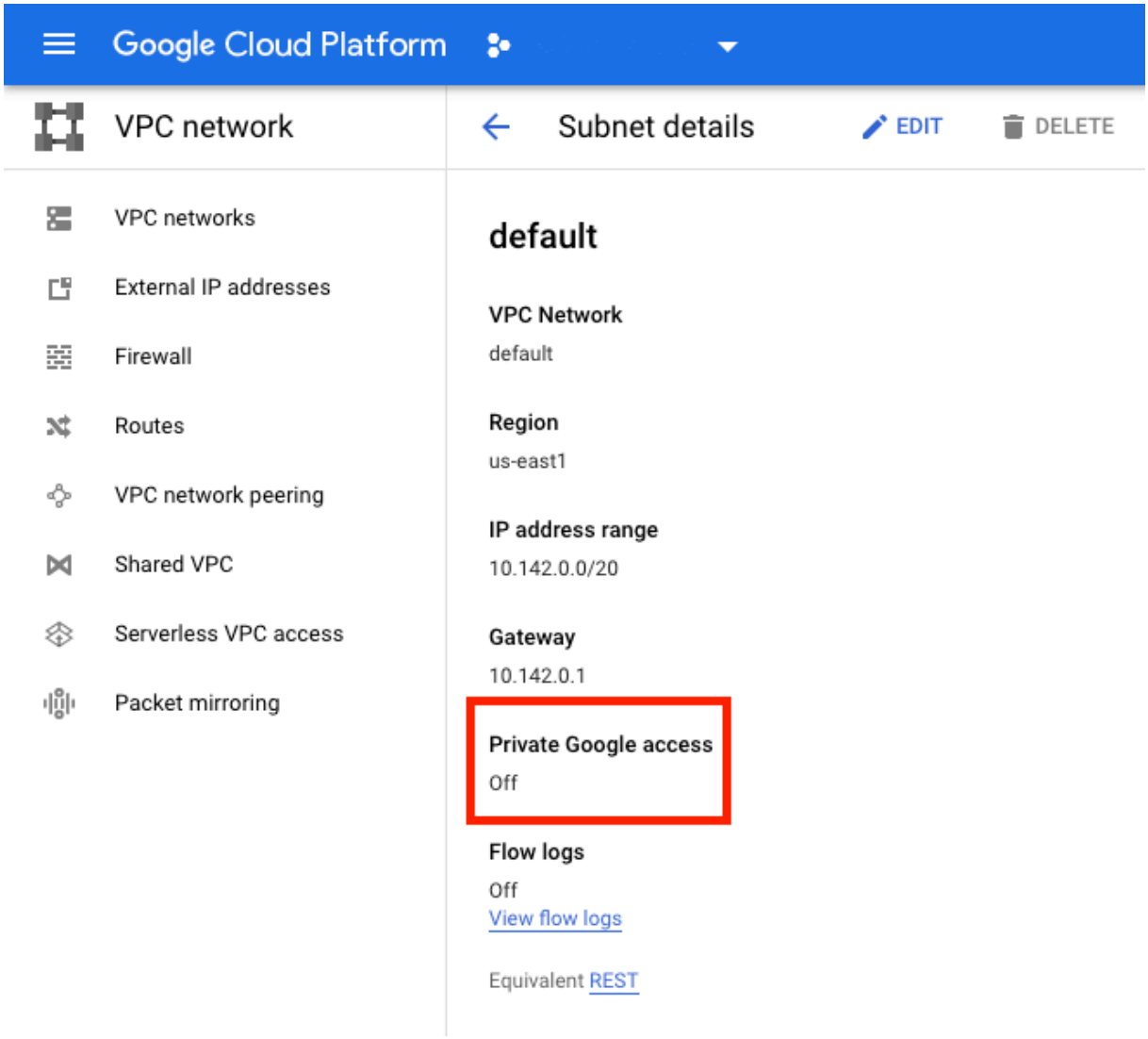
Ativar o acesso privado do Google

Quando uma VM não tem um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Quando você ativa o acesso privado, a VM se conecta ao conjunto de endereços IP externos usados pela API do Google e serviços associados.

> **Nota:**
>
> Independentemente de o acesso privado do Google estar ativado, todas as VMs com e sem endereços IP públicos devem ser capazes de acessar as APIs públicas do Google, especialmente se dispositivos de rede de terceiros tiverem sido instalados no ambiente.

Para garantir que uma VM na sua sub-rede possa acessar as APIs do Google sem um endereço IP público para provisionamento do MCS:

1. No Google Cloud, acesse a **configuração da rede VPC**.
2. Na tela Subnet details, ative **Private Google access**.



Para obter mais informações, consulte Como configurar o acesso privado do Google.

> **Importante:**
>
> Se a sua rede está configurada para impedir o acesso da VM à Internet, certifique-se de que a sua organização assuma os riscos associados à ativação do acesso privado do Google para a sub-rede à qual a VM está conectada.

Adicionar uma conexão

Siga as orientações em Criar uma conexão e recursos. A descrição a seguir orienta você para configurar uma conexão de hospedagem:

1. Em **Manage > Configuration**, selecione **Hosting** no painel esquerdo.
2. Selecione **Add Connection and Resources** na barra de ações.

3. Na página **Connection**, selecione **Create a new Connection** e **Citrix provisioning tools**, depois selecione **Next**.

    - **Connection type**. Selecione **Google Cloud** no menu.
    - **Connection name**. Digite um nome para a conexão.

4. Na página **Region**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Next**.

5. Na página **Network**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Next**. O nome do recurso ajuda a identificar a combinação de região e rede. As redes virtuais com o sufixo *(Shared)* anexado ao nome representam VPCs compartilhadas. Se você configurar uma função do IAM no nível da sub-rede para uma VPC compartilhada, somente sub-redes específicas da VPC compartilhada aparecem na lista de sub-redes.

    > **Nota:**
    >
    > - O nome do recurso pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )'`).

6. Na página **Summary**, confirme as informações e selecione **Finish** para sair da janela **Add Connection and Resources**.

Depois de criar a conexão e os recursos, a conexão e os recursos que você criou são listados. Para configurar a conexão, selecione a conexão e, em seguida, selecione a opção aplicável na barra de ações.

Da mesma forma, você pode excluir, renomear ou testar os recursos criados na conexão. Para fazer isso, selecione o recurso na conexão e, em seguida, selecione a opção aplicável na barra de ações.

Preparar uma instância de VM mestre e um disco permanente

> **Dica:**
>
> Disco permanente é o termo do Google Cloud para disco virtual.

Para preparar a sua instância de VM mestre, crie e configure uma instância de VM com propriedades que correspondam à configuração desejada para as instâncias do VDA clonadas no seu catálogo de máquinas planejado. A configuração não se aplica somente ao tamanho e ao tipo da instância. Também inclui atributos de instância, como metadados, tags, atribuições de GPU, marcas de rede e propriedades da conta de serviço.

Como parte do processo, o MCS usa sua instância de VM mestre para criar o *modelo de instância* do Google Cloud. O modelo de instância é então usado para criar as instâncias do VDA clonadas que compõem o catálogo de máquinas. As instâncias clonadas herdam as propriedades (exceto as propriedades de VPC, sub-rede e disco permanente) da instância de VM mestre a partir da qual o modelo de instância foi criado.

Depois de configurar as propriedades da instância de VM mestre de acordo com suas especificações, inicie a instância e prepare o disco permanente para a instância.

Recomendamos que você crie manualmente um instantâneo do disco. Isso permite que você use uma convenção de nomenclatura significativa para controlar as versões, oferece mais opções para gerenciar versões anteriores da sua imagem mestre e economiza tempo na criação do catálogo de máquinas. Se você não criar o seu próprio instantâneo, o MCS cria um instantâneo temporário para você (que é apagado no final do processo de provisionamento).

Criar um catálogo de máquinas

> **Nota:**
>
> Crie os seus recursos antes de criar um catálogo de máquinas. Use as convenções de nomenclatura estabelecidas pelo Google Cloud ao configurar catálogos de máquinas. Consulte Diretrizes de nomenclatura de bucket e objeto para obter mais informações.

Siga as orientações em Criar catálogos de máquinas. A descrição a seguir é exclusiva para os catálogos do Google Cloud.

1. Entre no Web Studio e selecione **Machine Catalogs** no painel esquerdo.
2. Selecione **Create Machine Catalog** na barra de ações.
3. Na página **Operating System**, selecione **Multi-session OS** e depois selecione **Next**.
    - O Citrix Virtual Apps and Desktops também oferece suporte ao SO de sessão única.
4. Na página **Machine Management**, selecione as opções **Machines that are power managed** e **Citrix Machine Creation Services** e selecione **Next**. Se houver vários recursos, selecione um no menu.
5. Na página **Master Image**, selecione uma VM e o nível funcional mínimo para o catálogo e, em seguida, selecione **Next**. Se você quiser usar a funcionalidade de locação única, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente. Consulte Habilitar a seleção de zona.
6. Na página **Storage Types**, selecione o tipo de armazenamento usado para conter o sistema operacional desse catálogo de máquinas. Cada uma das opções de armazenamento a seguir

tem características únicas de preço e desempenho. (Um disco de identidade é sempre criado usando o disco permanente padrão por zona.)

- Disco permanente padrão
- Disco permanente balanceado
- Disco permanente SSD

Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte https://cloud.google.com/compute/docs/disks/.

7. Na página **Virtual Machines**, especifique quantas VMs você deseja criar, confira a especificação detalhada das VMs e selecione **Next**. Se você usar grupos de nós de locatário único para catálogos de máquinas, certifique-se de selecionar **apenas** as zonas em que os nós de locatário único reservados estão disponíveis. Consulte Habilitar a seleção de zona.
8. Na página **Computer Accounts**, selecione uma conta do Active Directory e, em seguida, selecione **Next**.
   - Se você selecionar **Create new Active Directory accounts**, selecione um domínio e insira a sequência de caracteres que representa o esquema de nomenclatura para as contas de computador de VMs provisionadas criadas no Active Directory. O esquema de nomenclatura de conta pode conter de 1 a 64 caracteres e não pode conter espaços em branco ou caracteres não ASCII ou especiais.
   - Se você selecionar **Use existing Active Directory accounts**, selecione **Browse** para navegar até as contas de computador existentes do Active Directory para as máquinas selecionadas.
9. Na página **Domain Credentials**, selecione **Enter credentials**, digite o nome de usuário e a senha, selecione **Save** e selecione **Next**.
   - A credencial digitada deve ter permissões para realizar operações na conta do Active Directory.
10. Na página **Summary**, confirme as informações, especifique um nome para o catálogo e selecione **Finish**.

    > **Nota:**
    >
    > O nome do catálogo pode conter de 1 a 39 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

A criação do catálogo de máquinas pode levar muito tempo para ser concluída. Para verificar se as máquinas foram criadas nos grupos de nós de destino, vá para o console do Google Cloud.

Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS), você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Quando o parâmetro `MachineProfile` não é usado, as propriedades do hardware são capturadas da VM da imagem mestre ou do instantâneo. Algumas propriedades que você define explicitamente, por exemplo, `StorageType`, `CatalogZones` e `CryptoKeyIs`, são ignoradas do perfil da máquina.

- Para criar um catálogo com um perfil de máquina, use o comando `New-ProvScheme`. Por exemplo, `New-ProvScheme –MachineProfile "path to VM"`. Se você não especificar o parâmetro `MachineProfile`, as propriedades de hardware serão capturadas da VM da imagem mestre.
- Para atualizar um catálogo com um novo perfil de máquina, use o comando `Set-ProvScheme`. Por exemplo, `Set-ProvScheme –MachineProfile "path to new VM"`. Esse comando não altera o perfil da máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo têm o novo perfil de máquina.
- Você também pode atualizar a imagem mestre; no entanto, quando você atualiza a imagem mestre, as propriedades do hardware não são atualizadas. Se você quiser atualizar as propriedades de hardware, você deve atualizar o perfil da máquina usando o comando `Set-ProvScheme`. Essas alterações só se aplicarão às novas máquinas no catálogo. Para atualizar as propriedades de hardware de uma máquina existente, você pode usar o comando `Request-ProvVMUpdate`.

Criar um novo catálogo de máquinas com perfil de máquina como modelo de instância

Você pode selecionar um modelo de instância do GCP como uma entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP, portanto, são muito econômicos.

Para criar um novo catálogo de máquinas com perfil de máquina como um modelo de instância usando comandos do PowerShell:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Encontre um modelo de instância em seu projeto do GCP usando o seguinte comando:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Crie um novo catálogo de máquinas com perfil de máquina como modelo de instância usando o comando NewProvScheme:


```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

Para obter mais informações sobre o comando New-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Conclua a criação do catálogo de máquinas usando os comandos do PowerShell. Para obter informações sobre como criar um catálogo usando o Remote PowerShell SDK, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Para alterar o perfil da máquina de um catálogo de máquinas existente para ser um modelo de instância:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

Para obter informações sobre o comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

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 das máquinas do Google Cloud. Use o nó **Search** no painel esquerdo para localizar a máquina cuja energia você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Delete

- Start
- Restart
- Force Restart
- Shut Down
- Force Shutdown
- Add to Delivery Group
- Manage Tags
- Turn On Maintenance Mode

Você também pode gerenciar as máquinas do Google Cloud usando Autoscale. Para isso, adicione as máquinas do Google Cloud a um grupo de entrega e ative Autoscale para o grupo de entrega. Para obter mais informações sobre Autoscale, consulte Autoscale.

Atualizar máquinas provisionadas usando o PowerShell

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, isso não afeta as máquinas existentes. Usando o comando `Request-ProvVMUpdate` dos comandos do PowerShell, agora você pode aplicar o esquema de provisionamento atual a uma máquina persistente ou não persistente existente ou a um conjunto de máquinas. Atualmente, no GCP, a atualização de propriedade suportada por esse recurso é o perfil da máquina.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento

Para atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Atualize o esquema de provisionamento. Por exemplo,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
<!--NeedCopy-->
```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,


```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Atualize as máquinas existentes.

   - Para atualizar todas as máquinas existentes:

     ```
     Request-ProvVMUpdate  – ProvisioningSchemeName "my-catalog"
     <!--NeedCopy-->
     ```

   - Para atualizar uma lista de máquinas específicas:

     ```
     Request-ProvVMUpdate -ProvisioningSchemeName "my-catalog" -
         VMName "vm1","vm2"
     <!--NeedCopy-->
     ```

   - Para atualizar máquinas com base na saída de `Get-ProvVM`:

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Request-
         ProvVMUpdate
     <!--NeedCopy-->
     ```

5. Encontre máquinas com uma atualização agendada. Por exemplo,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
       , ProvisioningSchemeUpdateAfter
   <!--NeedCopy-->
   ```

6. Reinicialize as máquinas. Na próxima vez que forem ligadas, as alterações às propriedades serão aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando:

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

Proteger a exclusão acidental da máquina

O Citrix DaaS permite proteger os recursos do MCS no Google Cloud para evitar exclusão acidental. Configure a VM provisionada definindo o sinalizador `deletionProtection` como TRUE.

Por padrão, as VMs provisionadas por meio do plug-in do Google Cloud ou MCS são criadas com o InstanceProtection ativado. A implementação é aplicável a catálogos persistentes e não persistentes. Os catálogos não persistentes são atualizados quando as instâncias são recriadas a partir do modelo. Para máquinas persistentes existentes, você pode definir o sinalizador no console do Google Cloud. Para obter mais informações sobre como definir o sinalizador, consulte o site de documentação do Google. Novas máquinas adicionadas a catálogos persistentes são criadas com `deletionProtection` habilitado.

Se você tentar excluir uma instância de VM para a qual definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você receber a permissão `compute.instances.setDeletionProtection` ou a atribuição da função **Compute Admin** do IAM, poderá redefinir o sinalizador para permitir que o recurso seja excluído.

Importar máquinas do Google Cloud criadas manualmente

Você pode *criar uma conexão com o Google Cloud* e a seguir *criar um catálogo contendo máquinas do Google Cloud*. Em seguida, você pode ligar e desligar manualmente as máquinas do Google Cloud por meio do Citrix DaaS. Com esse recurso, você pode:

- Importar máquinas com SO multissessão do Google Cloud criadas manualmente para um catálogo de máquinas do Citrix Virtual Apps and Desktops.
- Remover as máquinas com SO multissessão do Google Cloud criadas manualmente de um catálogo do Citrix Virtual Apps and Desktops.
- Usar os recursos existentes de gerenciamento de energia do Citrix Virtual Apps and Desktops para gerenciar a energia das máquinas com SO multissessão Windows do Google Cloud. Por exemplo, defina um agendamento de reinicialização para essas máquinas.

Essa funcionalidade não requer alterações no fluxo de trabalho de provisionamento existente do Citrix Virtual Apps and Desktops nem a remoção de qualquer recurso existente. Recomendamos que você use o MCS para provisionar máquinas na interface Full Configuration do Citrix DaaS, em vez de importar máquinas do Google Cloud criadas manualmente.

Nuvem privada virtual compartilhada

Nuvens privadas virtuais compartilhadas (VPCs) compreendem um projeto host, a partir do qual as sub-redes compartilhadas são disponibilizadas, e um ou mais projetos de serviço que usam o recurso. As VPCs compartilhadas são boas opções para instalações maiores porque fornecem controle, uso e administração centralizados dos recursos corporativos compartilhados do Google Cloud. Para obter mais informações, consulte o site de documentação do Google.

Com esse recurso, o MCS (Machine Creation Services) oferece suporte ao provisionamento e ao gerenciamento de catálogos de máquinas implantados em VPCs compartilhadas. Esse suporte, que é funcionalmente equivalente ao suporte fornecido atualmente nas VPCs locais, difere em duas áreas:

1. Você deve conceder permissões extras para a conta de serviço usada para criar a conexão de host. Esse processo permite que o MCS acesse e use os recursos da VPC compartilhada.
2. Você deve criar duas regras de firewall, uma para entrada e outra para saída. Essas regras de firewall são usadas durante o processo de masterização de imagens.

Novas permissões necessárias

É necessária uma conta de serviço do Google Cloud com permissões específicas ao criar a conexão do host. Essas permissões adicionais devem ser concedidas a todas as contas de serviço usadas para criar conexões de host baseadas em VPC compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas no Citrix DaaS. Elas são usadas para facilitar a implementação de VPCs locais. Com as VPCs compartilhadas, essas permissões adicionais permitem o acesso a outros recursos de VPC compartilhadas.

No máximo quatro permissões extras devem ser concedidas à conta de serviço associada à conexão de host para aceitar à VPC compartilhada:

1. **compute.firewalls.list** –Essa permissão é obrigatória. Permite que o MCS recupere a lista de regras de firewall presentes na VPC compartilhada.
2. **compute.networks.list** –Essa permissão é obrigatória. Permite que o MCS identifique as redes VPC compartilhadas disponíveis para a conta de serviço.
3. **compute.subnetworks.list** –Essa permissão é opcional, dependendo de como você usa as VPCs. Permite que o MCS identifique as sub-redes nas VPCs compartilhadas visíveis. Essa permissão já é necessária ao usar VPCs locais, mas também deve ser atribuída no projeto host da VPC compartilhada.
4. **compute.subnetworks.use** –Essa permissão é opcional, dependendo de como você usa as VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionadas. Essa permissão já é necessária para usar VPCs locais, mas também deve ser atribuída no projeto host da VPC compartilhada.

Ao usar essas permissões, considere que existem abordagens diferentes com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão no nível do projeto:
  - Permite o acesso a todas as VPCs compartilhadas dentro do projeto host.

  - Requer que as permissões 3 e 4 sejam atribuídas à conta de serviço.

- Permissão no nível da sub-rede:
  - Permite o acesso a sub-redes específicas dentro da VPC compartilhada.
  - As permissões 3 e 4 são intrínsecas à atribuição de nível de sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que corresponde às suas necessidades organizacionais e aos padrões de segurança.

> **Dica:**
>
> Para obter mais informações sobre as diferenças entre as permissões no nível do projeto e no nível da sub-rede, consulte a documentação do Google Cloud.

Regras de firewall

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como o disco do sistema de imagem mestre para o catálogo. Quando esse processo ocorre, o disco é conectado temporariamente a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impeça todo o tráfego de rede de entrada e de saída. Isso é feito por meio de um par de regras de firewall deny-all: uma para tráfego de entrada e outra para tráfego de saída. Ao usar os VCPs locais do Google Cloud, o MCS cria esse firewall na rede local e o aplica à máquina para masterização. Após a conclusão da masterização, a regra de firewall é removida da imagem.

Recomendamos manter um número mínimo de novas permissões necessárias para usar VPCs compartilhadas. As VPCs compartilhadas são recursos corporativos de nível superior e normalmente têm protocolos de segurança mais rígidos. Por esse motivo, crie um par de regras de firewall no projeto host nos recursos da VPC compartilhada, uma para entrada e outra para saída. Atribua a maior prioridade a elas. Aplique uma nova tag de destino a cada uma das regras, usando o seguinte valor:

```
citrix-provisioning-quarantine-firewall
```

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura regras de firewall que contenham essa tag de destino. Em seguida, ele examina as regras quanto à sua exatidão e as aplica à máquina usada para preparar a imagem mestre para o catálogo. Se as regras de firewall não forem encontradas ou se as regras forem encontradas, mas as regras ou suas prioridades estiverem incorretas, uma mensagem semelhante à seguinte será exibida:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```


Configurar a VPC compartilhada

Antes de adicionar a VPC compartilhada como uma conexão de host na interface Full Configuration do Citrix DaaS, conclua as etapas a seguir para adicionar contas de serviço do projeto que você pretende provisionar:

1. Crie uma função do IAM.
2. Adicione a conta de serviço usada para criar uma conexão de host CVAD à função do IAM do projeto host da VPC compartilhada.
3. Adicione a conta de serviço do Cloud Build do projeto que você pretende provisionar à função do IAM do projeto host da VPC compartilhada.
4. Crie regras de firewall.

Crie uma função do IAM Determine o nível de acesso da função —*acesso no nível do projeto* ou um modelo mais restrito usando o *acesso no nível da sub-rede*.

Acesso no nível do projeto para a função do IAM. Para a função do IAM no nível do projeto, inclua as seguintes permissões:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função do IAM no nível do projeto:

1. No console do Google Cloud, navegue para **IAM & Admin > Roles**.
2. Na página **Roles**, selecione **CREATE ROLE**.
3. Na página **Create Role**, especifique o nome da função. Selecione **ADD PERMISSIONS**.
    a) Na página **Add permissions**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filter table**. Selecione a permissão e, em seguida, selecione **ADD**.
    b) Selecione **CREATE**.

Subnet-level IAM role. Essa função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` depois de selecionar **CREATE ROLE**. Para esse nível de acesso do IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função do IAM no nível da sub-rede:

1. No console do Google Cloud, navegue para **VPC network** > **Shared VPC**. A página **Shared VPC** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.

2. Na página **Shared VPC**, selecione a sub-rede que deseja acessar.
3. No canto superior direito, selecione **ADD MEMBER** para adicionar uma conta de serviço.
4. Na página **Add members**, conclua estas etapas:

    a) No campo **New members**, digite o nome da sua conta de serviço e selecione a sua conta de serviço no menu.
    b) Selecione o campo **Select a role** e depois **Compute Network User**.
    c) Selecione **SAVE**.

5. No console do Google Cloud, navegue para **IAM & Admin** > **Roles**.
6. Na página **Roles**, selecione **CREATE ROLE**.
7. Na página **Create Role**, especifique o nome da função. Selecione **ADD PERMISSIONS**.

    a) Na página **Add permissions**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filter table**. Selecione a permissão e, em seguida, selecione **ADD**.
    b) Selecione **CREATE**.

Adicionar uma conta de serviço à função do IAM do projeto host Depois de criar uma função do IAM, siga estas etapas para adicionar uma conta de serviço ao projeto host:

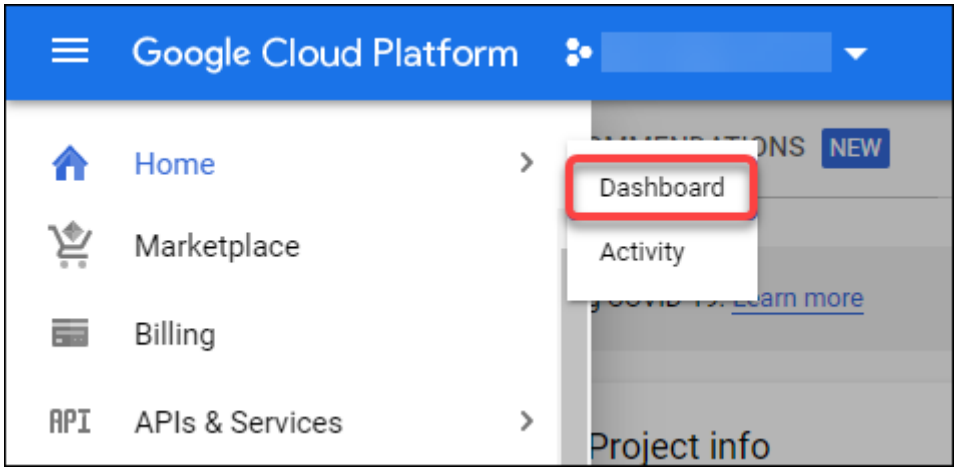
1. No console do Google Cloud, navegue até o projeto do host e vá para **IAM & Admin > IAM**.
2. Na página **IAM**, selecione **ADD** para adicionar uma conta de serviço.
3. Na página **Add members**:

    a) No campo **New members**, digite o nome da sua conta de serviço e selecione a sua conta de serviço no menu.
    b) Selecione um campo de função, digite a função do IAM que você criou e, em seguida, selecione a função no menu.
    c) Selecione **SAVE**.

Agora, a conta de serviço já está configurada para o projeto host.

Adicionar a conta de serviço do Cloud Build à VPC compartilhada Cada assinatura do Google Cloud tem uma conta de serviço que tem, como nome, o número do ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar qual é o número do ID do projeto selecionando **Home** e **Dashboard** no console do Google Cloud:



Na tela, procure **Project Number** abaixo da área **Project Info**.

Execute as etapas a seguir para adicionar a conta de serviço do Cloud Build à VPC compartilhada:

1. No console do Google Cloud, navegue até o projeto host e vá para **IAM & Admin** > **IAM**.
2. Na página **Permissions**, selecione **ADD** para adicionar uma conta.
3. Na página **Add members**, conclua estas etapas:

    a) No campo **New members**, digite o nome da conta de serviço do Cloud Build e selecione a sua conta de serviço no menu.
    b) Selecione o campo **Select a role**, digite `Computer Network User` e, em seguida, selecione a função no menu.
    c) Selecione **SAVE**.

Criar regras de firewall Como parte do processo de masterização, o MCS copia a imagem da máquina selecionada e a usa para preparar o disco do sistema de imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que executa scripts de preparação. Essa VM deve ser executada em um ambiente isolado que proíba todo o tráfego de rede de entrada e saída. Para criar um ambiente isolado, o MCS exige duas regras de firewall *deny all* (uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall em *Host Project* da seguinte forma:

1. No console do Google Cloud, navegue até o projeto host e, em seguida, para **VPC network > Firewall**.
2. Na página **Firewall**, selecione **CREATE FIREWALL RULE**.
3. Na página **Create a firewall rule**, preencha estes dados:

    - **Name**. Digite um nome para a regra.
    - **Network**. Selecione a rede VPC compartilhada à qual a regra de firewall de entrada se aplica.

- **Priority**. Quanto menor for o valor, maior será a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
- **Direction of traffic**. Selecione **Ingress**.
- **Action on match**. Selecione **Deny**.
- **Targets**. Use o padrão, **Specified target tags**.
- **Target tags**. Digite `citrix-provisioning-quarantine-firewall`.
- **Source filter**. Use o padrão, **IP ranges**.
- **Source IP ranges**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
- **Protocols and ports**. Selecione **Deny all**.

4. Selecione **CREATE** para criar a regra.
5. Repita as etapas de 1 a 4 para criar outra regra. Em **Direction of traffic**, selecione **Egress**.

Adicionar uma conexão Adicione uma conexão aos ambientes de nuvem do Google. Consulte Adicionar uma conexão.

Habilitar a seleção de zona

O Citrix Virtual Apps and Desktops suporta a seleção de zona. Com a seleção de zona, você especifica as zonas nas quais deseja criar as VMs. Com a seleção de zona, os administradores podem colocar nós de locatário único nas zonas de sua escolha. Para configurar a locação única, você deve fazer o seguinte no Google Cloud:

- Reservar um nó de locatário único no Google Cloud
- Criar a imagem mestre do VDA

Como reservar um nó de locatário único no Google Cloud

Para reservar um nó de locatário único, consulte a documentação do Google Cloud.

> **Importante:**
>
> Um modelo de nó é usado para indicar as características de desempenho do sistema reservado no grupo de nós. Essas características incluem o número de vGPUs, a quantidade de memória alocada para o nó e o tipo de máquina usado para máquinas criadas no nó. Para obter mais informações, consulte a documentação do Google Cloud.

Criar a imagem mestre do VDA

Para implantar máquinas no nó de locatário único com sucesso, você precisa executar etapas extras ao criar uma imagem de VM mestre. As instâncias de máquina no Google Cloud têm uma propriedade chamada *node affinity labels*. As instâncias usadas como imagens mestre para catálogos implantados no nó de locatário único exigem um *node affinity label* que corresponda ao nome do **target node group**. Para isso, tenha em mente o seguinte:

- Para uma nova instância, defina o rótulo no console do Google Cloud ao criar uma instância. Para obter detalhes, consulte Definir um rótulo de afinidade de nó ao criar uma instância.
- Para uma instância existente, defina o rótulo usando a linha de comando **gcloud**. Para obter detalhes, consulte Definir um rótulo de afinidade de nó para uma instância existente.

> **Nota:**
>
> Se você pretende usar a locação única com uma VPC compartilhada, consulte Nuvem privada virtual compartilhada.

Definir um rótulo de afinidade de nó ao criar uma instância Para definir o rótulo de afinidade do nó:

1. No console do Google Cloud, navegue até **Compute Engine > VM instances**.
2. Na página **VM instances**, selecione **Create instance**.
3. Na página **Instance creation**, digite ou configure a informação necessária e selecione **management, security, disks, networking, sole tenancy** para abrir o painel de configurações.
4. Na guia **Sole tenancy**, selecione **Browse** para visualizar os grupos de nós disponíveis no projeto atual. A página **Sole-tenant node** é exibida, mostrando uma lista de grupos de nós disponíveis.
5. Na página **Sole-tenant node**, selecione o grupo de nós aplicável na lista e selecione **Select** para voltar à guia **Sole tenancy**. O campo de rótulos de afinidade do nós é preenchido com as informações selecionadas. Essa configuração garante que os catálogos de máquinas criados a partir da instância sejam implantados no grupo de nós selecionado.
6. Selecione **Create** para criar a instância.

Definir um rótulo de afinidade de nó para uma instância existente Para definir o rótulo de afinidade do nó:

1. Na janela de terminal do Google Cloud Shell, use o comando *gcloud compute instances* para definir um rótulo de afinidade de nó. Inclua as seguintes informações no comando **gcloud**:
    - **Nome da VM**. Por exemplo, use uma VM existente chamada `s*2019-vda-base`.*

- **Nome do grupo de nós**. Use o nome do grupo de nós que você criou anteriormente. Por exemplo, `mh-sole-tenant-node-group-1`.
- **A zona em que a instância reside**. Por exemplo, a VM reside em `*us-east-1b* zone`.

Por exemplo, digite o seguinte comando na janela do terminal:

- `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

Para obter mais informações sobre o comando *gcloud compute instances*, consulte a documentação do Google Developer Tools em https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Navegue até a página **VM instance details** da instância e verifique se o campo **Node Affinities** é preenchido com o rótulo.

Criar um catálogo de máquinas Depois de definir o rótulo de afinidade do nó, configure o catálogo de máquinas.

Preview: Usar chaves de criptografia gerenciadas pelo cliente (CMEK)

Você pode usar chaves de criptografia gerenciadas pelo cliente (CMEK) para catálogos do MCS. Ao usar essa funcionalidade, você atribui a função `CryptoKey Encrypter/Decrypter` do serviço Key Management Service do Google Cloud ao agente de serviço do Compute Engine. A conta Citrix DaaS deve ter as permissões corretas no projeto em que a chave está armazenada. Consulte Ajudar a proteger recursos usando chaves do Cloud KMS para obter mais informações.

Seu agente de serviço do Compute Engine está no seguinte formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Esse formulário é diferente da conta de serviço padrão do Compute Engine.

> **Nota:**
>
> Essa conta de serviço do Compute Engine talvez não apareça na tela **IAM Permissions** do Google Console. Nesse caso, use o comando `gcloud` conforme descrito em Ajudar a proteger recursos usando chaves do Cloud KMS.

Atribuir permissões à conta Citrix DaaS

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões de KMS no *nível do projeto* ou permissões de KMS no *nível do recurso*. Consulte Permissões e funções para obter mais informações.

Permissões no nível do projeto Uma opção é fornecer à conta Citrix DaaS permissões no nível do projeto para navegar pelos recursos do Cloud KMS. Para isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua essa função personalizada à sua conta Citrix DaaS. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

Permissões de nível do recurso Na outra opção, de permissões no nível do recurso, no console do Google Cloud, navegue até a `cryptoKey` que você usa para o provisionamento de MCS. Adicione uma conta Citrix DaaS a um keyring ou chave que você usa para provisionamento de catálogo.

> **Dica:**
>
> Com essa opção, você não pode procurar chaves regionais para o seu projeto no inventário porque a conta do Citrix DaaS não tem permissões de lista de nível do projeto nos recursos do Cloud KMS. No entanto, você ainda pode provisionar um catálogo usando o CMEK especificando o `cryptoKeyId` correto nas propriedades personalizadas `ProvScheme`, como descrito abaixo.

Provisionar com CMEK usando propriedades personalizadas

Ao criar o seu esquema de provisionamento via PowerShell, especifique uma propriedade `CryptoKeyId` em `ProvScheme CustomProperties`. Por exemplo:

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
        yourCryptoKeyId>" />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

`cryptoKeyId` deve ser especificada no seguinte formato:

`projectId:location:keyRingName:cryptoKeyName`

Por exemplo, se você quiser usar a chave `my-example-key` no keyring `my-example-key-ring` na região `us-east1` e no projeto com ID `my-example-project-1`, suas configurações personalizadas `ProvScheme` serão semelhantes a:


```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Todas as imagens e discos provisionados do MCS relacionados a esse esquema de provisionamento usam essa chave de criptografia gerenciada pelo cliente.

> **Dica:**
>
> Se você usar chaves globais, o local das propriedades do cliente deverá indicar `global` e não o nome da **região**, que no exemplo acima é **us-east1**. Por exemplo: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

Rotação de chaves gerenciadas pelo cliente

O Google Cloud não é compatível com a rotação de chaves em imagens ou discos permanentes existentes. Depois que uma máquina é provisionada, ela é vinculada à versão da chave em uso no momento em que foi criada. No entanto, uma nova versão da chave pode ser criada, e essa nova chave é usada para máquinas recém-provisionadas ou recursos criados quando um catálogo é atualizado com uma nova imagem mestre.

Considerações importantes sobre keyrings Os keyrings não podem ser renomeados ou excluídos. Além disso, você pode incorrer em encargos imprevistos ao configurá-los. Ao excluir ou remover um keyring, o Google Cloud exibe uma mensagem de erro:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
   about the security implications of allowing multiple keys or key
   versions over time to have the same resource name, so we decided to
   make names immutable. (And you can't delete them, because we wouldn'
   t be able to do a true deletion--there would still have to be a
   tombstone tracking that this name had been used and couldn't be
   reused).
We're aware that this can make things untidy, but we have no immediate
   plans to change this.
If you want to avoid getting billed for a key or otherwise make it
   unavailable, you can do so by deleting all the key versions; neither
    keys nor key rings are billed for, just the active key versions
   within the keys.
<!--NeedCopy-->
```


> **Dica:**
>
> Para obter mais informações, consulte Editing or deleting a key ring from the console.

Compatibilidade de acesso uniforme no nível do bucket

O Citrix DaaS é compatível com a política de controle de acesso uniforme no nível do bucket no Google Cloud. Essa funcionalidade aumenta o uso da política do IAM que concede permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com controle de acesso uniforme no nível do bucket, o Citrix DaaS permite que você use uma lista de controle de acesso (ACL) para controlar o acesso a buckets de armazenamento ou objetos armazenados neles. Consulte Acesso uniforme no nível do bucket para obter informações gerais sobre o acesso uniforme no nível do bucket no Google Cloud. Para obter informações de configuração, consulte Requerer acesso uniforme no nível do bucket.

Google Cloud Marketplace

Você pode navegar e selecionar imagens oferecidas pela Citrix no **Google Cloud Marketplace** para criar catálogos de máquinas. Atualmente, o MCS suporta somente o fluxo de trabalho de perfil de máquina para esse recurso.

Para pesquisar o produto Citrix VDA VM no Google Cloud Marketplace, acesse https://console.cloud.google.com/marketplace.

Você pode usar uma imagem personalizada ou uma imagem Citrix Ready no **Google Cloud Marketplace** para atualizar uma imagem de um catálogo de máquinas.

> **Nota:**
>
> Se o perfil da máquina não contiver informações sobre o tipo de armazenamento, o valor será derivado das propriedades personalizadas.

As imagens compatíveis do Google Cloud Marketplace são:

- Windows 2019 Single Session
- Windows 2019 Multi Session
- Ubuntu

Exemplo de uso de uma imagem pronta da Citrix como fonte para criar um catálogo de máquinas:

```
1 New-ProvScheme -ProvisioningSchemeName GCPCatalog \
2 -HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
3 -MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
     win2019-single-vda-v20220819.publicimage \
```



```
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

URLs do ponto de extremidade de serviço

Você deve ter acesso às seguintes URLs:

- https://oauth2.googleapis.com
- https://cloudresourcemanager.googleapis.com
- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

Projetos do Google Cloud

Existem basicamente dois tipos de projetos do Google Cloud:

- Projeto de provisionamento: nesse caso, a conta de administrador atual é proprietária das máquinas provisionadas no projeto. Esse projeto também é conhecido como projeto local.
- Projeto de VPC compartilhada: projeto no qual máquinas criadas no projeto de provisionamento usam a VPC do projeto de VPC compartilhada. A conta de administrador usada para provisionar o projeto tem permissões limitadas nesse projeto –especificamente, somente permissões para usar a VPC.

Sobre as permissões do GCP

Esta seção tem a lista completa das permissões do GCP. Use o conjunto completo de permissões, conforme indicado na seção, para que a funcionalidade funcione corretamente.

Criar uma conexão de host

- Permissões mínimas necessárias para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
```



```
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Cloud Datastore User

- Permissões adicionais necessárias para a VPC compartilhada para a conta de serviço do Citrix Cloud no projeto de VPC compartilhada:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User

Gerenciamento de energia de VMs

Permissões mínimas necessárias para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
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
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Cloud Datastore User

Criar, atualizar ou excluir VMs

- Permissões mínimas necessárias para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
```



```
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Admin
- Storage Admin
- Cloud Build Editor
- Service Account User
- Cloud Datastore User

- Permissões adicionais necessárias para a VPC compartilhada para a conta de serviço do Citrix Cloud no projeto de VPC compartilhada para criar uma unidade de hospedagem usando VPC e sub-rede do projeto de VPC compartilhada:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
```



```
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Cloud Datastore User

- Permissões mínimas exigidas para a conta de serviço Cloud Build no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```


As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Cloud Build Service Account
- Compute Instance Admin
- Service Account User

- Permissões mínimas exigidas para a conta do serviço Cloud Compute no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Permissões adicionais necessárias para a VPC compartilhada para a conta de serviço do Cloud Build no projeto de Provisioning exigido pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute Network User
- Storage Account User
- Cloud Datastore User

- Permissões adicionais necessárias para o Cloud Key Management Service (KMS) para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Compute KMS Viewer

Permissões gerais

A seguir estão as permissões para a conta do Citrix Cloud Service no projeto Provisioning para todos os recursos suportados no MCS. Essas permissões oferecem a melhor compatibilidade daqui para frente:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
```



```
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização da Nutanix

January 3, 2024

Siga estas instruções quando usar o Nutanix Acropolis para fornecer máquinas virtuais em sua implantação do Citrix Virtual Apps and Desktops. O processo de configuração inclui as seguintes tarefas:

- Instalar e registrar o plug-in Nutanix em seu ambiente Citrix Virtual Apps and Desktops.
- Criar uma conexão com o hipervisor Nutanix Acropolis.
- Criar um catálogo de máquinas que use um instantâneo de uma imagem mestre que você cria no hipervisor Nutanix.

Para obter mais informações, consulte o Manual de instalação do plug-in Nutanix Acropolis MCS, disponível no Nutanix Support Portal.

Instalar e registrar o plug-in Nutanix

Conclua o procedimento a seguir para instalar e registrar o plug-in Nutanix em todos os seus Delivery Controllers. Use o Citrix Studio para criar uma conexão com o Nutanix. Em seguida, crie um catálogo de máquinas que use um instantâneo da imagem mestre que você criou no ambiente Nutanix.

> **Dica:**
>
> Recomendamos que você pare e reinicie o Citrix Host Service, o Citrix Broker Service e o Machine Creation Services quando instalar ou atualizar o plug-in Nutanix.

Para obter informações sobre a instalação do plug-in Nutanix, consulte o site da documentação do Nutanix.

Criar uma conexão com Nutanix

As informações a seguir são um complemento às orientações em Conexões e recursos. Para estabelecer uma conexão com o Nutanix, siga as orientações gerais neste artigo, cuidando dos detalhes específicos ao Nutanix.

No assistente **Add Connection and Resources**, selecione o tipo de conexão Nutanix na página **Connection** e especifique o endereço e as credenciais, além de um nome para a conexão. Na página **Network**, selecione uma rede para a unidade de hospedagem.

Os seguintes tipos de conexão estão disponíveis para seleção: **Nutanix AHV**, **Nutamix AHV DRaaS** e **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique o endereço e as credenciais do cluster do Prism Element (PE).

- Para **Nutanix AHV PC**, especifique o endereço e as credenciais do Prism Central (PC).

  > **Nota:**
  >
  > Atualmente, o tipo de conexão Nutanix AHV PC só é usado 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 do NC2 no Azure.

- Para **Nutanix AHV DRaaS**, especifique o endereço e o nome de usuário do locatário do DRaaS. Importe seus arquivos de credenciais públicos e privados do Nutanix DRaaS (`.pem`).

> **Dica:**
>
> Se você implantar máquinas usando o Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

Criar um catálogo de máquinas usando um instantâneo Nutanix

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar um catálogo, siga as orientações gerais neste artigo, cuidando dos detalhes específicos ao Nutanix.

O instantâneo que você seleciona é o modelo usado para criar as VMs no catálogo. Antes de criar o catálogo, crie imagens e instantâneos no Nutanix. Para obter mais informações, consulte a documentação do Nutanix.

No assistente de criação de catálogo:

- As páginas **Operating System** e **Machine Management** não contêm informações específicas ao Nutanix.
- A página **Container** ou **Cluster and Container** é exclusiva do Nutanix.

  Se você implantar máquinas usando o Nutanix AHV XI como recursos, verá a página **Container**. Selecione o contêiner em que os discos de identidade das VMs serão colocados.

  Se você implantar máquinas usando o Nutanix AHV Prism Central (PC) como recursos, verá a página **Cluster and Container**. Selecione qual cluster usar para a implantação de VMs e, em seguida, um contêiner.

- Na página **Master Image**, selecione o instantâneo da imagem. O nome dos instantâneos do Acropolis devem ter o prefixo "XD_"para usar no Citrix Virtual Apps and Desktops. Use o console do Acropolis para renomear seus instantâneos, se necessário. Se você renomear instantâneos, reinicie o assistente de criação de catálogos para ver uma lista atualizada.
- Na página **Virtual Machines**, indique o número de CPUs virtuais e o número de núcleos por vCPU.

- Na página **Network Cards**, selecione o tipo de NIC para filtrar as redes associadas. Existem dois tipos de NIC: **VLAN** e **OVERLAY**. Selecione uma ou mais NICs contidas na imagem mestre e, em seguida, selecione uma rede virtual associada para cada NIC.
- As páginas **Machine Identities**, **Domain Credentials**, **Scopes** e **Summary** não contêm informações específicas do Nutanix.

Soluções de nuvem e parceiros da Nutanix

June 28, 2023

O Citrix Virtual Apps and Desktops oferece suporte à seguinte solução de nuvem e parceiros da Nutanix:

- Nutanix Cloud Clusters na AWS

Nutanix Cloud Clusters na AWS

O Citrix Virtual Apps and Desktops é compatível com o Nutanix Cloud Clusters na AWS. O Nutanix Clusters simplifica a forma como os aplicativos são executados em nuvens privadas ou em várias nuvens públicas. Para obter mais informações sobre o Nutanix Cloud Clusters na AWS, consulte Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Dica:**
>
> Esse suporte fornece a mesma funcionalidade de um cluster local da Nutanix. Somente um único cluster é suportado, o *Prism Element*. Para obter mais informações, veja aqui.

Requisitos

Você precisa do seguinte para usar os clusters Nutanix na AWS:

- Uma conta Nutanix.
- Uma conta da AWS com as seguintes permissões:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Criar um cluster Nutanix

Para criar um cluster Nutanix:

1. Faça login na sua conta Nutanix.
2. Localize a opção de **Nutanix cluster** e clique em **Launch**. O **Nutanix Console** é aberto. Para obter mais informações, consulte Get Started with Nutanix Cluster on AWS.
3. Escolha criar uma **new VPC**.

O processo de criação do cluster pode falhar com os seguintes erros:

- Falha ao criar o cluster dentro de um determinado período. Exclusão do cluster.
- Host Nutanix Cluster - Nó `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Nó `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

Se o cluster não tiver sido criado:

- Tente recriar um cluster em uma região diferente.
- Tenha o cuidado de excluir o Nutanix CloudFormation Stack (CFS) antes de tentar novamente.

Além de outros recursos, o Nutanix CFS cria:

- 1 VPC chamada *Nutanix Cluster 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

Depois que o cluster for criado, recupere o endereço do **Nutanix Prism**:

1. Vá para o **Nutanix Console**.
2. No canto superior direito do console, passe o mouse sobre o link **Launch Prism Element** e copie o URL.

Conecte-se ao Nutanix Prism

Depois de criar um cluster Nutanix, conecte-se ao Nutanix Prism.

Para se conectar ao Nutanix Prism:

1. Crie uma VM bastion na sub-rede 10.0.129.0/24.
2. RDP na VM bastion, vá para o URL do **Prism Element** que você copiou na seção anterior.
3. Faça login usando as credenciais padrão: `admin:nutanix/4u`. Lembre-se de alterar a senha.

Crie uma VM no cluster da Nutanix

Depois de se conectar ao **Nutanix Prism**, crie VMs no cluster da Nutanix.

Se a VM precisar de acesso à Internet

1. Vá para o console da AWS.
2. Crie uma nova sub-rede 10.0.130.0/24 na mesma VPC criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas dessa sub-rede para direcionar todo o tráfego local para o gateway NAT acima.
4. RDP na VM bastion, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
5. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a mesma sub-rede 10.0.130.0/24 usada na AWS.
6. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa nova sub-rede.

Se a VM não precisar de acesso à Internet

1. RDP na VM bastion, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
2. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a sub-rede 10.0.129.0/24.
3. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa sub-rede.

> **Dica:**
>
> Verifique se as informações de horário e fuso horário nas VMs estão configuradas corretamente. Isso aplica-se especialmente ao AD.

Criar conexão de host

1. Inicie o Web Studio.
2. Selecione o nó de hospedagem e clique em **Add Connection and Resources**.
3. Na tela **Conexão**, selecione **Criar uma nova conexão**e, no **Endereço de 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

June 28, 2023

> **Importante:**
>
> A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade da licença. Para obter mais informações, consulte Citrix Licensing Data.

Os componentes principais são o Citrix Delivery Controller, Citrix Studio, Web Studio, Citrix Director e Citrix License Server.

> **Nota:**
>
> O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação local do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio —um console de gerenciamento baseado na web que oferece total paridade de recursos com o Citrix Studio. Para obter mais informações sobre o Web Studio, consulte Instalar o Web Studio.

(Nas versões anteriores a 2003, os componentes principais incluíam o Citrix StoreFront. Você ainda pode instalar o StoreFront clicando no bloco **Citrix StoreFront** ou executando o comando disponível na mídia de instalação.)

Antes de iniciar uma instalação, revise este artigo e Preparar a instalação.

Este artigo descreve a sequência do assistente de instalação ao instalar componentes principais. Equivalentes de linhas 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

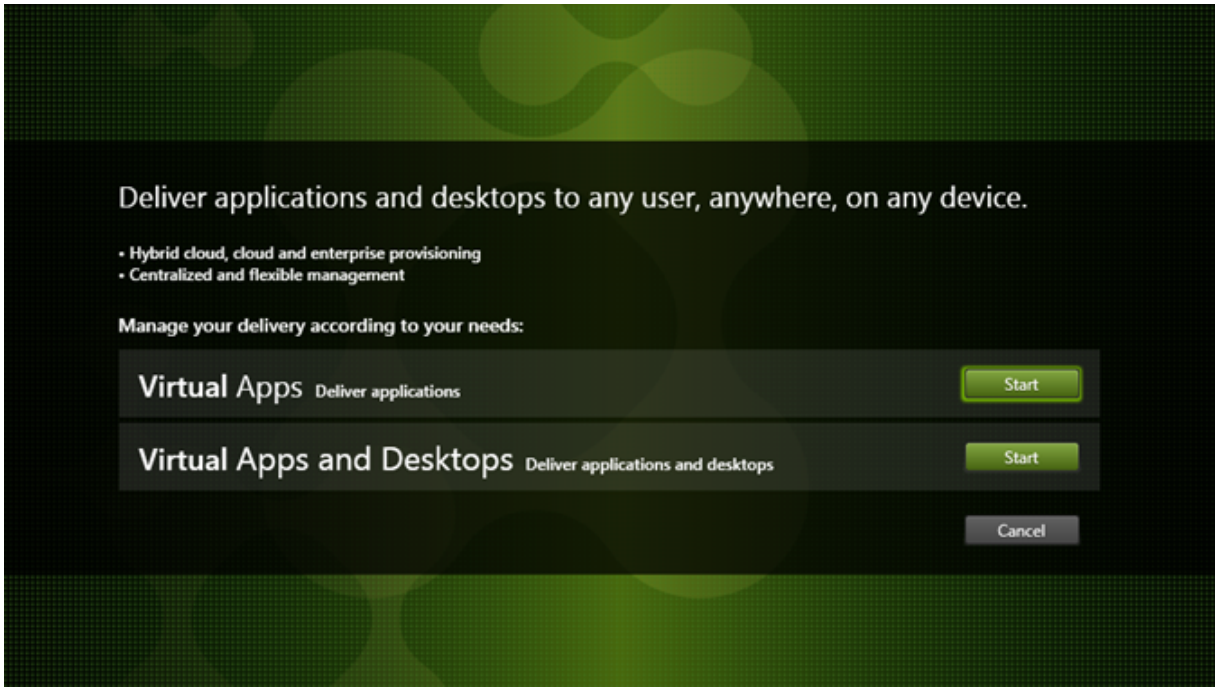
Use as credenciais da sua conta da Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o arquivo ISO do produto.

Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.

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 for iniciado automaticamente, clique duas vezes em **AutoSelect** no aplicativo ou na unidade montada.

Etapa 2. Escolha qual produto instalar

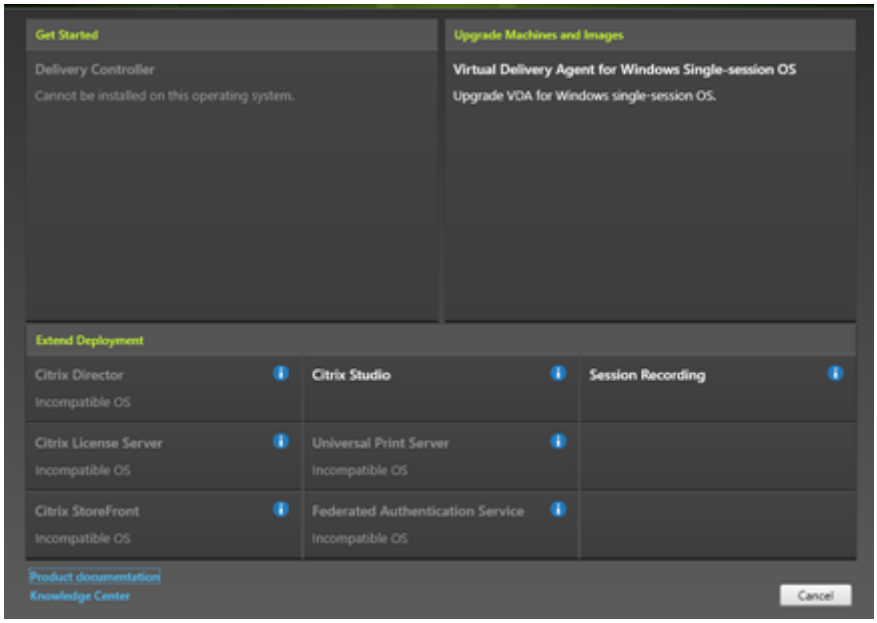


Clique em **Start** ao lado do produto a ser instalado: Virtual Apps ou Virtual Apps and Desktops.

(Se a máquina já tiver os componentes do Citrix Virtual Apps and Desktops instalados, esta página não será exibida.)

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

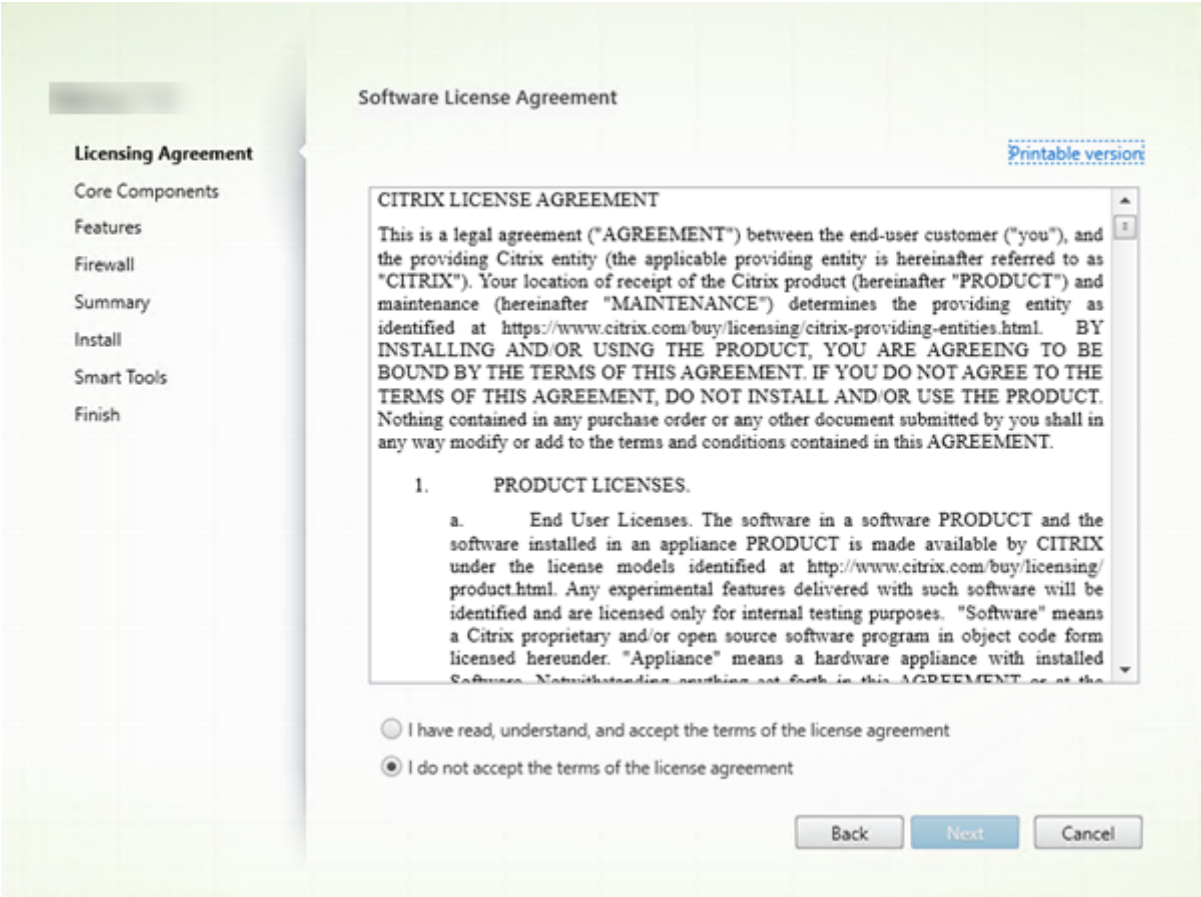


Se você está apenas começando, selecione **Delivery Controller**. (Em uma página mais diante, você seleciona os componentes específicos para instalar na máquina.)

Se você já instalou um Controller (nesta máquina ou em outra) e deseja instalar outro componente, selecione o componente na seção **Extend Deployment**.

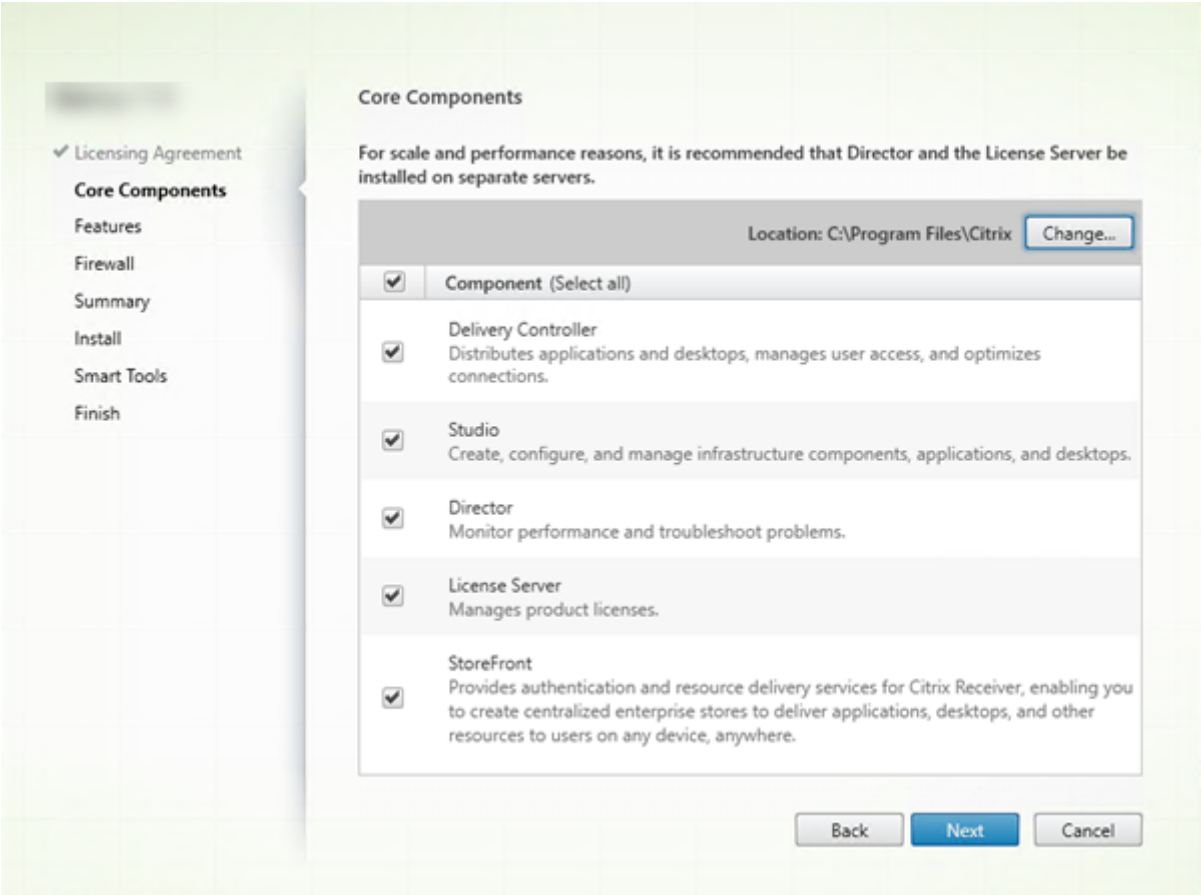
Opção de linha de comando: `/components`

Etapa 4. Leia e aceite o contrato de licença



Na página **Licensing Agreement**, depois de ler o contrato de licença, indique que você leu e aceitou as condições. Clique em **Next**.

Etapa 5. Selecione os componentes para instalar e o local de instalação



Na página **Core components**:

- **Location:** por padrão, os componentes são instalados em `C:\Program Files\Citrix`. O padrão é adequado para a maioria das implantações. Se você especificar um local diferente, ele deve ter permissões de execução para o serviço de rede.
- **Components:** por padrão, as caixas de seleção para todos os componentes principais estão marcadas. Instalar todos os componentes principais em um servidor é adequado para provas de conceito, teste ou pequenas implantações de produção. Para ambientes de produção maiores, a Citrix recomenda instalar o Director, StoreFront e License Server em servidores separados.

> **Nota:**
>
> Se você estiver instalando componentes em mais de um servidor, instale o Citrix License Server e as licenças primeiro, antes de instalar outros componentes em outros servidores. Para obter orientações, consulte a seção Instalação automática do Guia de licenciamento para Citrix Virtual Apps and Desktops.

Um ícone o alerta quando você optar por não instalar um componente principal necessário na máquina. O alerta relembra você de instalar o componente, embora não necessariamente nessa máquina.

Clique em **Next**.

Opções de linha de comando: `/installdir`, `/components`, `/exclude`

Verificação de hardware

Quando você instala ou atualiza um Delivery Controller, o hardware é verificado. O instalador alerta se a máquina tiver menos do que a quantidade recomendada de RAM (5 GB), o que pode afetar a estabilidade do site. Para obter mais informações, consulte Requisitos de hardware.

Graphical interface: uma caixa de diálogo é exibida.

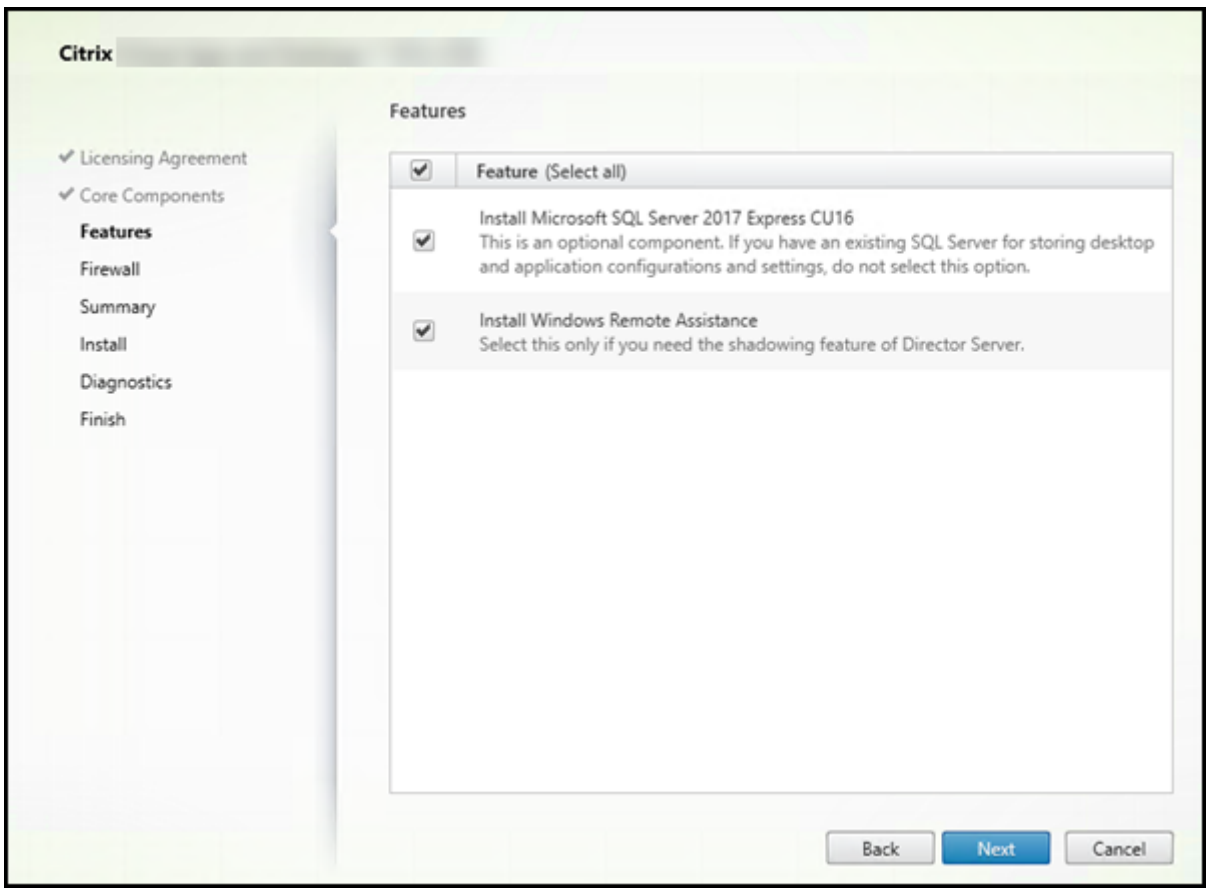
- Recomendado: clique em **Cancel** para parar a instalação. Adicione mais RAM à máquina e inicie a instalação novamente.
- Como alternativa, clique em **Next** para continuar com a instalação. O site pode ter problemas de estabilidade.

Command-line interface: 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 substituir o aviso. Seu site pode ter problemas de estabilidade.

Ao atualizar, você também é notificado se a versão do SO ou do SQL Server não for mais suportada. Consulte Atualizar uma implantação.

Etapa 6. Ativar ou desativar recursos



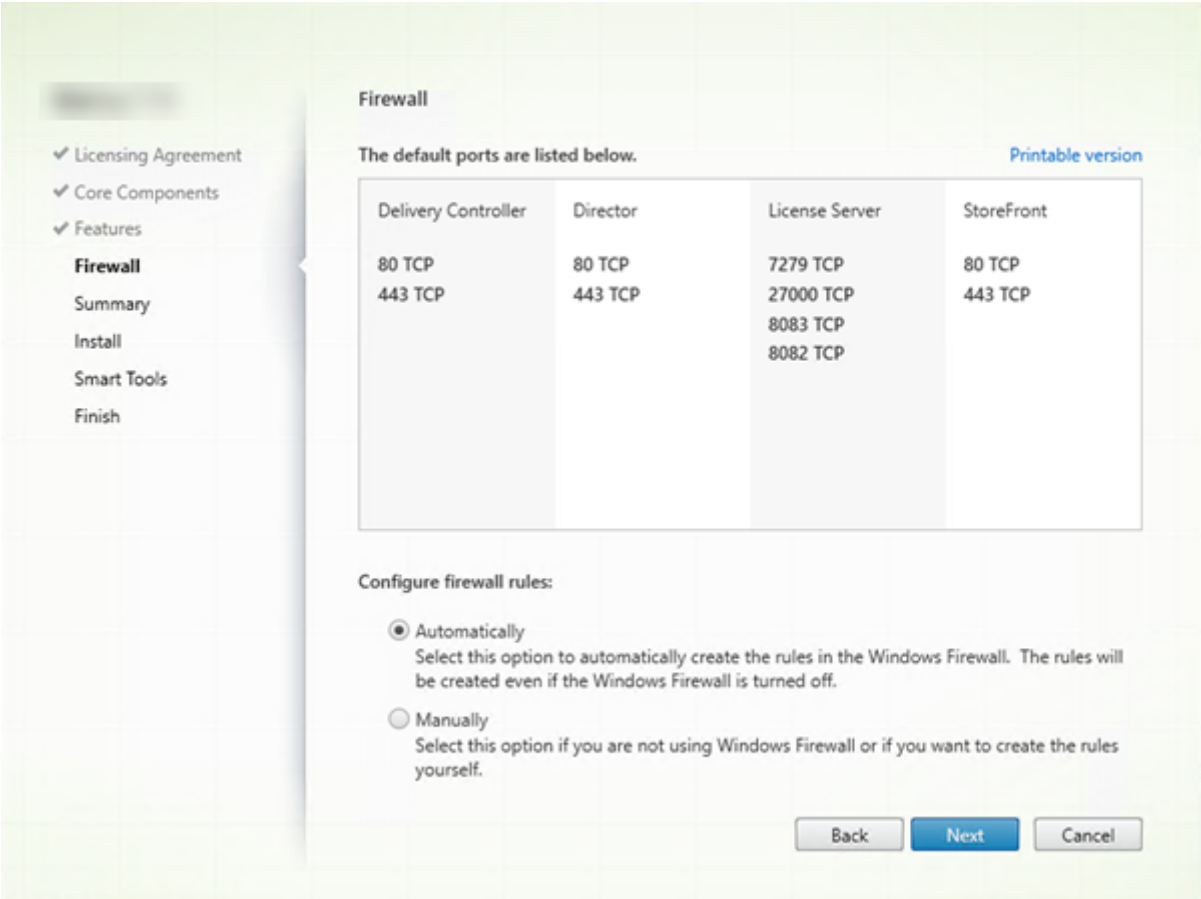
Na página **Features**:

- Escolha se deseja instalar o Microsoft SQL Server Express para usar como banco de dados do site. Por padrão, essa seleção está ativada. Se você não estiver familiarizado com os bancos de dados do Citrix Virtual Apps and Desktops, consulte Bancos de dados.
- Quando você instala o Director, a Assistência Remota do Windows é instalada automaticamente. Você escolhe se deseja ativar o sombreamento na Assistência Remota do Windows para usar com o sombreamento do usuário do Director. Habilitar o sombreamento abre a porta TCP 3389. Por padrão, esse recurso está ativado. A configuração padrão é adequada para a maioria das implantações. Esse recurso aparece somente quando você instala o Director.

Clique em **Next**.

Opções de linha de comando: `/nosql` (para evitar a instalação), `/no_remote_assistance` (para evitar a ativação)

Etapa 7. Abra as portas do firewall do Windows



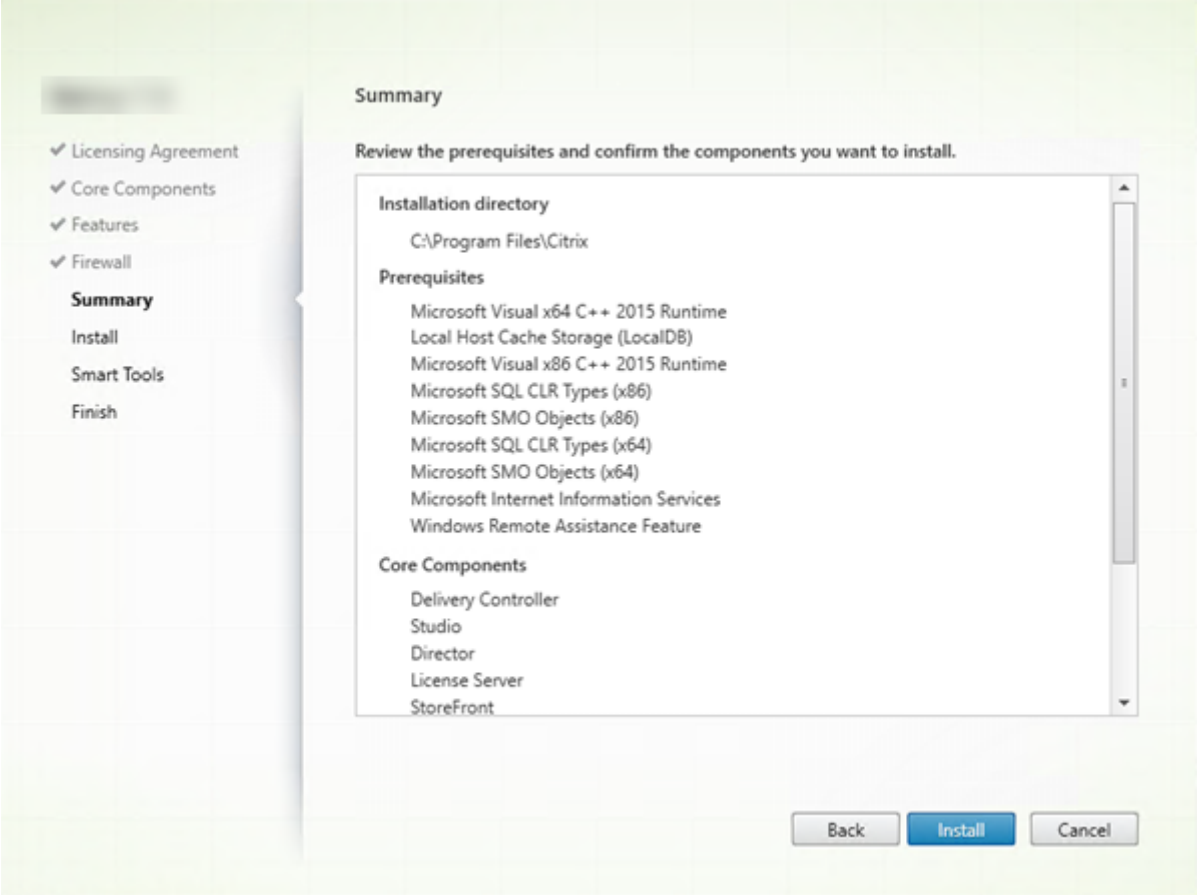
Por padrão, as portas na página **Firewall** são abertas automaticamente se o Serviço do Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. A configuração padrão é adequada para a maioria das implantações. Para obter informações sobre portas, consulte Network ports.

Clique em **Next**.

(O gráfico mostra as listas de portas quando você instala todos os componentes principais na máquina. Esse tipo de instalação geralmente se aplica apenas a implantações de teste.)

Opção de linha de comando: `/configure_firewall`

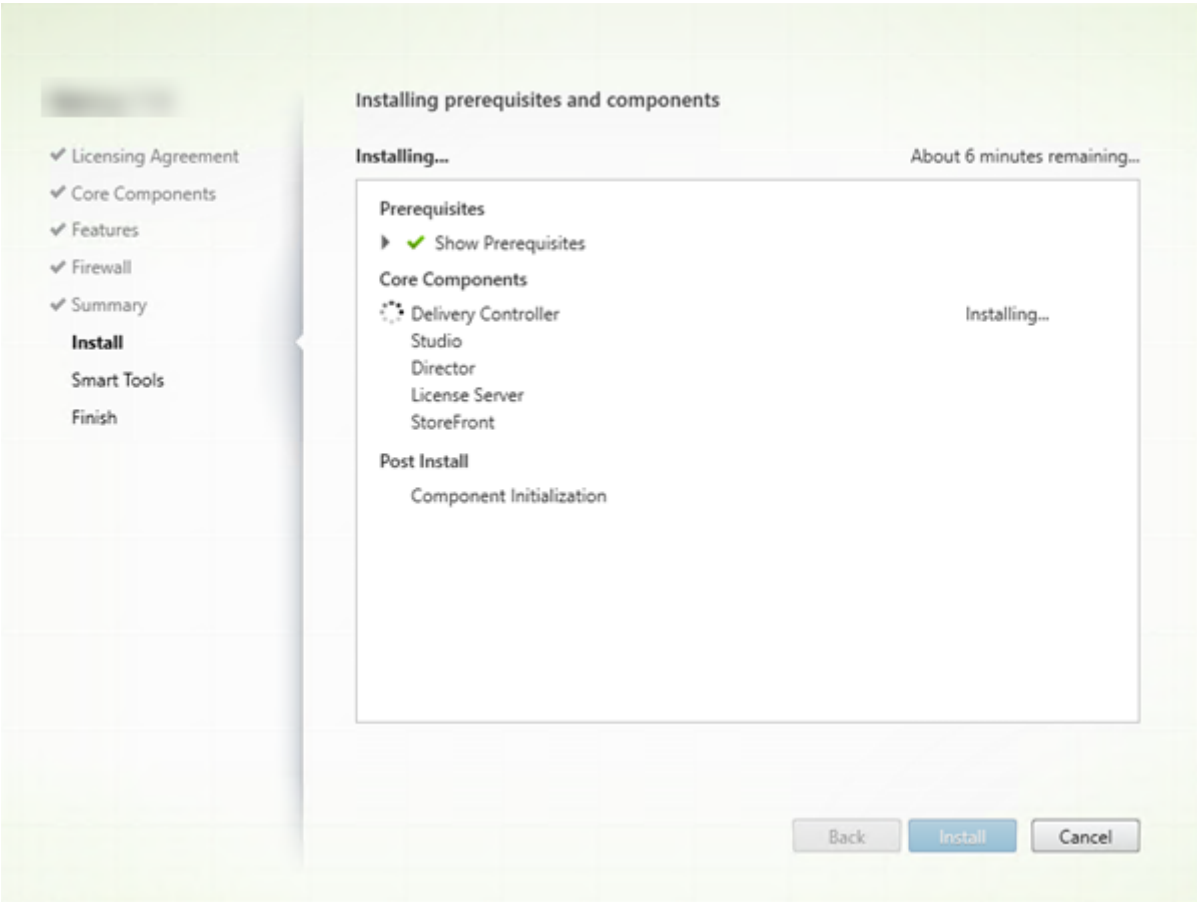
Etapa 8. Verifique os pré-requisitos e confirme a instalação



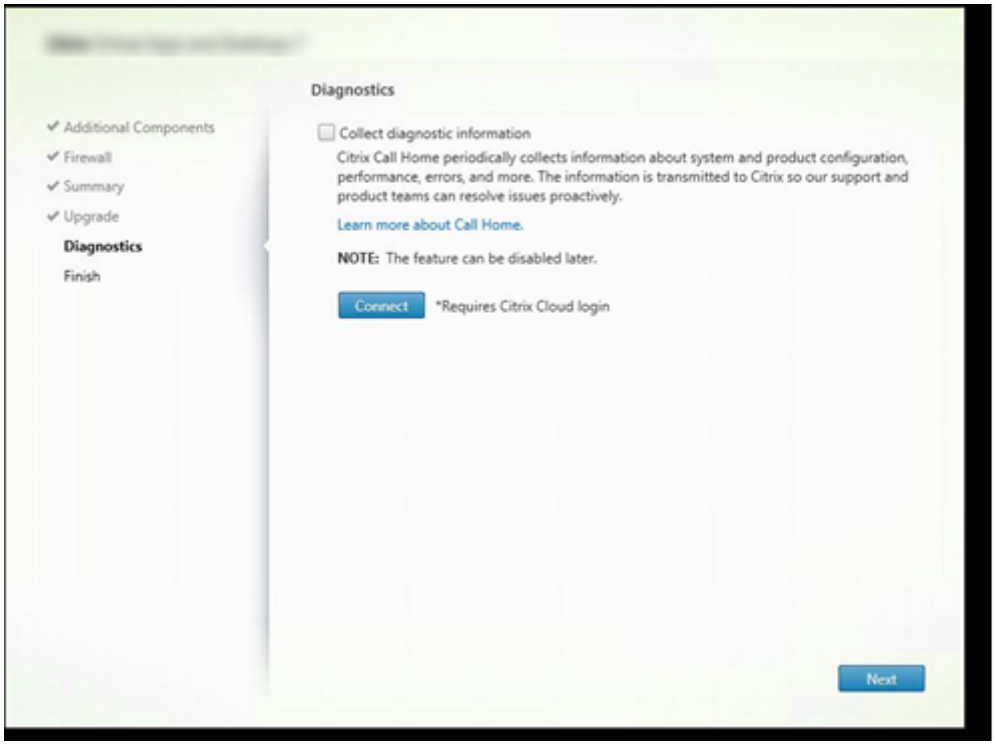
A página **Summary** lista o que será instalado. Use o botão **Back** para retornar às páginas anteriores do assistente e alterar as seleções, se necessário.

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

A tela mostra o andamento da instalação:



Etapa 9. Compartilhamento de informações de diagnóstico com o Cloud Software Group



Na página **Diagnostics**, escolha se deseja participar do Citrix Call Home.

Esta página é exibida ao instalar um Delivery Controller usando a interface gráfica. Quando você instala o StoreFront (mas não um Controller), o assistente exibe esta página. Quando você instala outros componentes principais (mas não um Controller ou StoreFront), o assistente não exibe esta página.

Durante uma atualização, esta página não será exibida se o Call Home já estiver habilitado ou se o instalador encontrar um erro relacionado ao Citrix Telemetry Service.

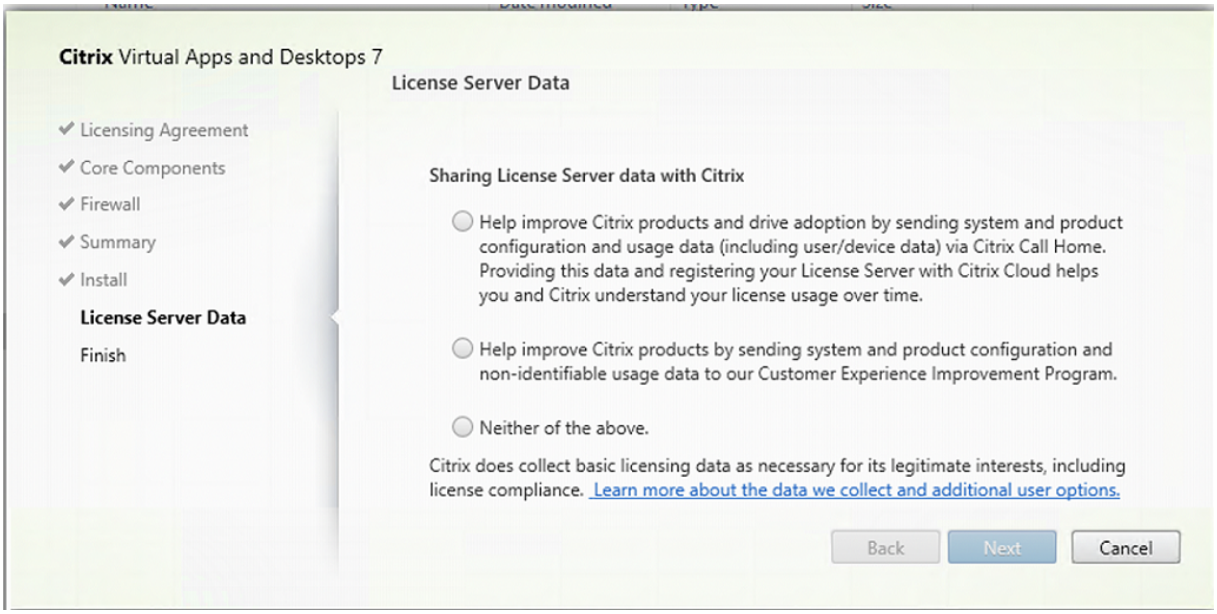
Se você optar por participar (o padrão), clique em **Connect**. Quando solicitado, insira as credenciais da sua conta da Citrix. Você pode alterar sua escolha de registro mais tarde, após a instalação.

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

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

Para obter mais informações, consulte Call Home.

Etapa 10. Compartilhando dados do License Server com o Cloud Software Group



Na página **License Server Data**, solicitamos que você compartilhe dados do Call Home ou do Programa de Aperfeiçoamento da Experiência do Usuário (CEIP) para nos ajudar. Além disso, o Cloud Software Group também exige a coleta de dados básicos de licenciamento, incluindo a conformidade da licença, conforme necessário para seus interesses legítimos.

A página **License Server Data** aparece quando você instala o License Server:

- Como um componente autônomo.
- Como um componente principal, durante a instalação de um Delivery Controller.

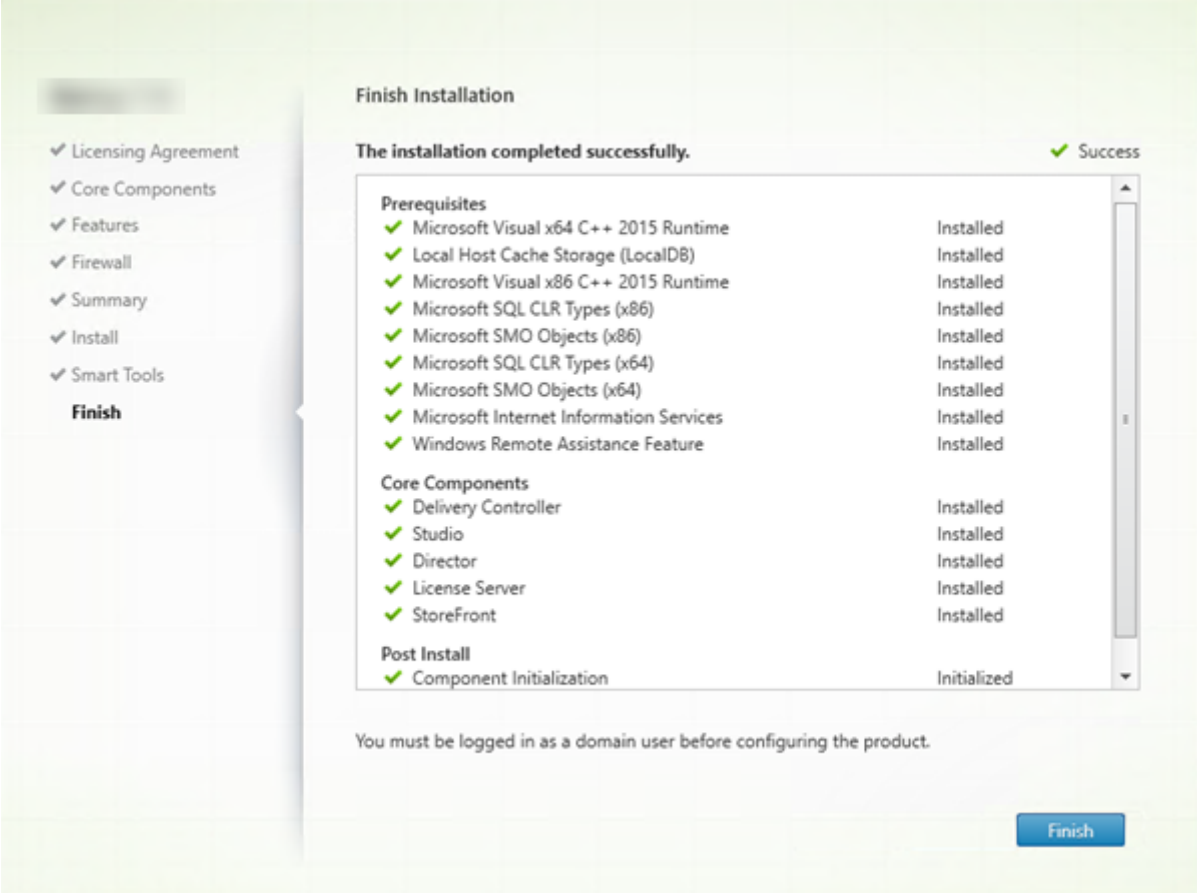
Durante uma atualização, essa página não será exibida se a configuração já estiver definida no arquivo `/CITRIX.opt:.`

O License Server monitora vários tipos de dados do usuário, como dados de licenciamento, dados do Call Home e dados do CEIP. Para ativar os dados do Call Home e a coleta de dados do CEIP, você deve optar por participar (opção opt in).

Para obter mais informações sobre como habilitar a coleta de dados do CEIP e o Call Home ao instalar usando a linha de comando, consulte Opções de linha de comando para instalar componentes principais.

Para obter mais informações sobre a coleta de dados de licenciamento do Cloud Software Group, consulte os Programas de coleta de dados do Citrix Licensing.

Etapa 11. Conclua a instalação



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

Clique em **Finish**.

Etapa 12. Instale 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.

Depois de criar o site, instale os VDAs.

A qualquer hora, você pode usar o instalador de produto completo para ampliar a sua implantação com os seguintes componentes:

- **Componente de servidor Universal Print Server:** inicie o instalador no seu servidor de impressão.

  1. Selecione **Universal Print Server** na seção **Extend Deployment**.
  2. Aceite o contrato de licença.
  3. Na página **Firewall**, por padrão, as portas TCP 7229 e 8080 estão abertas no firewall se o Serviço do Firewall do Windows estiver em execução, mesmo que o firewall não esteja ativado. Você pode desabilitar essa ação padrão se quiser abrir as portas manualmente.

  Para instalar esse componente a partir da linha de comando, consulte Opções de linha de comando para instalar um Universal Print Server.

- Federated Authentication Service.
- Session Recording.
- Workspace Environment Management.

Instalar o Web Studio

April 4, 2024

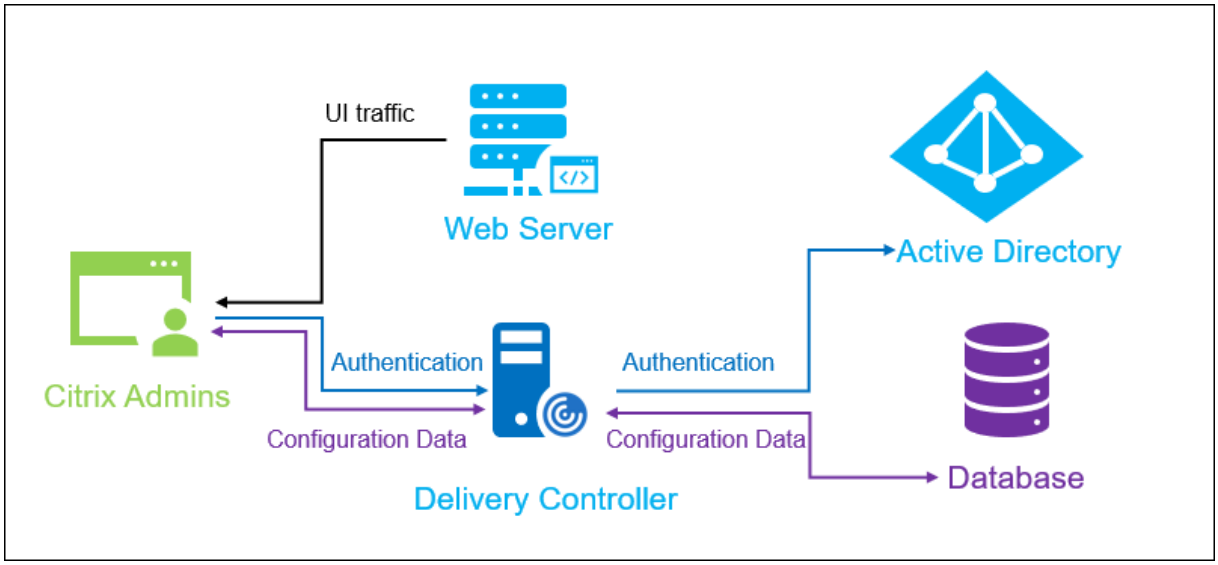
> **Requisitos de licença:**
>
> Para usar o Web Studio, você precisa ter um dos seguintes tipos de licença:
>
> - Licença de assinatura universal Citrix.
> - Assinatura local da Citrix para licenças de varejo anuais e temporárias.
> - Qualquer licença local para Citrix Service Providers (CSP).

Introdução

O Citrix Studio é um console de gerenciamento baseado em Windows que permite configurar e gerenciar sua implantação do Citrix Virtual Apps and Desktops. O Web Studio é a próxima geração do Citrix Studio —um console de gerenciamento baseado na web que oferece total paridade de recursos com o Citrix Studio. Com a mesma aparência da interface Full Configuration do Citrix DaaS, o Web Studio moderniza sua experiência de gerenciamento ao fornecer uma experiência web nativa.

Você pode implantar o Web Studio em qualquer servidor Windows com o Serviços de Informações da Internet (IIS) instalado. Para uma implantação rápida, recomendamos que você instale o Web Studio

juntamente com um Delivery Controller. Nesse caso, o Web Studio é instalado como um site no Delivery Controller. Recomendamos que você siga essa configuração para uma arquitetura simples e menos sobrecarga de gerenciamento. O diagrama a seguir mostra a arquitetura do Web Studio:



Um fluxo de trabalho geral para colocar o Web Studio em funcionamento é o seguinte:

1. Instale o Web Studio.
2. Configure um site.
3. Adicione Delivery Controllers ao Web Studio para gerenciamento.
4. Faça login no Web Studio.

Novos recursos disponíveis no Web Studio em comparação com 2212

Os seguintes recursos agora estão disponíveis no Web Studio:

- **Suporte para configurar o roaming de sessão**. Anteriormente, o PowerShell era a sua única opção para configurar o roaming de sessão para aplicativos e áreas de trabalho. Agora você pode fazer isso usando o Web Studio. Para obter mais informações, consulte Gerenciar grupos de entrega.
- **Algumas ações renomeadas para melhor alinhá-las a seus significados reais.** Renomeamos as seguintes ações em **Machine Catalogs** e **Delivery Groups**. Os fluxos de trabalho para realizar essas ações permanecem inalterados.
  - **Update Machines** renomeado para **Change Master Image**
  - **Rollback Machine Update** renomeado para **Roll Back Master Image**
  - **Upgrade Catalog** renomeado para **Change Functional Level**
  - **Upgrade Delivery Group** renomeado para **Change Functional Level**

  - **Undo Upgrade Catalog** renomeado para **Undo Functional Level Change**
  - **Undo Upgrade Delivery Group** renomeado para **Undo Functional Level Change**

- **Uso de um perfil de máquina ativado por padrão para a criação do catálogo do Azure**. Ao criar catálogos de máquinas do Azure usando o Web Studio, a opção **Use a machine profile** agora está selecionada por padrão. Para obter mais informações, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager.
- **Anotar uma imagem ao atualizar máquinas**. No Web Studio, agora você pode fazer anotações em uma imagem adicionando uma nota sobre ela ao atualizar um catálogo criado pelo MCS. Cada vez que você atualiza o catálogo, é criada uma entrada relacionada à nota se você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como null (-). Para exibir o histórico de notas da imagem, selecione o catálogo, clique em **Template Properties** no painel inferior e, em seguida, clique em **View note history**. Para obter mais informações, consulte Alterar a imagem mestre de um catálogo.
- **Melhore o desempenho preservando uma VM provisionada durante o ciclo de energia**. Adicionamos a configuração **Retain VMs across power cycles** à página **Machine Catalog Setup > Disk Settings**. A configuração permite preservar uma máquina virtual provisionada durante o ciclo de energia em ambientes do Azure. Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.
- **Modo proxy para o Web Studio.** Anteriormente, o console do Web Studio precisava se comunicar com o servidor do Web Studio e com os Delivery Controllers ao gerenciar sites. Com o modo proxy, o servidor Web Studio agora pode atuar como um proxy para Delivery Controllers, tornando-se assim o único ponto de acesso ao console do Web Studio. Para obter mais informações, consulte Configurar o Web Studio como um proxy para Delivery Controllers.

> **Nota:**
>
> Algumas das fontes de informações acima levam você para a documentação do Citrix DaaS. No Citrix DaaS, o Web Studio é conhecido como Full Configuration. Estamos atualizando a documentação atual para cobrir o Web Studio. A implementação das atualizações é um processo contínuo. Agradecemos a sua paciência durante esta transição.

Requisitos do sistema

Sistemas operacionais compatíveis:

- 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

- Windows 11
- Windows 10

Pré-requisitos

Esta versão do Web Studio é compatível com as implantações do Citrix Virtual Apps and Desktops 2212 e posteriores.

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

Limitação conhecida

Se você usa o Web Studio e o Citrix Studio de forma intercambiável, considere a seguinte limitação:

- Um modelo criado no Web Studio não é exibido no Citrix Studio e vice-versa. Isso ocorre porque o Web Studio usa um banco de dados diferente do Citrix Studio para armazenar modelos. Como solução alternativa, crie uma política a partir de um modelo no Web Studio e, em seguida, crie um modelo a partir dessa política no Citrix Studio, e vice-versa.

Instalar o Web Studio

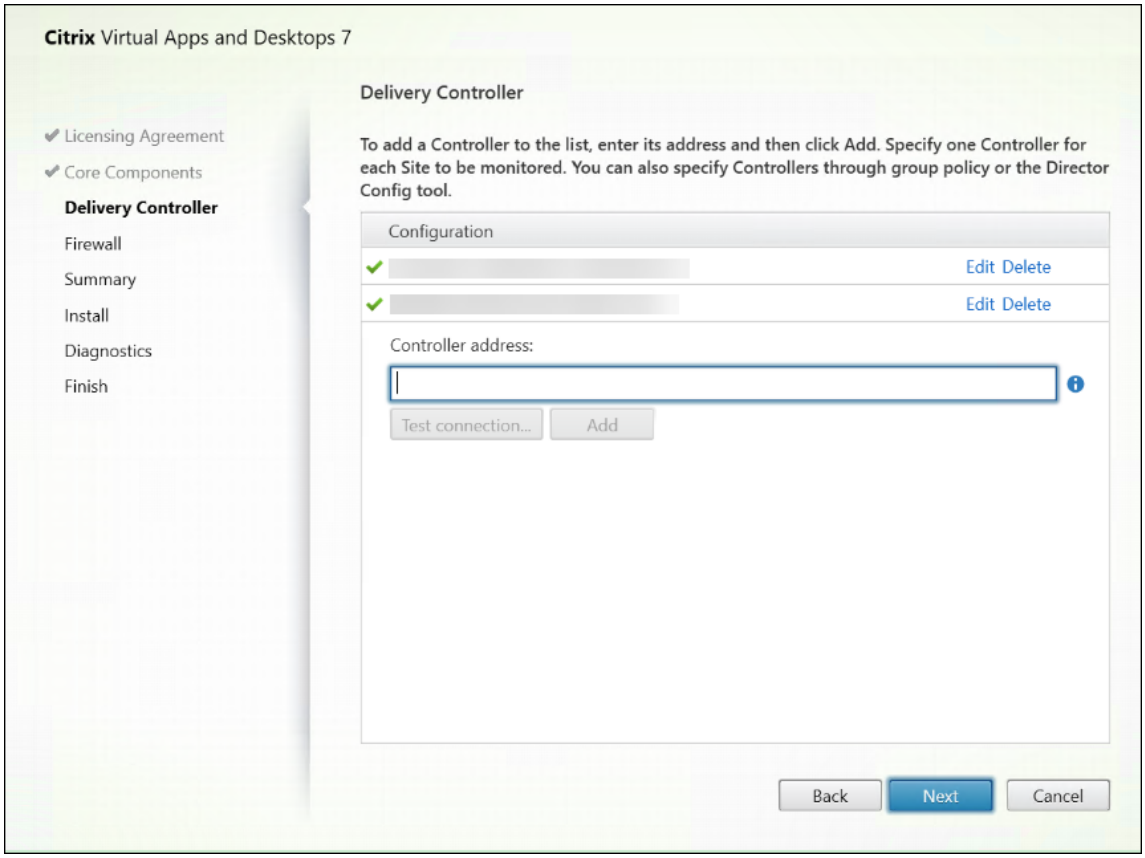
As informações a seguir são um complemento à orientação em Instalar componentes principais. Para instalar o Web Studio:

- Instale o Web Studio usando o instalador ISO do produto completo para Citrix Virtual Apps and Desktops. O instalador ISO verifica os pré-requisitos, instala todos os componentes ausentes, instala o site do Web Studio (no Delivery Controller, se incluído na instalação do Delivery Controller) e executa a configuração básica.
- Se o Web Studio não tiver sido incluído durante a instalação, use o instalador para adicionar o Web Studio.
- Ao instalar o Web Studio, você é solicitado a digitar o endereço de um Delivery Controller.

  > **Nota:**
  >
  > - Você pode adicionar mais de um Delivery Controller. O Web Studio tenta se conectar a eles em ordem aleatória. Se o Delivery Controller ao qual o Web Studio está tentando se conectar estiver inacessível, o Web Studio fará o fallback automaticamente para outros Delivery Controllers.
  > - Se o Director foi selecionado em **Core Components** e instalado, os Delivery Controllers adicionados aqui serão usados tanto para o Web Studio quanto para o

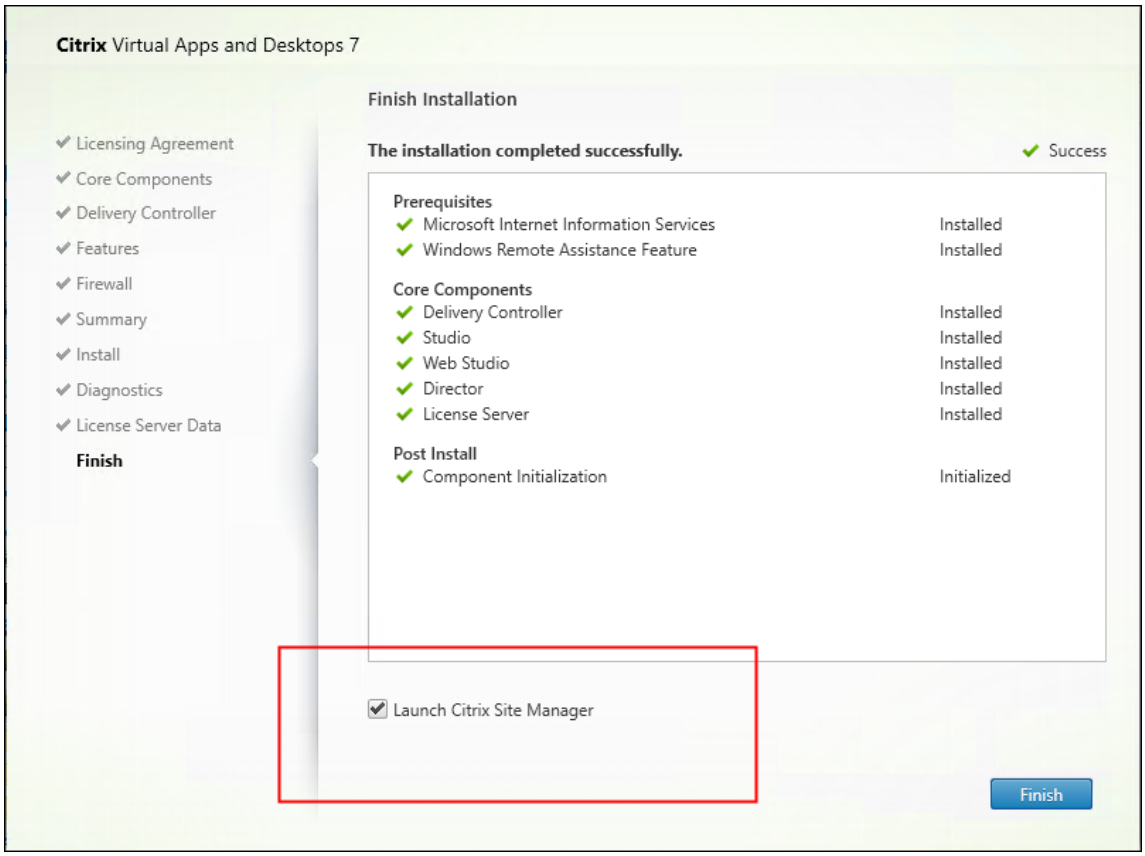
Director.

- Se você não tiver o certificado público confiável externo configurado e não quiser solicitar o certificado de uma CA corporativa, basta configurar o FQDN do seu Delivery Controller.
- Se você tiver o certificado público confiável externo e puder configurar o DNS público para o seu Delivery Controller, poderá digitar o nome do DNS como o endereço do Delivery Controller.
- Se você puder solicitar o certificado da CA corporativa e puder especificar seu DNS pessoal, poderá adicionar seu DNS pessoal como o endereço do Delivery Controller.



- Para proteger as comunicações entre o navegador e o servidor web e entre o navegador e o Delivery Controller, a criptografia TLS deve estar habilitada no site do IIS que hospeda o Web Studio e no Delivery Controller. Se nenhum certificado TLS estiver configurado para o Delivery Controller, o instalador cria um certificado autoassinado, com o FQDN do Delivery Controller e o localhost como o certificado do nome DNS. Se um certificado TLS estiver configurado, o instalador não fará nenhuma alteração. Para obter mais informações sobre criptografia TLS, consulte Proteger uma implantação do Web Studio (opcional).
- Na página **Finish**, a caixa de seleção **Launch Site Manager** é marcada por padrão para que o Citrix Site Manager seja aberto automaticamente. Para iniciá-lo mais tarde, abra o menu Iniciar

da área de trabalho e selecione **Citrix > Citrix Site Manager**. Antes de iniciar o Web Studio, você precisa usar o Citrix Site Manager para criar um site ou ingressar em um site existente. Para obter mais informações, consulte Configurar um site.



> **Nota:**
>
> Você também pode usar a linha de comando para instalar o Web Studio. Exemplo: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Para obter mais informações, consulte Instalar usando a linha de comando.

Configurar um site

Para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como site), use a ferramenta Citrix Site Manager. A ferramenta é instalada automaticamente com um Delivery Controller.

Para configurar um site, siga estas etapas:

1. Em um Delivery Controller, abra o menu Iniciar da área de trabalho e selecione **Citrix > Citrix Site Manager**.

2. No Citrix Site Manager, selecione **Create a site**. O assistente Site Setup é exibido.
3. Crie um site e defina suas configurações da seguinte forma:
    - Na página **Introduction**, digite um nome para o site.
    - A página **Databases** contém seleções para configurar os bancos de dados de log de site, monitoramento e configuração. Para obter mais informações, consulte a Etapa 3. Bancos de dados.
    - No **Licenciamento**, especifique o endereço do servidor de licenças e indique qual licença usar (instalar). Para obter mais informações, consulte a Etapa 4. Licenciamento.
4. Na página **Summary**, verifique todas as configurações e clique em **Submit**.

    O endereço IP desse controlador é adicionado automaticamente ao site.

    > **Nota:**
    >
    > O usuário que cria um site se torna administrador completo dele. Para obter mais informações, consulte Administração delegada.

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

1. Execute o Citrix Site Manager neste novo Controller.
2. Selecione **Join an existing site**.
3. Digite o endereço de um Controller que já foi adicionado ao site.
4. Clique em **Submit**.

Adicionar Delivery Controllers ao Web Studio para gerenciamento

Use a ferramenta de configuração do Studio para adicionar os Delivery Controllers ao Web Studio para gerenciamento. Essa ferramenta está disponível na pasta de instalação do Web Studio.

Por padrão, a ferramenta é instalada na seguinte pasta padrão.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Suponha que você queira configurar os dois Delivery Controllers a seguir para o site que você deseja gerenciar com o Web Studio: `ddc1.studio.local` e `ddc2.studio.local`. Execute o seguinte comando do PowerShell:

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

> **Nota:**
>
> - A ferramenta requer permissões de administrador do computador.

> - As alterações na configuração do Delivery Controller podem não entrar em vigor imediatamente devido às configurações em cache no servidor IIS. Para efeito imediato, acesse o servidor Web Studio, abra Internet Information Services (IIS) Manager, navegue até Start Page > Sites > Default Web Site e selecione **Restart** no painel Manage Website.

Configurar o Web Studio como um proxy para Delivery Controllers (opcional)

Por padrão, ao gerenciar sua implantação usando o console do Web Studio, você se conecta ao servidor do Web Studio e aos Delivery Controllers por meio do navegador da Web. Oferecemos a opção de configurar o servidor Web Studio como um proxy para Delivery Controllers. Como resultado, você se conecta somente ao servidor do Web Studio ao gerenciar sua implantação.

Esta seção orienta você a configurar um servidor Web Studio como um proxy para Delivery Controllers. Presumimos que o Web Studio e os Delivery Controllers estejam instalados em servidores diferentes.

Antes de começar, verifique se você tem todos os componentes principais necessários instalados em sua implantação. Para obter mais informações, consulte Instalar componentes principais.

Para ativar o modo proxy para o Web Studio, siga estas etapas:

1. Faça backup do arquivo `manifest.json` em `C:\Program Files\Citrix\Web Studio\Site\assets\json\`.
2. No servidor Web Studio, execute o Windows PowerShell como administrador.
3. Execute o comando a seguir para substituir `fqdn_of_webstudio_machine` pelo FQDN do seu servidor Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"/
   ProxyServer fqdn_of_webstudio_machine
   ```

Para desativar o modo proxy do Web Studio, substitua `manifest.json` em `C:\Program Files\Citrix\Web Studio\Site\assets\json\` pelo arquivo `manifest.json` do qual você fez backup.

> **Nota:**
>
> Como uma boa prática, recomendamos que você proteja sua implantação do Web Studio usando um certificado público confiável externo ou uma autoridade de certificação (CA) corporativa. Para obter mais informações, consulte Proteger uma implantação do Web Studio.

Fazer login no Web Studio

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

Para fazer login no Web Studio, abra o menu Iniciar da área de trabalho e selecione **Citrix > Citrix Web Studio**. Administradores com permissões para o Web Studio devem ser usuários de domínio do Active Directory. Ao fazer login no Web Studio, considere os seguintes cenários:

- Se você ainda não especificou Delivery Controllers para o site. Você é solicitado a especificar um Delivery Controller para que tenha acesso temporário ao Web Studio.
- Se os Delivery Controllers especificados estiverem inacessíveis no momento, você não poderá fazer login no Web Studio. Teste suas conexões para garantir que esses Delivery Controllers estejam acessíveis. Ou especifique um Delivery Controller alternativo para que você tenha acesso temporário ao Web Studio.

Próximas etapas

1. Instalar VDAs
2. Use o Web Studio para fornecer aplicativos e áreas de trabalho virtuais para seus usuários por meio de:
   a) Criação de um catálogo de máquinas
   b) Criação de um grupo de entrega
   c) Criação de um grupo de aplicativos (opcional)

   As fontes de informações direcionam você para os artigos específicos do Citrix Studio (o console de gerenciamento baseado em Windows). O Citrix Studio e o Web Studio têm uma aparência diferente, mas os fluxos de trabalho para definir as configurações permanecem os mesmos (salvo indicação em contrário).

Instalar VDAs

April 3, 2024

> **Importante:**
>
> Se você estiver atualizando e sua versão atual tiver o software Personal vDisk ou AppDisks instalado, consulte Remoção de PvD, AppDisks e hosts não suportados.

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

Antes de iniciar uma instalação, consulte Preparar a instalação e complete todas as tarefas de preparação.

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

Este artigo descreve a sequência do assistente de instalação ao instalar um VDA. Equivalentes de linhas de comando são fornecidos. Para obter detalhes, consulte Instalar usando a linha de comando.

Etapa 1. Baixe o software do produto e inicie o assistente

Se você estiver usando o instalador do produto completo:

1. Se você ainda não baixou o ISO do produto:
    - Use as credenciais da sua conta da Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o arquivo ISO do produto.
    - Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.
2. Use uma conta de administrador local na imagem ou na máquina onde você está instalando o VDA. Insira o DVD na unidade ou monte o arquivo ISO. Se o instalador não for iniciado automaticamente, clique duas vezes em **AutoSelect** no aplicativo ou na unidade montada.

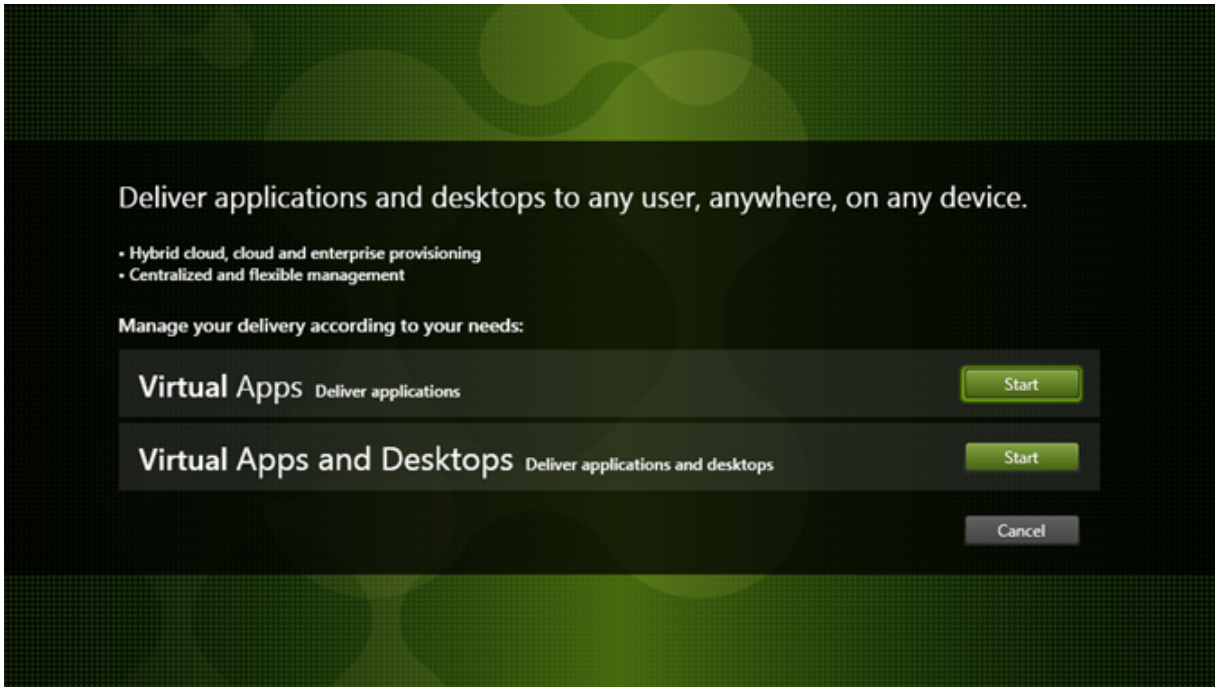
    O assistente de instalação é iniciado.

Se você estiver usando um pacote autônomo:

1. Use as credenciais da sua conta da Citrix para acessar a página de download do Citrix Virtual Apps and Desktops. Baixe o pacote apropriado:
    - `VDAServerSetup.exe`: *versão* do VDA de SO multissessão
    - `VDAWorkstationSetup.exe`: *versão* do VDA de SO de sessão única
    - `VDAWorkstationCoreSetup.exe`: *versão* do VDA de serviços principais de SO de sessão única
2. Clique com o botão direito no pacote e escolha **Executar como administrador.**

    O assistente de instalação é iniciado.

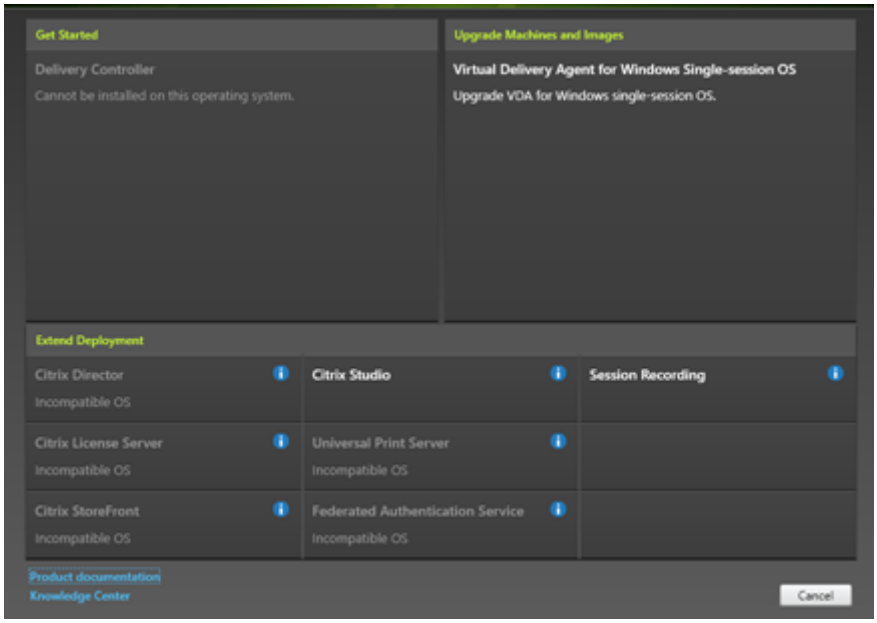
Etapa 2. Escolha qual produto instalar



Clique em **Start** ao lado do produto a ser instalado: Citrix Virtual Apps ou Citrix Virtual Desktops. (Se a máquina já tiver um componente Citrix Virtual Apps ou Citrix Virtual Desktops instalado, esta página não será exibida.)

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

Etapa 3. Selecione o VDA

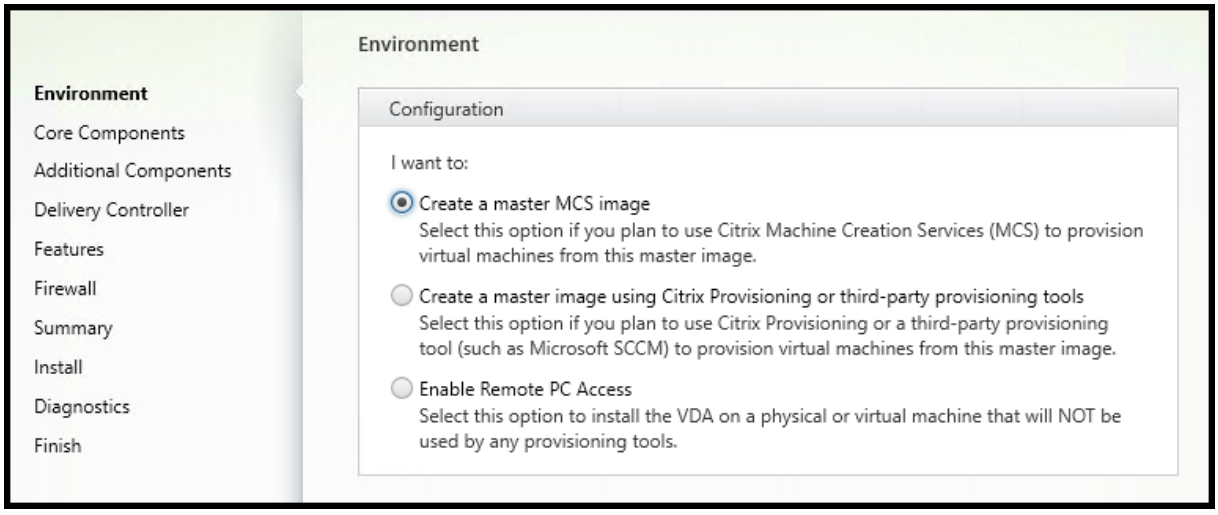


Selecione a entrada **Virtual Delivery Agent**. O instalador sabe se ele está sendo executado em um sistema operacional de sessão única ou multissessão, senso assim oferece apenas o tipo de VDA apropriado.

Por exemplo, quando você executa o instalador em uma máquina Windows Server 2016, a opção de VDA para SO multissessão está disponível. A opção VDA para SO de sessão única não é oferecida.

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

Etapa 4. Especifique como o VDA será usado



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

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

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

Escolha uma das seguintes opções:

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

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

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

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

  Opção de linha de comando: `/masterpvsimage`

- (Aparece apenas em máquinas de SO multissessão) **Enable brokered connections to a server:**

selecione esta opção para instalar um VDA em uma máquina física ou virtual que não é usada como uma imagem para provisionar outras máquinas.

Opção de linha de comando: `/remotepc`

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

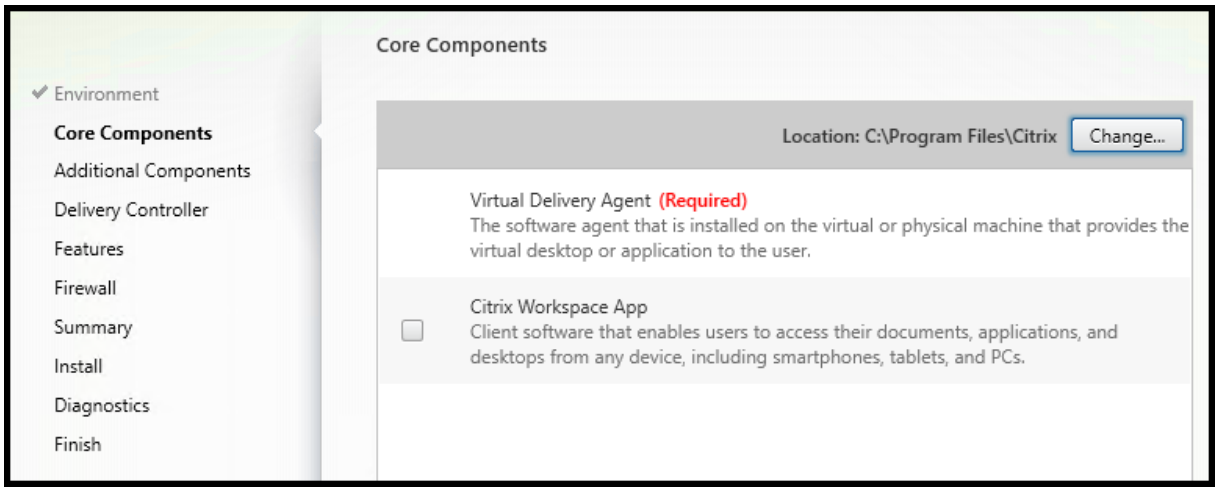
  Opção de linha de comando: `/remotepc`

Clique em **Avançar**.

Esta página não aparece:

- Se você estiver atualizando um VDA
- Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`

Etapa 5. Selecione os componentes para instalar e o local de instalação



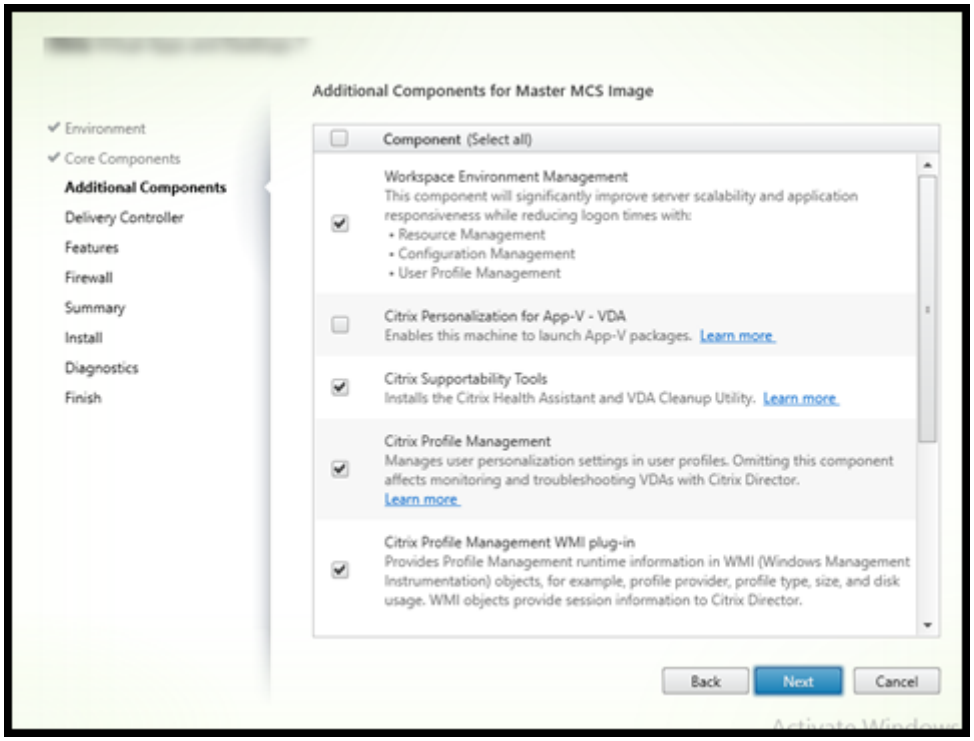
Na página **Core components**:

- **Location:** por padrão, os componentes são instalados em `C:\Program Files\Citrix`. Esse padrão é adequado para a maioria das implantações. Se você especificar um local diferente, tal local deverá ter permissões de execução para o serviço de rede.
- **Components:** por padrão, o aplicativo Citrix Workspace para Windows não é instalado com o VDA. Se você estiver usando o instalador `VDAWorkstationCoreSetup.exe`, o aplicativo Citrix Workspace para Windows nunca será instalado, portanto, essa caixa de seleção não 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. Instale componentes adicionais



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

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

Página Additional Components	Página Environment: “Master image with MCS”ou “Master image with Citrix Provisioning” selecionado	Página Environment: “Enable brokered connections to server”(para SO multissessão) ou “Remote PC Access”(para SO de sessão única) selecionado
Citrix Personalization for App-V	Não selecionado	Não selecionado
User Personalization Layer	Não selecionado	Não é mostrado porque não é válido para este caso de uso.
Citrix Profile Management	Selecionado	Não selecionado
Citrix Profile Management WMI Plug-in	Selecionado	Não selecionado

Página Additional Components	Página Environment: “Master image with MCS”ou “Master image with Citrix Provisioning” selecionado	Página Environment: “Enable brokered connections to server”(para SO multissessão) ou “Remote PC Access”(para SO de sessão única) selecionado
Citrix VDA Upgrade Agent	Não selecionado	Não selecionado
Citrix Files para Windows	Não selecionado	Não selecionado
Citrix Files para Outlook	Não selecionado	Não selecionado
MCSIO write cache for storage optimization	Não selecionado	Não selecionado
Rendezvous protocol configuration	Não selecionado	Não selecionado

Esta página não aparece se:

- Você está usando o instalador `VDAWorkstationCoreSetup.exe`. Além disso, as opções de linha de comando para os componentes adicionais não são válidas com esse instalador.
- Você está atualizando um VDA e todos os componentes adicionais já estão instalados. Se alguns dos componentes adicionais já estiverem instalados, a página listará apenas os componentes que não estão instalados.

Marque ou desmarque as seguintes caixas de seleção. (Os componentes podem aparecer em uma ordem diferente no instalador.)

- **Citrix Personalization for App-V:** instale este componente se usar aplicativos de pacotes do Microsoft App-V. Para obter detalhes, consulte Implementar e entregar aplicativos App-V.

  Opção de linha de comando: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar a instalação de componentes, `/exclude "Citrix Personalization for App-V – VDA"` para prevenir a instalação de componentes

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

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

  Opção de linha de comando: `/includeadditional "User Personalization Layer"` para habilitar a instalação de componentes, `/exclude "User Personalization Layer"` para prevenir a instalação de componentes

- **Citrix Profile Management:** este componente gerencia as configurações de personalização do usuário em perfis de usuário. Para obter detalhes, consulte Profile Management.

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

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

  Opção de linha de comando: `/includeadditional "Citrix Profile Management "` para habilitar a instalação de componentes, `/exclude "Citrix Profile Management "` para prevenir a instalação de componentes

- **Citrix Profile Management WMI plug-in:** este plug-in fornece informações de runtime do Profile Management em objetos WMI (Instrumentação de Gerenciamento do Windows) (por exemplo, provedor de perfil, tipo de perfil, tamanho e uso do disco). Objetos WMI fornecem informações da sessão ao Director.

  Opção de linha de comando: `/includeadditional "Citrix Profile Management WMI Plugin"` para habilitar a instalação de componentes, `/exclude "Citrix Profile Management WMI Plugin"` para prevenir a instalação de componentes

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

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

- **Citrix Files for Windows:** este componente permite que os usuários se conectem à conta do Citrix Files. Assim, eles podem interagir com o Citrix Files por meio de uma unidade mapeada no sistema de arquivos Windows (sem exigir uma sincronização completa de seu conteúdo). Para obter mais informações, consulte Content Collaboration.

  Opções de linha de comando: `/includeadditional "Citrix Files for Windows "` para ativar a instalação de componentes, `/exclude "Citrix Files for Windows"` para impedir a instalação de componentes

- **Citrix Files for Outlook:** o Citrix Files for Outlook permite ignorar restrições de tamanho de arquivo e adicionar segurança aos anexos ou e-mails enviando-os através do Citrix Files. Você

pode fornecer uma solicitação de upload seguro de arquivos para colegas de trabalho, clientes e parceiros diretamente no seu e-mail. Para obter mais informações, consulte Content Collaboration.

Opções de linha de comando: `/includeadditional "Citrix Files for Outlook "` para ativar a instalação de componentes, `/exclude "Citrix Files for Outlook"` para impedir a instalação de componentes

- **MCSIO write cache for storage optimization:** Instala o driver Citrix MCS IO. Para obter mais informações, consulte Armazenamento compartilhado por hipervisores e Configurar cache para dados temporários.

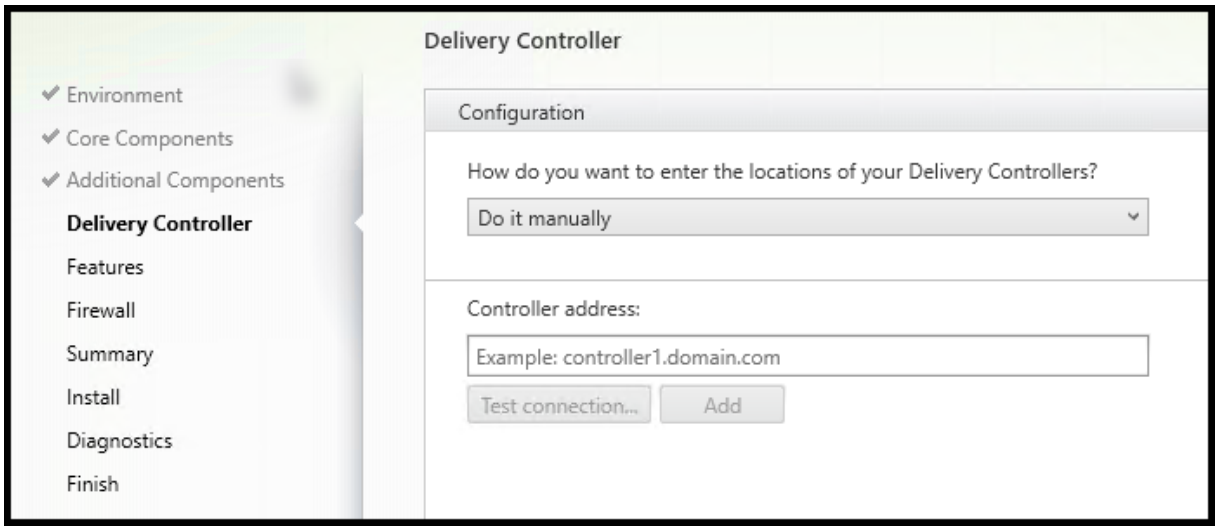
  Opções de linha de comando: `/includeadditional "Citrix MCS IODriver"` para ativar a instalação de componentes, `/exclude "Citrix MCS IODriver"` para impedir a instalação de componentes

- **Rendezvous Proxy Configuration:** instale este componente se você planeja usar o protocolo Rendezvous com o Citrix Gateway Service em seu ambiente e tem um proxy não transparente em sua rede para as conexões de saída. Somente proxies HTTP são aceitos.

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

  Opção de linha de comando: `/includeadditional "Citrix Rendezvous V2"` para habilitar a instalação de componentes, `/exclude "Citrix Rendezvous V2"` para prevenir a instalação de componentes

Etapa 7. Endereços do Delivery Controller



Na página **Delivery Controller**, escolha como deseja inserir os endereços dos Controllers instalados. A Citrix recomenda que você especifique os endereços durante a instalação do VDA (**Do it manually**). O VDA não pode se registrar com um Controller até que tenha a informação. Se um VDA não puder se registrar, os usuários não poderão acessar aplicativos e áreas de trabalho nesse VDA.

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

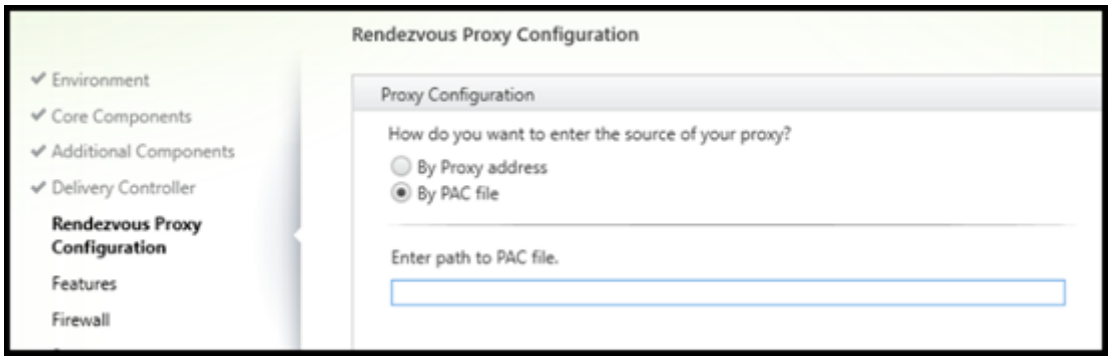
Clique em **Avançar**. Se selecionou **Do it later (Advanced)**, você será solicitado a confirmar que especificará os endereços do Controller posteriormente.

Outras considerações:

- O endereço não pode conter caracteres não alfanuméricos.
- Se você especificar endereços durante a instalação do VDA e na política de grupo, as configurações da política substituem as configurações fornecidas durante a instalação.
- O registro bem-sucedido do VDA exige que as portas de firewall usadas para se comunicar com o Controller estejam abertas. Essa ação é ativada por padrão na página **Firewall** do assistente.
- Depois de especificar as localizações do Controller (durante ou após a instalação do VDA), você pode usar o recurso de atualização automática para atualizar os VDAs quando os Controllers forem adicionados ou removidos. Para obter detalhes sobre como os VDAs descobrem e se registram em Controllers, consulte VDA registration.

Opção de linha de comando: `/controllers`

Etapa 8. Rendezvous Proxy Configuration



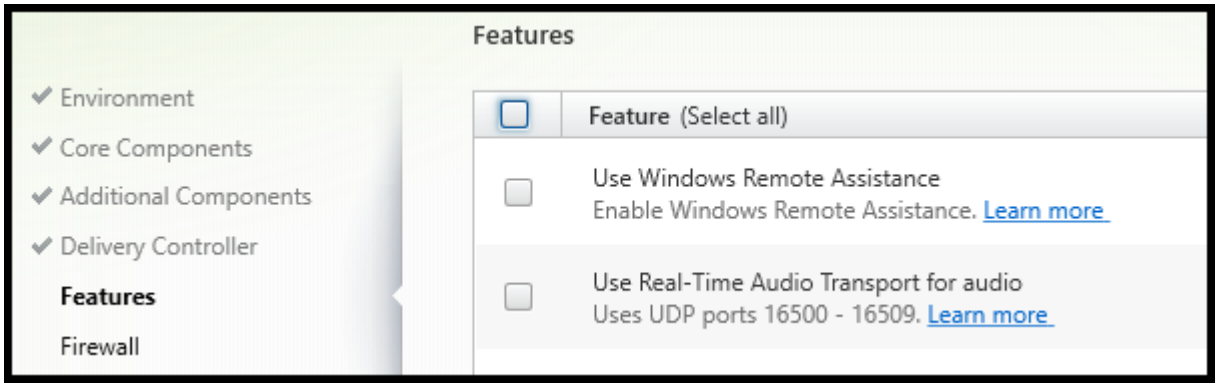
A página **Rendezvous Proxy Configuration** é exibida apenas se você marcar a caixa de seleção **Rendezvous Proxy Configuration** na página **Additional Components**.

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

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

Opção de linha de comando: `/proxyconfig`

Etapa 9. Ativar ou desativar recursos



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

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

  Opção de linha de comando: `/enable_remote_assistance`

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

  Opção de linha de comando: `/enable_real_time_transport`

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

  Opção de linha de comando: `/enable_ss_ports`

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

  Opção de linha de comando: `/xendesktopcloud`

Se esta página contiver um recurso chamado **MCS I/O**, não o use. O recurso MCS IO é configurado na página **Additional Components**.

Clique em **Avançar**.

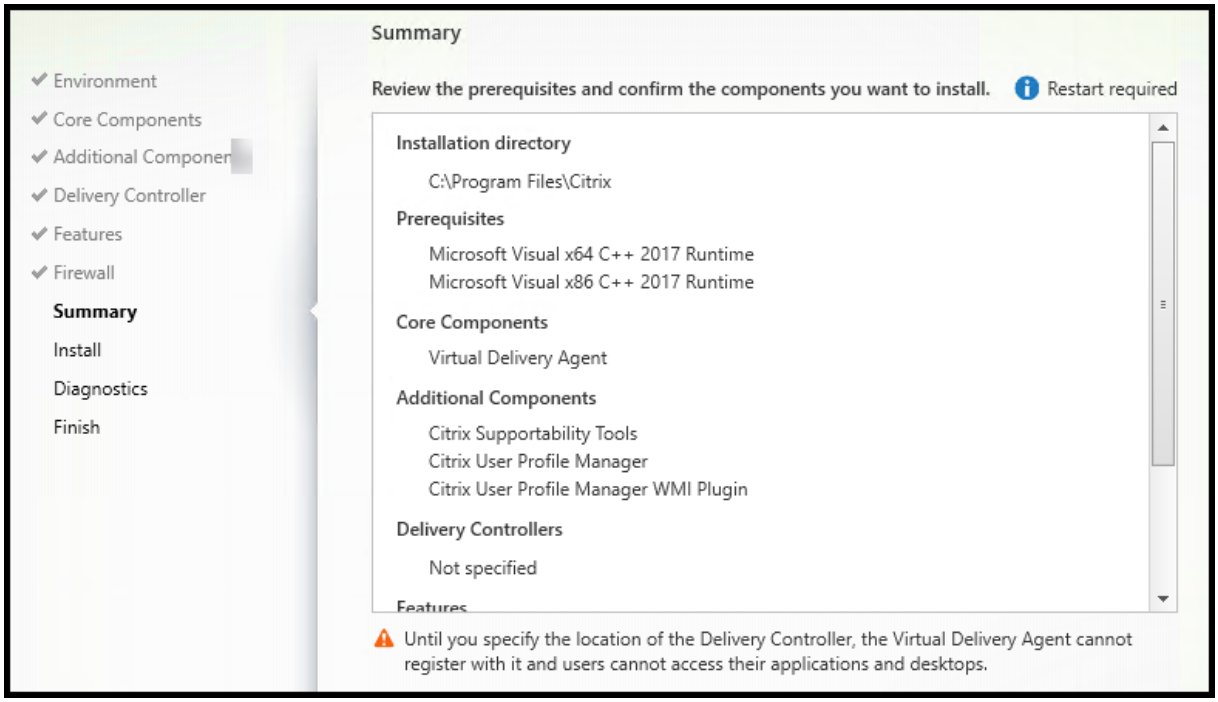
Etapa 10. Portas de firewall

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

Clique em **Avançar**.

Opção de linha de comando: `/enable_hdx_ports`

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



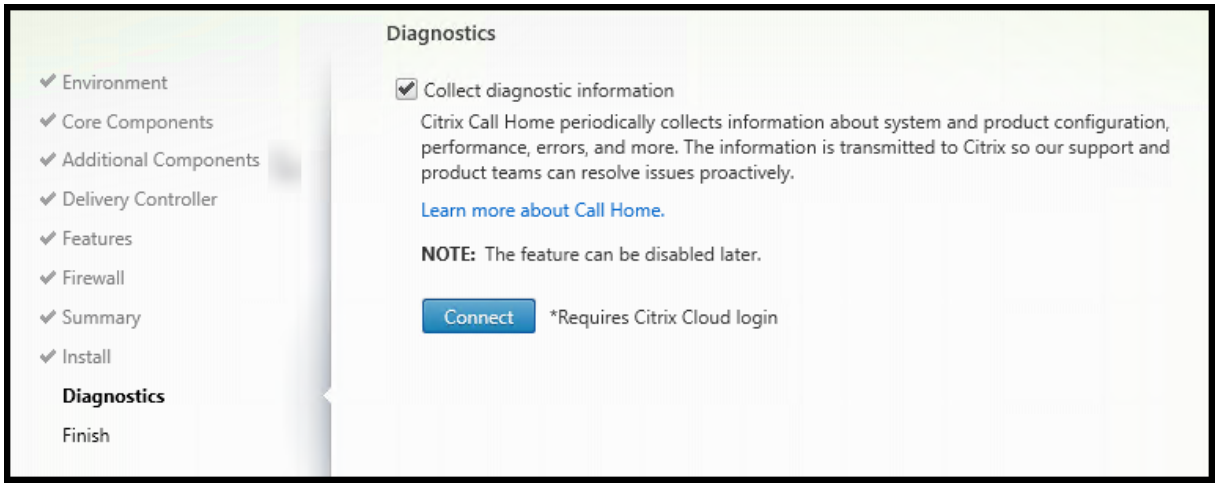
A página **Summary** lista o que será instalado. Use o botão **Back** para retornar às páginas anteriores do assistente e alterar as seleções.

(Somente VDAs de sessão única) Marque a caixa de seleção **Enable automatic restore if update fails** para habilitar o recurso de restauração em caso de falha. Para obter detalhes, consulte Restaurar em caso de falha de instalação ou atualização.

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

Se os pré-requisitos ainda não estiverem instalados ou ativados, a máquina poderá reinicializar uma ou mais vezes. Consulte Preparar a instalação.

Etapa 12. Diagnóstico



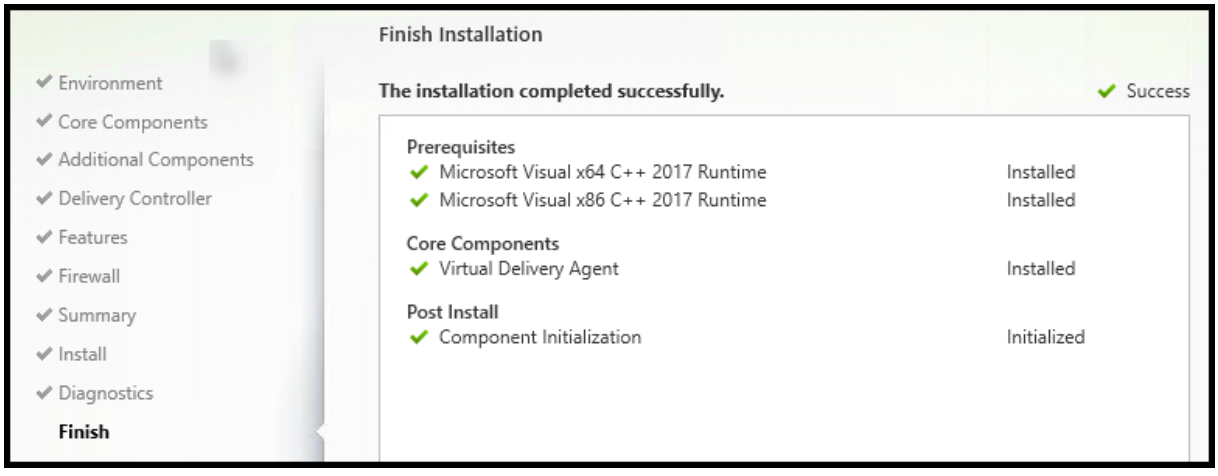
Na página **Diagnostics**, escolha se deseja participar do Citrix Call Home. Se você optar por participar (o padrão), clique em **Connect**. Quando solicitado, insira as credenciais da sua conta da Citrix.

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

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

Para obter mais informações, consulte Call Home.

Etapa 13. Conclua a instalação



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

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

Próximas etapas

Repita o procedimento acima para instalar VDAs em outras máquinas ou imagens, se necessário.

Depois de instalar todos os VDAs, inicie o Studio. Se você ainda não criou um site, o Studio o guiará automaticamente para essa tarefa. Depois disso, o Studio o guiará para criar um catálogo de máquinas e, em seguida, um grupo de entrega. Veja:

- 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.

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

Personalizar um VDA

Para personalizar um VDA instalado:

1. No recurso do Windows para remover ou alterar programas, selecione **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Em seguida, clique com o botão direito e selecione **Alterar**.
2. Selecione **Customize Virtual Delivery Agent Settings**. Quando o instalador for iniciado, você pode alterar:
    - Endereços do Controller
    - Porta TCP/IP para registrar no Controller (padrão = 80)
    - Se as portas do Firewall do Windows devem ser abertas automaticamente

Solucionar problemas

- Para obter informações sobre como a Citrix reporta o resultado de instalações de componentes, consulte Códigos de retorno da instalação Citrix.
- Na tela do Studio de um grupo de entrega, a entrada **Installed VDA version** no painel **Details** pode não refletir a versão instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou uma área de trabalho aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Instalar usando a linha de comando

September 13, 2023

> **Importante:**
>
> - Se você estiver atualizando e sua versão atual usa ou tiver o software Personal vDisk ou AppDisks instalado, consulte Remover PvD, AppDisks e hosts não suportados.
> - A Citrix coleta dados básicos de licenciamento conforme necessário para seus interesses legítimos, incluindo conformidade de licenciamento. Para obter mais informações, consulte Citrix Licensing Data.

Introdução

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

Este artigo descreve como emitir comandos de instalação de produto. Antes de iniciar qualquer instalação, revise Preparar a instalação. Este artigo inclui descrições dos instaladores disponíveis.

Para ver o progresso da execução do comando e os valores de retorno, você deve ser o administrador original ou usar a opção **Executar como administrador**. Para obter mais informações, consulte a documentação sobre comandos da Microsoft.

Como complemento ao uso dos comandos de instalação diretamente, são fornecidos scripts de exemplo no ISO do produto que instalam, atualizam ou removem VDAs em máquinas no Active Directory. Para obter detalhes, consulte Instalar VDAs usando scripts.

Se você tentar instalar ou atualizar em uma versão do sistema operacional Windows que não é compatível com esta versão do Citrix Virtual Apps and Desktops, uma mensagem lhe fornecerá informações sobre suas opções. Veja Sistemas operacionais anteriores.

Para obter informações sobre como a Citrix reporta o resultado de instalações de componentes, consulte Códigos de retorno da instalação Citrix.

Usar o instalador de produto completo

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

1. Baixe o pacote de produtos da Citrix. As credenciais da conta da Citrix são necessárias para acessar o site de download.
2. Descompacte o arquivo. Opcionalmente, grave um DVD do arquivo ISO.
3. Faça logon no servidor onde está instalando os componentes usando uma conta de administrador local.
4. Insira o DVD na unidade ou monte o arquivo ISO.
5. No diretório `\x64\XenDesktop Setup` na mídia, execute o comando apropriado.

   Para instalar 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 Serviço de autenticação federada: a Citrix recomenda o uso da interface gráfica.

   Para instalar o Session Recording: siga as orientações em Session Recording.

   Para instalar o Workspace Environment Management: siga as orientações em Workspace Environment Management.

Opções de linha de comando para instalar componentes principais

As seguintes opções de parâmetros são válidas ao instalar componentes principais com o comando `XenDesktopServerSetup.exe`. Para obter mais detalhes sobre as opções, consulte Instalar componentes principais.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] ...

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

  - `DIAGNOSTIC`: escolha esse valor para permitir que o Citrix Licensing colete dados do Call Home.
  - `ANONYMOUS`: escolha esse valor para permitir que o Citrix Licensing colete dados CEIP não identificados (que não identificam usuários).
  - `NONE`: escolha esse valor para desativar a coleção de dados do CEIP pelo Citrix Licensing.

  Para obter mais informações sobre a coleta de dados do Call Home, consulte Citrix Licensing Call Home.

  Para obter mais detalhes sobre a coleta de dados do CEIP, consulte o Programa de Aperfeiçoamento da Experiência do Usuário do Citrix Licensing.

  Para obter mais detalhes sobre os dados do CEIP, consulte Elementos de dados do Citrix Licensing CEIP.

  Para obter mais detalhes sobre os dados de licenciamento do servidor de licenças, consulte os Dados do Citrix Licensing.

- **/components** *componente* [,*componente*] ...

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

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server

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

  (Nas versões anteriores a 2003, os valores válidos incluíam `STOREFRONT`. Para a versão 2003 e posterior, use o comando de instalação dedicado do StoreFront mencionado em Usar o instalador completo do produto).

- **/configure_firewall**

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

- **/disableexperiencemetrics**

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

- **/exclude** "*recurso*"[,"*recurso*"]

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

  - `"Local Host Cache Storage (LocalDB)"`: impede a instalação do banco de dados usado para o Cache de host local. Esta opção não afeta se a instalação do SQL Server Express é realizada para usar como banco de dados do site ou não.

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

  Exibe a ajuda do comando.

- **/ignore_hw_check_failure**

  Permite que a instalação ou atualização do Delivery Controller continue, mesmo que as verificações de hardware falhem (por exemplo, devido à RAM insuficiente). Para obter mais informações, consulte Verificação de hardware.

- **/ignore_site_test_failure**

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

  Durante uma atualização, esta opção é ignorada se uma versão do SQL Server não suportada for detectada. Para obter detalhes, consulte Verificação de versão do SQL Server.

- **/installdir *diretório***

  Diretório vazio existente onde os componentes serão instalados. Padrão = c:\Program Files\Citrix.

- **/logpath *caminho***

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

- **/no_remote_assistance**

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

- **/noreboot**

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

- **/noresume**

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

- **/nosql**

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

  Esta opção não tem efeito na instalação do SQL Server Express LocalDB usado para o cache de host local.

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

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

- **/remove**

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

- **/removeall**

  Remove todos os componentes principais instalados.

- **/sendexperiencemetrics**

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

- **/tempdir** *diretório*

  Diretório que mantém os arquivos temporários durante a instalação. Padrão = c:\Windows\Temp.

- **/xenapp**

  Instala o Citrix Virtual Apps. Se esta opção for omitida, o Citrix Virtual Apps and Desktops será instalado.

Exemplos de instalação de componentes principais

O comando a seguir instala um Delivery Controller, Studio, Citrix Licensing e SQL Server Express em um servidor. As portas de firewall necessárias para comunicações de componentes são abertas automaticamente.

```
\x64\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 de componentes são abertas automaticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

Usar um instalador autônomo de VDA

As credenciais da conta da Citrix são necessárias para acessar o site de download. Você deve ter privilégios administrativos elevados antes de iniciar a instalação ou usar **Executar como administrador**.

1. Baixe o pacote apropriado da Citrix:

   - Virtual Delivery Agent de SO multissessão: `VDAServerSetup_xxxx.exe`
   - Virtual Delivery Agent de SO de sessão única: `VDAWorkstationSetup_xxxx.exe`
   - Virtual Delivery Agent de serviços principais de SO de sessão única: `VDAWorkstationCoreSetup_x.exe`

2. Extraia os arquivos do pacote para um diretório existente primeiro e, em seguida, execute o comando de instalação, ou simplesmente execute o pacote.

   Para extrair os arquivos antes de instalá-los, use `/extract` com o caminho absoluto, por exemplo, `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. O diretório deve existir. Caso contrário, a extração falhará. Depois, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

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

- Para `VDAWorkstationSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

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

Se você estiver familiarizado com o instalador do produto completo:

- Execute o instalador autônomo `VDAServerSetup.exe` ou `VDAWorkstationSetup.exe` como se fosse o comando `XenDesktopVdaSetup.exe` em tudo, exceto em 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_x.exe`.

Para obter mais detalhes sobre as opções, consulte Instalar VDAs.

- **/components** *componente*[,*componente*]

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

  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: Aplicativo Citrix Workspace para Windows

  Para instalar o VDA e aplicativo Citrix Workspace para Windows, especifique `/components vda,plugins`.

  Se esta opção for omitida, somente o VDA será instalado (o aplicativo Citrix Workspace não).

  Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup_xxxx.exe`. Esse instalador não pode instalar o aplicativo Citrix Workspace.

- **/controllers** "*controller* [*controller*]"

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

- **/disableexperiencemetrics**

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

- **/enable_hdx_ports**

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

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

- **/enable_hdx_udp_ports**

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

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

- **/enable_real_time_transport**

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

- **/enable_remote_assistance**

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

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

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

  Se a instalação/atualização for concluída com sucesso:

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

  Para obter detalhes, consulte Restaurar em caso de falha de instalação ou atualização.

- **/enable_ss_ports**

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

- **/exclude** "*componente*"["*componente*"]

  Impede a instalação de um ou mais componentes opcionais separados por vírgula, cada qual entre aspas retas normais. Por exemplo, instalar ou atualizar um VDA em uma imagem que não é gerenciada pelo MCS não requer o componente Machine Identity Service. Os valores válidos são os seguintes:

SO multissessão	SO de sessão única	Serviços principais de SO de sessão única
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 Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in

SO multissessão	SO de sessão única	Serviços principais de SO de sessão única
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	`VDA WMI Proxy Plug-in`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	

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

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

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

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

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

  Exibe a ajuda do comando.

- **/includeadditional** "*componente*"[,"*componente*"]

  Inclui a instalação de um ou mais componentes opcionais separados por vírgula, cada qual entre aspas retas normais. Esta opção é útil quando você estiver criando uma implantação do

Remote PC Access e quiser instalar outros componentes que não estão incluídos por padrão. Os valores válidos são os seguintes:

SO multissessão	SO de sessão única
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization 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 VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

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

- **/installdir** *diretório*

  Diretório vazio existente onde os componentes serão instalados. Padrão = c:\Program Files\Citrix.

- **/install_mcsio_driver**

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

- **/logpath** *caminho*

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

  Esta opção não está disponível na interface gráfica.

- **/masterimage**

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

Esta opção não é válida quando usar o instalador `VDAWorkstationCoreSetup_xxxx.exe`.

- **/mastermcsimage**

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

- **/masterpvsimage**

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

- **/no_mediafoundation_ack**

  Reconhece que o Microsoft Media Foundation não está instalado, e vários recursos multimídia HDX não serão instalados e não funcionarão. Se essa opção for omitida e o Media Foundation não estiver instalado, a instalação do VDA será encerrada, pois as pré-condições não foram atendidas. A maioria das edições compatíveis do Windows vem com o Media Foundation já instalado, exceto as edições N. Se você ativar Recursos do Windows > Recursos de mídia *manualmente*, a chave de registro procurada pelo Citrix Meta Installer pode não ter um valor definido. Verifique a chave de registro `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` antes de iniciar o processo de instalação para confirmar se o valor existe e não está vazio.

- **/nodesktopexperience**

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

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

- **/noreboot**

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

- **/noresume**

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

- **/physicalmachine**

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

- **/portnumber** *porta*

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

- **/proxyconfig** "*endereço ou caminho do arquivo PAC*"

  Válido somente se o comando contiver /includeadditional "Citrix Rendezvous V2". O endereço ou o caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para obter detalhes do recurso, consulte Protocolo Rendezvous.

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

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

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

- **/reconfigure**

  Personaliza as configurações de VDA definidas anteriormente quando utilizado com as opções /portnumber, /controllers ou /enable_hdx_ports. Se você especificar esta opção sem também especificar a opção /quiet, a interface gráfica para personalizar o VDA é iniciada.

- **/remotepc**

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

  Esta opção não é válida quando usar o instalador VDAWorkstationCoreSetup.exe. Esse instalador exclui automaticamente a instalação destes componentes.

  /remotepc não é compatível com a opção /servervdi.

- **/remove**

  Remove os componentes especificados com a opção /components.

- **/remove_appdisk_ack**

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

- **/remove_pvd_ack**

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

- **/removeall**

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

- **/sendexperiencemetrics**

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

- **/servervdi**

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

  Antes de usar essa opção, consulte VDI do servidor.

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

- **/site_guid** *guid*

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

- **/tempdir** *diretório*

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

  Esta opção não está disponível na interface gráfica.

- **/virtualmachine**

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

  Esta opção não está disponível na interface gráfica.

- **/xendesktopcloud**

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

Exemplos de instalação de um VDA

Instalar um VDA com o instalador de produto completo:

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

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

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

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

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Personalizar um VDA

Depois de instalar um VDA, você pode personalizar várias configurações. No `\x64\XenDesktop Setup` diretório na mídia do produto, execute `XenDesktopVdaSetup.exe`, usando uma ou mais das seguintes opções, descritas em opções de linha de comando para instalar um VDA.

- `/reconfigure` (necessário quando personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Solucionar problemas de VDAs

- Na tela do Studio de um grupo de entrega, a entrada **Installed VDA version** no painel **Details** pode não refletir a versão instalada nas máquinas. A exibição de Programas e Recursos do Win-

dows da máquina mostra a versão real do VDA.

- Depois que um VDA é instalado, ele não pode entregar aplicativos ou uma área de trabalho aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Opções de linha de comando para instalar um Servidor de Impressão Universal

A seguinte opção é válida com o comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

Software	Pasta	Nome do arquivo
Microsoft Visual C++ 2017 Runtime, 32 bits e 64 bits	**Support > VcRedist_2017**	`vcredist_x64.exe` e `vcredist_x86.exe`
Citrix Diagnostic Facility	x64 > Virtual Desktop Components	`cdf_x64.msi`
Componente de servidor Universal Print Server	x64 > Universal Print Server	`UpsServer_x64.msi`

Quando esta opção não for especificada, o instalador exibe a página de **Firewall** a partir da interface gráfica. Selecione **Automatically** para que o instalador adicione automaticamente as regras de firewall do Windows, ou **Manually** para permitir que o administrador configure manualmente o firewall.

Depois de instalar o software em seus servidores de impressão, configure o Universal Print Server seguindo as instruções em Provisionar impressoras.

Mais informações

Para obter informações sobre como a Citrix reporta o resultado de instalações de componentes, consulte Códigos de retorno da instalação Citrix.

Instalar VDAs usando scripts

June 28, 2023

> **Nota:**
>
> A Citrix não é responsável por problemas causados por scripts que são adaptados para corresponder aos ambientes de produção do cliente. Para qualquer problema relacionado à instalação da Citrix, abra um caso de suporte técnico com os logs de instalação relevantes usando o portal de suporte Citrix.

Este artigo aplica-se à instalação de VDAs em máquinas com sistemas operacionais Windows. Para obter informações sobre sistemas operacionais VDAs para Linux, consulte a documentação do Linux Virtual Delivery Agent .

A mídia de instalação contém exemplos de scripts que instalam, atualizam ou removem Virtual Delivery Agents (VDA) de máquinas no Active Directory. Você também pode usar os scripts para fazer a manutenção das imagens mestre usadas por Machine Creation Services e Citrix Provisioning (anteriormente Provisioning Services).

Acesso necessário:

- Os scripts precisam de acesso Todos Leem ao compartilhamento de rede onde o comando de instalação VDA está localizado. O comando de instalação é `XenDesktopVdaSetup.exe` no ISO do produto completo, ou `VDAWorkstationSetup.exe` ou `VDAServerSetup.exe` em um instalador autônomo.
- Os detalhes de log são armazenados em cada máquina local. Para registrar resultados centralmente para revisão e análise, os scripts precisam de acesso Todos Leem/Gravam 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 de script, o log do instalador e os logs de instalação do MSI. Cada tentativa de instalação ou remoção é gravada 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 para pesquisar localmente nas máquinas de destino.

Antes de iniciar uma instalação, leia e complete as tarefas em Preparar a instalação.

Instalar ou atualizar VDAs usando o script

1. Obtenha o script de exemplo **InstallVDA.bat** em \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 para instalar: `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` estão incluídas por padrão no script e são necessárias: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.

3. Usando scripts de inicialização de políticas de grupo, atribua o script à unidade organizacional que contém suas máquinas. Essa UO deve conter somente máquinas nas quais você deseja instalar o VDA. Quando as máquinas nessa UO são reinicializadas, o script é executado em todas elas. Um VDA é instalado em cada máquina que possui um sistema operacional suportado.

Remover VDAs usando o script

1. Obtenha o script de exemplo UninstallVDA.bat em \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 para remover: `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 scripts de inicialização de políticas de grupo, atribua o script à unidade organizacional que contém suas máquinas. Essa UO deve conter somente máquinas das quais você deseja remover o VDA. Quando as máquinas na UO são reinicializadas, 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 segundos após o início da implantação. Você pode verificar se o processo em geral está

funcionando. Se o log não for copiado para o compartilhamento de log central como esperado, inspecione a máquina local mais detalhadamente. O script coloca dois arquivos de log de depuração na pasta `%temp%` de cada máquina:

- `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
- `VDA_Install_ProcessLog_<DateTimeStamp>.log`

Revise os logs para assegurar-se de que o script:

- Está em execução como esperado.
- Detecta adequadamente o sistema operacional de destino.
- Está configurado corretamente para apontar para `ROOT` do compartilhamento `DEPLOYSHARE` (contém o arquivo chamado `AutoSelect.exe`).
- É capaz de se autenticar nos dois compartilhamentos: `DEPLOYSHARE` e `LOG`.

- Para obter informações sobre como a Citrix reporta o resultado de instalações de componentes, consulte Códigos de retorno da instalação Citrix.
- Na tela do Studio de um grupo de entrega, a entrada **Installed VDA version** no painel **Details** pode não refletir a versão instalada nas máquinas. A exibição de programas e recursos da máquina mostra a versão real do VDA.
- Depois que um VDA é instalado, ele não pode entregar aplicativos ou uma área de trabalho aos usuários até que se registre em um Delivery Controller.

  Para saber mais sobre os métodos de registro de VDA e como solucionar problemas de registro, consulte Registro de VDA.

Instalar VDAs usando SCCM

June 28, 2023

> **Nota:**
>
> A Citrix não é responsável por problemas 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 qualquer problema relacionado à instalação da Citrix, abra um caso de suporte técnico com os logs de instalação relevantes usando o portal de suporte Citrix.

Visão geral

Para implantar com êxito um Virtual Delivery Agent (VDA) usando o Microsoft System Center Configuration Manager (SCCM) ou ferramentas de distribuição de software semelhantes, a Citrix recomenda o uso do instalador do VDA em uma sequência de etapas.

A Citrix não recomenda o uso do VDA Cleanup Utility como parte de uma instalação ou atualização de VDA. Use o VDA Cleanup Utility somente na eventualidade de o instalador do VDA ter falhado anteriormente.

Reinicializações

O número necessário de reinicializações durante a instalação do VDA depende do ambiente. Por exemplo:

- Uma reinicialização pode ser necessária no caso de atualizações pendentes, ou reinicializações das instalações de software anteriores podem ocorrer.
- Além disso, arquivos previamente bloqueados por outros processos podem precisar de atualizações, forçando uma reinicialização extra.
- Alguns componentes opcionais no instalador de VDA (como o Citrix Profile Management e o Citrix Files) podem exigir uma reinicialização.

O SCCM Task Sequencer gerencia todas as reinicializações necessárias.

Definir a sequência de tarefas

Depois de identificar todos os pré-requisitos e reinicializações, use o sequenciador de tarefas do SCCM para:

- O VDA pode ser instalado a partir de uma cópia acessível da mídia de instalação ou usando um dos instaladores autônomos de VDA:
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  Para obter mais informações sobre instaladores de VDA, consulte Instaladores.
- Ao atualizar um VDA, a máquina na qual ele está instalado deve estar no modo de manutenção, sem sessões.
- Quando uma instalação de VDA é executada pela primeira vez em uma máquina, o instalador de VDA que está sendo usado é copiado para essa máquina.

  - Quando usar um instalador de VDA diferente de `VDAWorkstationCoreSetup_XXXX.exe`, o instalador de VDA será copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
  - Quando usar `VDAWorkstationCoreSetup_XXXX.exe`, o instalador de VDA será copiado para `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.

‘

- A localização do diretório do instalador de VDA também é armazenada no registro “`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall`” “`MetaInstallerInstallLocat`”.
- Adicione as opções de linha de comando `/NOREBOOT`, `/NORESUME` e `/QUIET` às suas opções de linha de comando.
  - `/QUIET`: não mostra a interface do usuário durante a instalação, para que o SCCM tenha controle do processo de instalação.
  - `/NOREBOOT`: impede o instalador de VDA de reiniciar automaticamente. Os gatilhos do SCCM são reiniciados quando necessário.
  - `/NORESUME`: normalmente, 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 é reinicializada, o Windows usa a chave para iniciar o instalador de VDA. Esse 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. **SCCM TASK1:** Reinicializar a máquina para prepará-la.
2. **SCCM TASK2:** Iniciar a instalação do VDA.
   a) Adicione as opções `/quiet`, `/noreboot` e `/noresume` às suas opções de linha de comando.
   b) Execute o instalador 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 foi concluída e é necessária reinicializar.
      - Se um código de retorno for 3, reinicie a máquina e passe o controle para SCCM TASK3.
3. **SCCM TASK3:** Continuar a instalação do VDA.

a) Se SCCM TASK2 não retornar 0 ou 8, a instalação continuará após a conclusão da reinicialização.
b) O SCCM TASK3 se repete até que o instalador de VDA retorne um 0 ou 8 (indicando uma instalação bem-sucedida) ou um 3 (indicando que SCCM TASK3 deve ser repetido). Trate qualquer outro código de retorno como erro; o SCCM TASK3 irá informar o erro e parar.
c) Retome a instalação do VDA executando o instalador de VDA apropriado (`XenDesktopVdaSetup.exe` na maioria dos casos, ou `XenDesktopRemotePCSetup.exe` se `VDAWorkstationCoreSe.exe` foi usado) a partir do local onde foi copiado (conforme descrito em Definir a sequência de tarefas), sem parâmetros de linha de comando. (O instalador de VDA usa os parâmetros salvos durante a primeira execução do instalador.)
d) Fique atento ao código de retorno do instalador de VDA.
    - 0 ou 8: sucesso, instalação concluída, reinicialização necessária.
    - 3: instalação não concluída. Reinicialize a máquina e repita o SCCM TASK3 até que um 0 ou 8 seja retornado. Trate qualquer outro código de retorno como erro; o SCCM TASK3 irá informar o erro e encerrar.

Para obter mais informações sobre códigos de retorno, consulte Códigos de retorno de instalação Citrix.

Exemplos de comando de instalação de VDA

As opções de instalação disponíveis variam, dependendo de qual instalador é usado. Consulte os seguintes artigos para obter detalhes da opção de linha de comando.

- Instalar VDAs
- Instalar usando a linha de comando

Comandos de instalação para Remote PC Access

- O comando a seguir usa o instalador de VDA básico de sessão única (`VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

- O comando a seguir usa o instalador de VDA completo de sessão única (`VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```


Comando de instalação para VDI dedicado

- O comando a seguir usa o instalador de 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

January 3, 2024

> **Nota:**
>
> Durante a criação do site, depois de adicionar uma licença para habilitar a Licença Hybrid Rights, 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.

Site é o nome que você dá a uma implantação do Citrix Virtual Apps and Desktops. Inclui Delivery Controllers e outros componentes principais, Virtual Delivery Agents (VDA), 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 Controller estiver instalado no Server Core, use os cmdlets do PowerShell no Citrix Virtual Apps and Desktops SDK para criar um site.

Quando cria um site, você é automaticamente registrado no Programa de Aperfeiçoamento da Experiência do Usuário (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 seu registro a qualquer momento após a criação do site. Selecione **Settings** no painel esquerdo do Web Studio e localize a configuração do **Citrix Customer Experience Improvement Program**. Para obter detalhes, consulte http://more.citrix.com/XD-CEIP.

O usuário que cria um site se torna administrador completo dele. Para obter mais informações, consulte Administração delegada.

Leia este artigo antes de criar o site para saber o que esperar.

Etapa 1. Abra o assistente de criação de sites - Citrix Site Manager

Use a ferramenta Citrix Site Manager para configurar sua implantação do Citrix Virtual Apps and Desktops (também conhecida como site). A ferramenta é instalada automaticamente quando você instala

um Delivery Controller.

Para executar essa ferramenta, abra o menu Iniciar da área de trabalho em um Delivery Controller e selecione **Citrix > Citrix Site Manager**. Consulte Instalar o Web Studio.

Etapa 2. Nome do site

Na página **Introduction**, digite um nome para o site.

Etapa 3. Banco de dados

A página **Databases** contém seleções para configurar os bancos de dados de log de site, monitoramento e configuração. Para obter detalhes sobre opções e requisitos de configuração de banco de dados, consulte Bancos de dados.

> **Nota:**
>
> Se um ouvinte Always On de SQL Server estiver configurado para criptografia TLS, você será solicitado a inserir credenciais com permissões de criação do banco de dados. As tentativas de criar o banco de dados ainda assim falham mesmo se você inserir credenciais de administrador válidas. Verifique se o certificado do SQL Server inclui o nome DNS do ouvinte na SAN (Subject Alternative Names). Para obter mais informações, consulte https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

Se você optar por instalar o SQL Server Express para usar como o banco de dados do site (o padrão), ocorre uma reinicialização após a instalação do software. Essa reinicialização não ocorre se você optar por não instalar o software SQL Server Express para usar como o banco de dados do site.

Se você não estiver usando o SQL Server Express padrão, verifique se o software SQL Server está instalado nas máquinas antes de criar um site. Os requisitos do sistema listam as versões suportadas.

Se quiser adicionar mais Delivery Controllers ao site e já tiver instalado o software do Controller em outros servidores, você pode adicionar esses Controllers a partir dessa página. Se você também planeja gerar scripts que instalam os bancos de dados, adicione os Controllers antes de gerar os scripts.

Etapa 4. Licenciamento

No **Licenciamento**, especifique o endereço do servidor de licenças e indique qual licença usar (instalar).

- Especifique o endereço do servidor de licenças no formato `name:[port]`. O campo *name* deve ser um FQDN, NetBIOS ou endereço IP. Recomenda-se um FQDN. Se você omitir o número da porta, o padrão é 27000. Clique em **Connect**. Você não pode seguir para a próxima página até que seja estabelecida uma conexão com o servidor de licenças.
- Quando a conexão for feita, **Use an existing license** estará selecionado por padrão. A exibição lista os produtos compatíveis com os quais o produto pode ser configurado baseado nas licenças atualmente instaladas.
  - Se quiser configurar este produto como um dos produtos listados (por exemplo, Citrix Virtual Apps Premium ou Citrix Virtual Desktops Premium), usando uma dessas licenças, selecione essa entrada.
  - Se você já alocou e baixou uma licença (usando Citrix Manage Licenses Tool) para usar com este produto, mas ainda não instalou a licença:
    * Clique em **Browse for license file**.
    * No explorador de arquivos, localize e selecione a licença que você baixou. Os produtos associados agora aparecem na página **Licensing** do assistente de criação de 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 isso, o servidor de licenças deve ter acesso à Internet. Você deve ter o código de acesso da licença do produto desejado. A Citrix envia o código para você por e-mail.
    * Clique em **Allocate and download**.
    * Na caixa de diálogo **Allocate Licenses**, insira o código de acesso da licença enviado pela Citrix. Clique em **Allocate licenses**.
    * Os produtos associados à nova licença aparecem na página **Licensing** do assistente de criação de site. Selecione a entrada que deseja usar.

    Alternativamente, selecione **Use the free 30-day trial** e instale as licenças mais tarde. Para obter detalhes, consulte a documentação de licenciamento.

Etapa 5. Resumo

A página **Summary** lista as informações que você especificou. Use o botão **Back** se quiser mudar algo. Quando terminar, clique em **Concluir**.

Mais informações

Conexão de host, rede e armazenamento

Se estiver usando VMs em um hipervisor ou outro serviço para fornecer aplicativos e áreas de trabalho, você pode, opcionalmente, criar a primeira conexão com esse host. Você também pode especificar recursos de armazenamento e rede para essa conexão. Depois de criar o site, você pode modificar essa conexão e recursos e criar mais conexões. Para obter detalhes, consulte Criar e gerenciar conexões e recursos.

- Para obter informações especificadas sobre a página **Connection**, consulte Criar e gerenciar conexões e recursos.
  - Se você não estiver usando VMs em um hipervisor ou outro serviço (ou se usar o Web Studio para gerenciar áreas de trabalho em PCs blade dedicados), selecione o tipo de conexão **None**.
  - Se você estiver configurando um site de Acesso ao PC Remoto e planeja usar o recurso Wake on LAN, selecione o tipo **Microsoft System Center Virtual Machine Manager** ou **Remote PC Wake on LAN**. Para obter mais informações, consulte Wake on LAN.

  Além do tipo de conexão, especifique se você usará as ferramentas Citrix (como Machine Creation Services) ou outras ferramentas para criar VMs.
- Para obter informações especificadas nas páginas **Armazenamento** e **Rede**, consulte Armazenamento de host, Gerenciamento de armazenamento e Seleção de armazenamento.
- Se você tem a Licença Hybrid Rights e adicionou conexões de host de nuvem pública (por exemplo, AWS), essas conexões são listadas aqui. Para exibir essas conexões de host de nuvem pública, atualize o Web Studio alguns minutos depois de adicioná-las.

Remote PC Access

Para obter informações sobre implantações do Remote PC Access, consulte Remote PC Access.

Se 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 and Remote PC Access Wake on LAN.

Criar e gerenciar conexões e recursos

June 28, 2023

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 2006, se a sua implantação atual usar qualquer uma das tecnologias a seguir, você poderá atualizar sua implantação para a versão atual somente após remover itens no fim da vida útil (EOL) que usam essas tecnologias.
>
> - PvDs (Personal vDisks)
> - AppDisks
> - Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic
>
> Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.
>
> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Se quiser usar conexões de host de nuvem pública para sua implantação, você precisa da Licença Hybrid Rights para concluir sua nova instalação ou atualizar para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença Hybrid Rights, a atualização é pausada ou interrompida, e uma mensagem explicativa é exibida. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Efeito da Licença Hybrid Rights na conexão de host

Há três cenários em que a conexão de host aos hosts de nuvem pública é afetada com base nos direitos da Licença Hybrid Rights:

- Para criar uma nova conexão de host aos hosts de nuvem pública, você deve ter uma Licença Hybrid Rights.
- Se você tiver a Licença Hybrid Rights, mas a licença tiver expirado, as conexões existentes aos hosts de nuvem pública são marcadas como não autorizadas e entram no modo de manutenção. Quando as conexões de host existentes estão no modo de manutenção, você não pode fazer o seguinte:
  - Adicionar ou modificar conexões de host
  - Criar catálogo e atualizar imagem
  - Realizar ações de energia

- Quando as conexões de host não autorizadas mudam para autorizadas, as conexões de hospedagem existentes são reativadas.

Introdução

Opcionalmente, você pode criar sua primeira conexão aos recursos de hospedagem ao criar um Site. Mais tarde, você pode alterar essa conexão e criar outras conexões. A configuração de uma conexão inclui selecionar o tipo de conexão entre os hipervisores suportados e o armazenamento e a rede que você selecionou nos recursos da conexão.

Os administradores somente leitura podem exibir 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 compatíveis para hospedar e gerenciar máquinas em seu ambiente Citrix Virtual Apps ou Citrix Virtual Desktops. O artigo Requisitos do sistema lista os tipos compatíveis.

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 do Nutanix.
  - Documentação do Nutanix.
- **VMware:**
  - Ambientes de virtualização do VMware.
  - Documentação do produto VMware.
- **Microsoft Hyper-V:**
  - Artigo Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.
  - 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.

> **Nota:**
>
> As fontes de informação levam você para a documentação do Citrix DaaS. Se você estiver familiarizado com os hosts de nuvem pública no produto Citrix DaaS, a versão local tem várias diferenças. No Citrix DaaS, a interface de gerenciamento é conhecida como Full Configuration. No Virtual Apps and Desktops local, a interface de gerenciamento é conhecida como Web Studio. As atualizações do Service são lançadas aproximadamente a cada quatro semanas. Portanto, você notará que certos recursos disponíveis com o Service não estão disponíveis na versão local.

Armazenamento em host

Um produto de armazenamento é suportado quando gerenciado por um hipervisor compatível. O suporte Citrix auxilia esses fornecedores de produtos de armazenamento na solução de problemas e documenta esses problemas no Knowledge Center, conforme necessário.

Ao provisionar máquinas, os dados são classificados por tipo:

- Dados do sistema operacional (SO), que inclui imagens mestre.
- Dados temporários. Esses dados incluem todos os dados não persistentes gravados em máquinas provisionadas pelo MCS, arquivos de paginação do Windows, dados de perfil de usuário e quaisquer dados sincronizados com o ShareFile. Esses dados são descartados cada vez que uma máquina é reinicializada.

Fornecer armazenamento separado para cada tipo de dados pode reduzir a carga e melhorar o desempenho em cada dispositivo de armazenamento, fazendo melhor uso dos recursos disponíveis do host. Isso também permite que o armazenamento adequado seja usado para os diferentes tipos de dados —persistência e resiliência são mais importantes para alguns dados do que outros.

O armazenamento pode ser compartilhado (localizado centralmente, separado de qualquer host, usado por todos os hosts) ou local para um hipervisor. Por exemplo, o armazenamento compartilhado central pode ser um ou mais volumes de armazenamento em cluster do Windows Server 2012 (com ou sem armazenamento conectado) ou um dispositivo de um fornecedor de armazenamento. O armazenamento central também pode fornecer suas próprias otimizações, como caminhos de controle de armazenamento de hipervisor e acesso direto por meio de plug-ins de parceiros.

Armazenar dados temporários localmente evita a necessidade de atravessar a rede para acessar o armazenamento compartilhado. Isso também reduz a carga no dispositivo de armazenamento compartilhado. O armazenamento compartilhado pode ser mais caro, portanto, armazenar dados localmente pode reduzir as despesas. Esses benefícios devem ser ponderados em relação à disponibilidade de armazenamento suficiente nos servidores do hipervisor.

Ao criar uma conexão, você escolhe um dos dois métodos de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local para o hipervisor.

Ao usar o armazenamento local em um ou mais hosts Citrix Hypervisor para armazenamento de dados temporário, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

Armazenamento compartilhado por hipervisores

O método de armazenamento compartilhado por hipervisores armazena dados que precisam de persistência de longo prazo centralmente, fornecendo backup e gerenciamento centralizados. Esse armazenamento contém os discos de SO.

Ao selecionar esse método, você pode escolher se deseja usar o armazenamento local (em servidores no mesmo pool do hipervisor) para dados temporários da máquina. Esse método não requer persistência nem tanta resiliência quanto os dados no armazenamento compartilhado, referido como *cache de dados temporários*. O disco local ajuda a reduzir o tráfego para o armazenamento do SO principal. Esse disco é limpo após cada reinicialização de máquina. O disco é acessado através de um cache de memória de gravação. Se você usa o armazenamento local para dados temporários, o VDA provisionado estará vinculado ao host de um hipervisor específico. Se o host falhar, a VM não pode ser iniciada.

Exceção: o Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários no armazenamento local ao usar os volumes de armazenamento em cluster (CSV).

Crie uma conexão para armazenar dados temporários localmente e, em seguida, ative 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 através do cache de leitura das imagens de disco localmente. Por exemplo, o Citrix Hypervisor oferece IntelliCache, que reduz o tráfego de rede para o armazenamento central.

Armazenamento local para o hipervisor

O armazenamento local para o método do hipervisor armazena dados localmente no hipervisor. Com esse método, imagens 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 da imagem. Este processo resulta em tráfego significativo na rede de gerenciamento. A transferência das imagens também é demorada, e as imagens ficam disponíveis para cada host em momentos diferentes.

Criar uma conexão e recursos

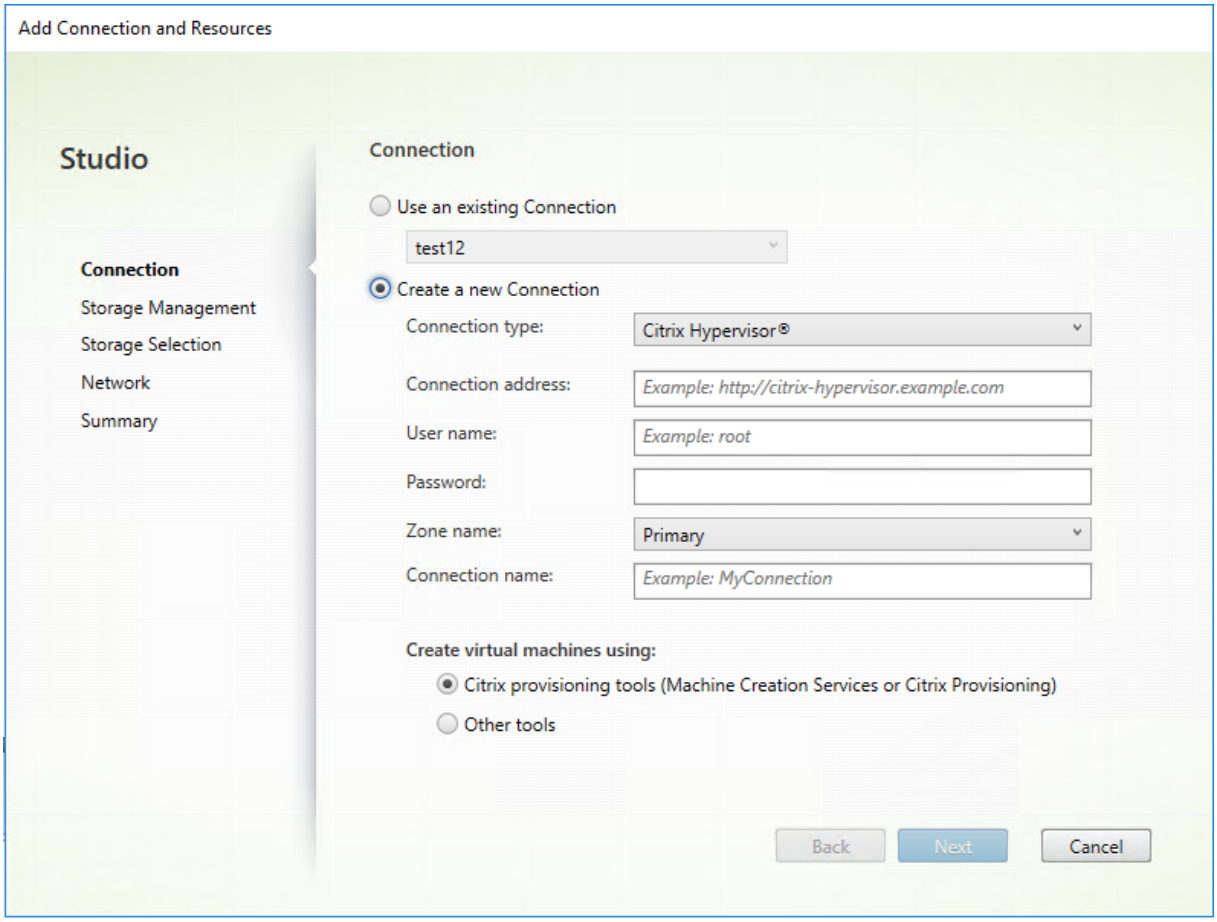
Você pode, opcionalmente, criar a primeira conexão quando criar o Site. O assistente de criação do Site contém as páginas relacionadas à conexão descritas nas seções a seguir.

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 criar uma conexão.

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione**Add Connections and Resources** na barra de ações.
4. O assistente orienta você pelas páginas a seguir (o conteúdo específico da página depende do tipo de conexão selecionado). Depois de concluir cada página, clique em **Next** até chegar à página **Summary**.

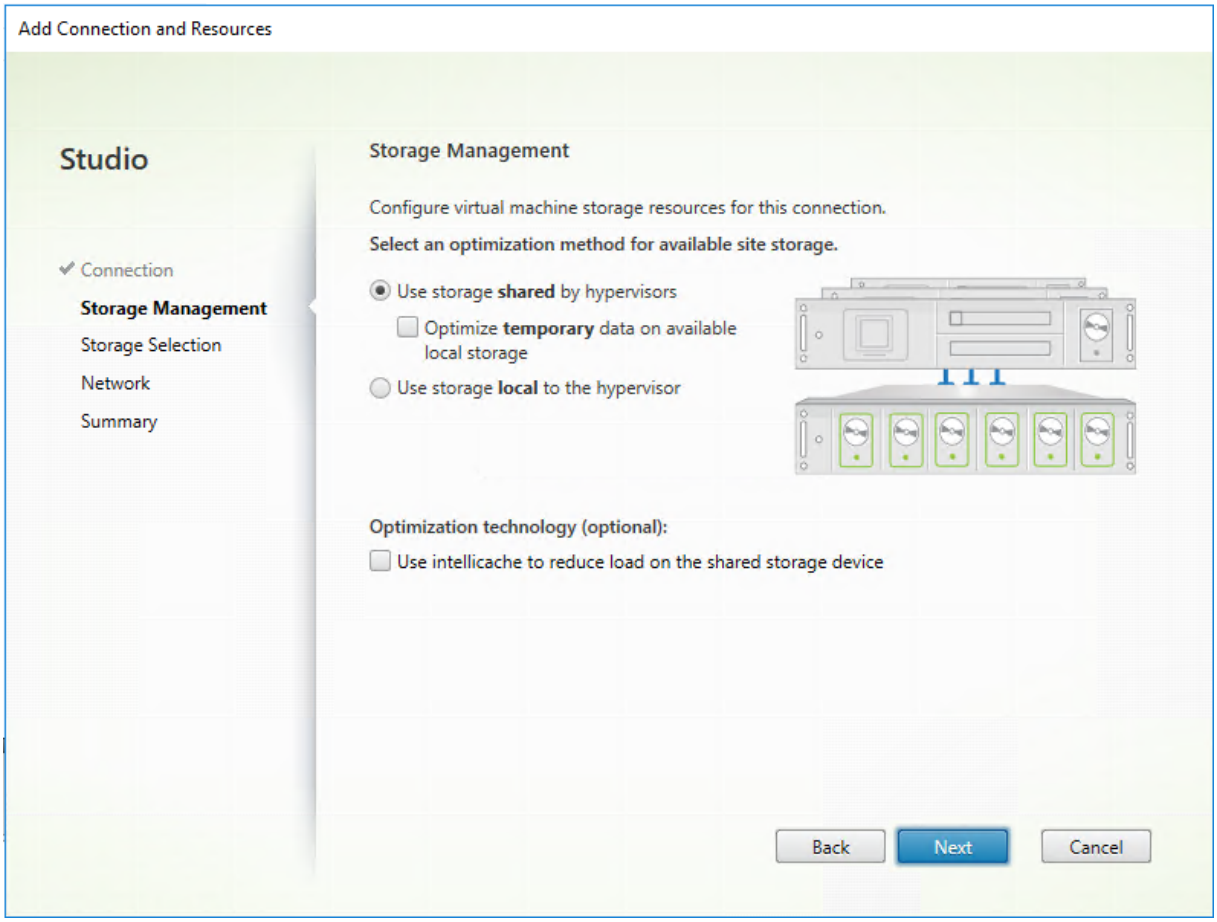
Conexão



Na página **Connection**:

- Para criar uma conexão, selecione **Create a new Connection**. Para criar uma conexão com base na mesma configuração de host que uma conexão existente, selecione **Use an existing Connection** e escolha a conexão relevante.
- Selecione o hipervisor que você está usando no campo **Connection type**. As conexões de host de nuvem pública são relacionadas na lista suspensa somente se você usar a Licença Hybrid Rights.
- O endereço de conexão e os campos de credenciais diferem, dependendo do tipo de conexão selecionado. Insira as informações solicitadas.
- Digite um nome para a conexão. Esse nome aparece no Web Studio.
- Escolha a ferramenta que você usa para criar máquinas virtuais: ferramentas do Web Studio (como Machine Creation Services ou Citrix Provisioning) ou outras ferramentas.

Gerenciamento de armazenamento



Para obter informações sobre tipos e métodos de gerenciamento de armazenamento, consulte Armazenamento em host.

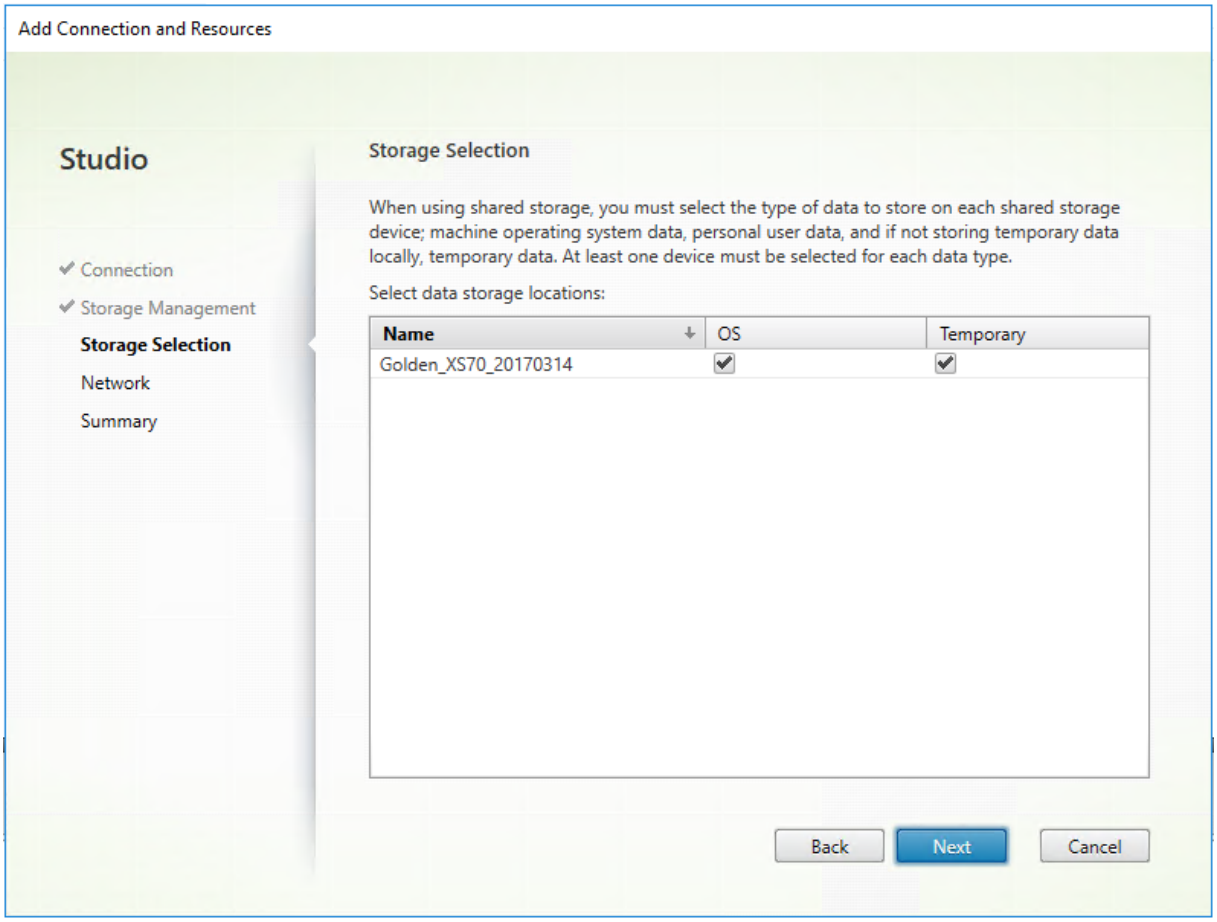
Se você estiver configurando uma conexão a um host Hyper-V ou VMware, navegue até o nome de cluster e selecione-o. Outros tipos de conexão não exigem um nome de cluster.

Selecione um método de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local para o hipervisor.

- Se você escolher armazenamento compartilhado por hipervisores, indique se deseja manter os dados temporários no armazenamento local disponível. (Você pode especificar tamanhos de armazenamento temporário não padrão nos Catálogos de Máquinas que usam essa conexão.) **Exceção:** ao usar os volumes de armazenamento em cluster (CSV), o Microsoft System Center Virtual Machine Manager não permite discos de cache de dados temporários no armazenamento local. Definir essa configuração de gerenciamento de armazenamento no Web Studio falhará.

Se você usa o armazenamento compartilhado em um pool do Citrix Hypervisor, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Usar o IntelliCache para conexões do Citrix Hypervisor.

Seleção de armazenamento



Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento em host.

Selecione pelo menos um dispositivo de armazenamento de host para cada tipo de dados disponível. O método de gerenciamento de armazenamento selecionado na página anterior afeta quais tipos de dados estão disponíveis para seleção nesta página. Selecione pelo menos um dispositivo de armazenamento para cada tipo de dados suportado antes de seguir para a próxima página do assistente.

A parte inferior da página **Storage Selection** contém mais opções de configuração se você escolher o armazenamento compartilhado por hipervisores e habilitado **Optimize temporary data on available local storage** 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, um dispositivo de armazenamento foi selecionado, como informa a linha "1 storage device selected"). Quando você passa o mouse sobre essa entrada, o nome dos dispositivos selecionados é exibido.

1. Clique em **Select** para alterar os dispositivos de armazenamento que devem ser usados.
2. Na caixa de diálogo **Select Storage**, marque ou desmarque as caixas de seleção de dispositivos de armazenamento e clique em **OK**.

Rede

Na página **Network**, insira um nome para os recursos. Esse nome aparece no Web Studio para identificar a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs usam.

Resumo

Na página **Summary**, revise suas seleções. Quando terminar, clique em **Finish**.

Lembre-se: armazenar dados temporários localmente permite que você configure valores não padrão para armazenamento de dados temporários quando você cria o catálogo de máquinas que contém as máquinas usando essa conexão. Consulte Criar catálogos de máquinas.

Editar configurações de conexão

Não use este procedimento para renomear uma conexão ou para criar uma conexão. Essas conexões são operações diferentes. Altere o endereço somente se a máquina host atual tiver um novo en-

dereço. Inserir um endereço para uma máquina diferente interrompe os catálogos de máquinas da conexão.

Não é possível alterar as configurações de **GPU** de uma conexão, pois os catálogos de máquinas que acessam esse recurso devem usar uma imagem mestre específica da GPU apropriada. Crie uma conexão.

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão e selecione **Edit Connection** na barra de ações.
4. Siga as instruções para as configurações disponíveis quando editar uma conexão.
5. Quando terminar, clique em **Apply** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Save** para aplicar as alterações e fechar a janela.

Página **Connection Properties**:

- Para alterar o endereço de conexão e as credenciais, selecione **Edit settings…** e insira as novas informações.
- Para especificar os servidores de alta disponibilidade para uma conexão do Citrix Hypervisor, selecione **Edit servers…** e selecione os servidores. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o Citrix Hypervisor se a imagem mestre do pool falhar.

  > **Nota:**
  >
  > Se você estiver usando HTTPS e quiser configurar servidores de alta disponibilidade, não instale um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor.

Página **Advanced**:

- Para um tipo de conexão Wake on LAN do Microsoft System Center Configuration Manager (ConfMgr), que é usada com Remote PC Access, 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 sejam iniciadas ao mesmo tempo. Cada tipo de conexão contém valores padrão específicos que são apropriados para a maioria dos casos e não devem ser alterados.
- A configuração **Simultaneous actions (all types)** especifica dois valores: o número absoluto máximo que pode ocorrer simultaneamente nesta conexão e a porcentagem máxima de todas as máquinas que usam a conexão. Você deve especificar os valores absoluto e percentual. O limite real aplicado é o menor dos valores.

Por exemplo, em uma implantação com 34 máquinas, se **Simultaneous actions (all types)** for definido como um valor absoluto de 10 e um valor percentual de 10, o limite real aplicado será 3 (ou seja, 10% de 34 arredondados para o número inteiro mais próximo, que é menor que o valor absoluto de 10 máquinas).

- **Maximum new actions per minute** é um número absoluto. Não há valor percentual.
- Insira as informações no campo **Connection options** somente sob a orientação de um representante do Suporte Citrix ou seguindo instruções explícitas na documentação.

Ativar ou desativar o modo de manutenção para uma conexão

Ligar o modo de manutenção para uma conexão impede que qualquer nova ação de energia afete as máquinas armazenadas na conexão. Os usuários não podem se conectar a uma máquina quando ela está no modo de manutenção. Se os usuários já estiverem conectados, o modo de manutenção entra em vigor quando eles fazem logoff.

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão. Para ativar o modo de manutenção, selecione **Turn On Maintenance Mode** na barra de ações. Para desativar o modo de manutenção, selecione **Turn Off Maintenance Mode**.

Você também pode ativar ou desativar o modo de manutenção para máquinas individuais. Além disso, você pode ativar ou desativar o modo de manutenção para as máquinas em catálogos de máquinas ou grupos de entrega.

Excluir uma conexão

A exclusão de uma conexão pode resultar na exclusão de um grande número de máquinas e perda de dados. Certifique-se de que seja feito o backup dos dados de usuário nas máquinas afetadas ou que eles não sejam mais necessários.

Antes de excluir uma conexão, certifique-se de que:

- Todos os usuários estão desconectados das máquinas armazenadas na conexão.
- Nenhuma sessão de usuário desconectada está sendo executada.
- O modo de manutenção está ativado para máquinas em pool e dedicadas.
- Todas as máquinas nos catálogos de máquinas usadas pela conexão estão desligadas.

Um catálogo de máquinas torna-se inutilizável quando você exclui uma conexão que é referenciada por esse catálogo. Se a conexão for referenciada por um catálogo, você tem a opção de excluir o catálogo. Antes de excluir um catálogo, verifique se ele não é usado por outras conexões.

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão e selecione **Delete Connection** na barra de ações.
4. Se a conexão tiver máquinas armazenadas nela, você será perguntado se as máquinas devem ser excluídas. Se tiverem que ser excluídas, especifique o que deve ser feito com as contas de computador do Active Directory associadas.

Renomear ou testar uma conexão

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão e depois selecione **Rename Connection** ou **Test Connection** na barra de ações.

Exibir detalhes da máquina em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão e selecione **View Machines** na barra de ações.

O painel superior lista as máquinas acessadas através da conexão. Selecione uma máquina para exibir seus detalhes no painel inferior. Os detalhes da sessão também são fornecidos para sessões abertas.

Use o recurso de pesquisa para encontrar máquinas rapidamente. Selecione uma pesquisa salva na lista, na parte superior da janela, ou crie uma pesquisa. Você pode pesquisar digitando todo ou parte do nome da máquina, ou pode criar uma expressão para usar em uma pesquisa avançada. Para criar uma expressão, clique em **Unfold** e selecione nas listas de propriedades e operadores.

Gerenciar máquinas em uma conexão

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione uma conexão e depois selecione **View Machines** no painel **Actions**.
4. Selecione uma das seguintes opções na barra de ações. Algumas ações não estão disponíveis, dependendo do estado da máquina e do tipo de host da conexão.

Ação	Descrição
Start	Inicia a máquina se estiver desligada ou suspensa.
Suspend	Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
Shut down	Solicita que o sistema operacional seja desligado.
Force shut down	Força o desligamento da máquina e atualiza a lista de máquinas.
Restart	Solicita que o sistema operacional seja desligado e, em seguida, inicializa a máquina novamente. Se o sistema operacional não conseguir, a área de trabalho permanecerá em seu estado atual.
Enable maintenance mode	Interrompe temporariamente as conexões com uma máquina. Os usuários não podem se conectar a uma máquina nesse estado. Se os usuários estiverem conectados, o modo de manutenção entra em vigor quando eles fazem logoff. (Você também pode ativar ou desativar o modo de manutenção para todas as máquinas acessadas por meio de uma conexão, conforme descrito acima.)
Remove from Delivery Group	Remover uma máquina de um grupo de entrega não a exclui do catálogo de máquinas que o grupo de entrega usa. Você pode remover uma máquina somente quando nenhum usuário está conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver removendo a máquina.

Ação	Descrição
Delete	Quando você exclui uma máquina, os usuários não têm mais acesso a ela, e a máquina é excluída do catálogo de máquinas. Antes de excluir uma máquina, certifique-se de que seja feito o backup de todos os dados de usuário ou que eles não sejam mais necessários. Você pode excluir uma máquina somente quando nenhum usuário está conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver excluindo a máquina.

Para ações que envolvem o desligamento da máquina, se a máquina não for desligada dentro de 10 minutos, ela será encerrada. Se o Windows tentar instalar atualizações durante o desligamento, existe o risco de a máquina ser encerrada antes que as atualizações sejam concluídas.

Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar o sistema operacional e os dados temporários das VMs que usam uma conexão. Você também pode especificar quais servidores usar para armazenamento de cada tipo de dados.

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione a conexão e selecione **Edit Storage** na barra de ações.
4. No painel esquerdo, selecione o tipo de dados: sistema operacional ou temporário.
5. Marque ou desmarque as caixas de seleção de um ou mais dispositivos de armazenamento para o tipo de dados selecionado.
6. Clique em **OK**.

Cada dispositivo de armazenamento na lista inclui seu nome e status de armazenamento. Os valores de status de armazenamento válidos são:

- **In use:** o armazenamento está sendo usado para criar máquinas.
- **Superseded:** o armazenamento está sendo usado apenas para máquinas existentes. Nenhuma nova máquina é adicionada a este armazenamento.
- **Not in use:** o armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo atualmente selecionado como **In use**, seu status será alterado para **Superseded**. As máquinas existentes continuarão a usar esse dispositivo de armazenamento (e podem gravar dados nele), portanto, é possível que o local fique cheio mesmo depois de não ser mais usado para criar máquinas.

Excluir, renomear ou testar recursos

1. Faça login no Web Studio.
2. Selecione **Hosting** no painel esquerdo.
3. Selecione o recurso e, em seguida, selecione a entrada apropriada na barra de ações: **Delete Resources**, **Rename Resources** ou **Test Resources**.

Timers de conexão

Você pode usar configurações de política para definir três timers de conexão:

- **Maximum connection timer:** determina a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e uma área de trabalho virtual. Use as configurações de política **Session connection timer** e **Session connection timer interval**.
- **Connection idle timer:** determina quanto tempo uma conexão ininterrupta do dispositivo do usuário a uma área de trabalho virtual é mantida se não houver nenhuma entrada pelo usuário. Use as configurações de política **Session idle timer** e **Session idle timer interval**.
- **Disconnect timer:** determina quanto tempo uma área de trabalho virtual desconectada e bloqueada pode permanecer bloqueada antes que seja feito logoff da sessão. Use as configurações de política **Disconnected session timer** e **Disconnected session timer interval**.

Quando você atualizar qualquer uma dessas configurações, assegure que elas sejam consistentes em toda a sua implantação.

Consulte a documentação de configurações de política para obter mais informações.

Criar catálogos de máquinas

April 3, 2024

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 2006, se a sua implantação atual usar qualquer uma das tecnologias a seguir, você poderá atualizar sua implantação para a versão atual somente após remover itens no fim da vida útil (EOL) que usam essas tecnologias.

> - PvDs (Personal vDisks)
> - AppDisks
> - Tipos de host de nuvem pública: Citrix CloudPlatform, Microsoft Azure Classic
>
> Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.
>
> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Se quiser usar conexões de host de nuvem pública para sua implantação, você precisa da Licença Hybrid Rights para concluir sua nova instalação ou atualizar para a versão atual.

Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença Hybrid Rights, a atualização é pausada ou interrompida. Uma mensagem explicativa é exibida. Os logs do instalador contêm detalhes. Para obter mais informações, consulte Atualizar uma implantação.

Efeito da Licença Hybrid Rights nas conexões de host

Há três cenários em que a conexão de host aos hosts de nuvem pública é afetada com base nos direitos da Licença Hybrid Rights:

- Para criar uma conexão de host aos hosts de nuvem pública, você deve ter uma Licença Hybrid Rights.
- Se você tiver a Licença Hybrid Rights, mas a licença tiver expirado, as conexões existentes aos hosts de nuvem pública são marcadas como não autorizadas e entram 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
  - Realizar 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 multissessão ou SO de sessão única. Um catálogo contendo máquinas de SO multissessão pode conter máquinas Windows ou Linux, mas não as duas.

O Web Studio o leva pelo processo de criação do primeiro catálogo de máquinas depois que você criar o site. Depois de criar o primeiro catálogo, o Web Studio o leva pelo processo de criação do primeiro grupo de entrega. Mais tarde, você pode alterar o catálogo criado e criar mais catálogos.

> **Dica:**
>
> A atualização de uma implantação existente habilita o recurso de otimização de armazenamento (MCS I/O) do Machine Creation Services (MCS), sem necessidade de configuração adicional. O Virtual Delivery Agent (VDA) e a atualização do Delivery Controller manipulam a atualização de MCS I/O.

Visão geral

Ao criar um catálogo de VMs, você especifica como provisionar essas VMs. Você pode usar o Machine Creation Services (MCS). Ou você pode usar suas próprias ferramentas para fornecer máquinas.

Considere o seguinte:

- O MCS suporta um único disco de sistema a partir da imagem da máquina virtual. Ele ignora o restante dos discos de dados anexados à imagem.
- Se usar o MCS para provisionar VMs, você fornece uma imagem mestre (ou instantâneo de uma imagem) para criar VMs idênticas no catálogo. Antes de criar o catálogo, você primeiro usa as ferramentas para criar e configurar a imagem mestre. Esse processo inclui a instalação de um Virtual Delivery Agent (VDA) na imagem. Em seguida, você cria o catálogo de máquinas no Web Studio. Você seleciona essa imagem (ou instantâneo), especifica o número de VMs a serem criadas no catálogo e configura informações adicionais.
- Se suas máquinas já estiverem disponíveis, você ainda deve criar um ou mais catálogos de máquinas para essas máquinas.
- Se você estiver criando um catálogo usando o SDK do PowerShell diretamente, poderá especificar um modelo de hipervisor (**VMTemplates**), em vez de uma imagem ou um instantâneo.
- Usar um modelo para provisionar um catálogo é considerado um recurso experimental. Ao usar esse método, a preparação da máquina virtual pode falhar. Consequentemente, o catálogo não pode ser publicado usando o modelo.

Quando 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 as 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 esteja configurado corretamente. Quando os testes forem concluídos, você pode ver um relatório de teste. Execute os testes quando quiser usando o Web Studio.

> **Nota:**
>
> O MCS não suporta o Windows 10 IoT Core e Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

Para obter detalhes técnicos sobre as ferramentas Citrix Provisioning, consulte Citrix Virtual Apps and Desktops Image Management.

Verificação de licença RDS

No momento, o Web Studio não executa a verificação de licenças válidas do Microsoft RDS ao criar um catálogo de máquinas que contém máquinas com SO multissessão Windows. Para exibir o status da licença do Microsoft RDS para um **máquinas com SO multissessão** Windows, vá para Citrix Director. Veja o status da licença do Microsoft RDS no painel **Machine Details**. O painel está localizado na página **Machine Details and the User Details**. Para obter mais informações, consulte Integridade da licença do Microsoft RDS.

Registro de VDA

Um VDA deve ser registrado em um Delivery Controller ao iniciar sessões intermediadas. Os VDAs não registrados podem resultar na subutilização de recursos disponíveis. Há várias razões para que um VDA não possa ser registrado, muitas das quais um administrador pode resolver. O Web Studio fornece informações sobre solução de problemas no assistente de criação de catálogo e depois de você adicionar máquinas de um catálogo para 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 a máquina.

Se a mensagem identificar uma máquina problemática, remova a máquina ou adicione-a. Por exemplo, se uma mensagem indicar que é possível que as informações sobre uma máquina não sejam obtidas, adicione a máquina de qualquer maneira.

Para obter mais informações, consulte:

- CTX136668 para obter instruções para a solução de problemas de registro do VDA
- Versões VDA e níveis funcionais
- Métodos de registro de VDA

Resumo da criação de um catálogo MCS

Apresentamos a seguir uma breve visão geral das ações padrão do MCS depois que você fornece informações no assistente de criação de catálogo.

- Se você selecionou uma imagem mestre (em vez de um instantâneo), o MCS criará um instantâneo.
- O MCS cria uma cópia completa do instantâneo e coloca a cópia em cada local de armazenamento definido na conexão do host.
- O MCS adiciona as máquinas ao Active Directory, que cria identidades exclusivas.
- O MCS cria o número de VMs especificadas no assistente, com dois discos definidos para cada VM. Além dos dois discos por VM, uma imagem mestre também é armazenada no mesmo local de armazenamento. Se você tiver vários locais de armazenamento definidos, cada um deles obterá os seguintes tipos de disco:
  - A cópia completa do instantâneo que é somente leitura e compartilhada entre as VMs recém-criadas.
  - Um disco de identidade exclusivo de 16 MB que dá a cada VM uma identidade exclusiva. Cada VM obtém um disco de identidade.
  - Um disco de diferença exclusivo para armazenar gravações feitas na VM. Esse disco é provisionado pelo thin (se suportado pelo armazenamento do host) e aumenta até o tamanho máximo da imagem mestre, se necessário. Cada VM obtém um disco de diferença. O disco de diferença mantém as alterações feitas durante as sessões. É permanente para áreas de trabalho dedicadas. Para áreas de trabalho em pool, ele é excluído e um novo é criado após cada reinicialização através do Delivery Controller.

Como alternativa, ao criar VMs para fornecer áreas de trabalho estáticas, você pode especificar (na página **Machines** do assistente de criação de catálogo) clones de VM thick (cópia completa). Os clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem o seu próprio arquivo.

Considerações sobre armazenamento MCS

Há muitos fatores a considerar ao decidir sobre soluções, configurações e capacidades de armazenamento para MCS. As informações a seguir fornecem considerações apropriadas sobre a capacidade de armazenamento:

Considerações sobre a capacidade:

- Discos

  Os discos Delta ou Differencing (Diff) consomem a maior quantidade de espaço na maioria das

implantações MCS por VM. Cada VM criada pelo MCS recebe no mínimo dois discos após a criação.

  - Disk0 = Diff Disk: contém o SO quando copiado da imagem base mestre.
  - Disk1 = Identity Disk: 16 MB - contém dados do Active Directory de cada VM.

  À medida que o produto evolui, pode ser preciso adicionar mais discos para satisfazer determinados casos de uso e consumo de recursos que você tenha. Por exemplo:

  - O MCS Storage Optimization cria um disco de estilo cache de gravação para cada VM.
  - O MCS adicionou a capacidade de usar clones completos, contrário ao cenário de disco Delta descrito na seção anterior.

  Os recursos do Hypervisor também podem entrar na equação. Por exemplo:

  - Citrix Hypervisor IntelliCache cria um disco de leitura no armazenamento local para cada Citrix Hypervisor. Essa opção economiza IOPS em comparação à imagem mestre, que pode ser mantida no local de armazenamento compartilhado.

- Sobrecarga do hipervisor

  Diferentes hipervisores usam arquivos específicos que criam sobrecarga para VMs. Os hipervisores também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir sobrecargas para:

  - Arquivos de log
  - Arquivos específicos do Hypervisor. Por exemplo:
    * VMware adiciona mais arquivos à pasta de **armazenamento da VM**. Consulte VMware Best Practices.
    * Calcule os seus requisitos totais de tamanho de máquinas virtuais. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de permuta e 100 MB para arquivos de log, o que consome 36,1 GB no total.
  - Snapshots for XenServer; Snapshots for VMware.

- Sobrecarga do processo

  Criar um catálogo, adicionar uma máquina e atualizar um catálogo têm implicações únicas no armazenamento. Por exemplo:

  - A criação de um catálogo inicial requer que uma cópia do disco base seja copiada para cada local de armazenamento.
    * Essa opção também requer que você crie uma VM de preparação temporariamente.
  - A adição de uma máquina a um catálogo não exige copiar o disco base para cada local de armazenamento. A criação do catálogo varia de acordo com os recursos selecionados.

  - Atualizar o catálogo para criar um disco básico extra em cada local de armazenamento. Atualizações de catálogo também apresentam um pico de armazenamento temporário, onde cada VM no catálogo possui 2 discos Diff por um determinado período de tempo.

Mais considerações:

- **Dimensionamento de RAM:** afeta o tamanho de determinados discos e arquivos do hipervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de instantâneos.
- **Provisionamento thin/thick:** o armazenamento NFS é preferido devido aos recursos de provisionamento dinâmico.

Otimização de armazenamento de Machine Creation Services (MCS)

Com o recurso de otimização de armazenamento MCS (Machine Creation Services), 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 MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico, ao incluir suporte para um arquivo de despejo de memória do Windows gravado no disco de cache de gravação.
- O MCS I/O mantém a tecnologia de *cache em RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação multicamada mais adequada. Essa funcionalidade permite que um administrador equilibre entre o custo de cada camada, RAM e disco, e desempenho para atender à expectativa de carga de trabalho desejada.

Atualizar o método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. MCS I/O não suporta mais cache somente RAM. Especifique um tamanho de disco no Web Studio durante a criação do catálogo de máquinas.
2. O disco de cache de gravação da VM é criado e formatado automaticamente ao inicializar uma VM pela primeira vez. Uma vez que a VM esteja ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.
3. O pagefile, ou arquivo de paginação, é redirecionado para o volume formatado, `MCSWCDisk`. Como resultado, o tamanho de disco considera a quantidade total de espaço em disco. Ele inclui o delta entre o tamanho do disco e a carga de trabalho gerada, acrescido do tamanho do arquivo de paginação. Isso geralmente é associado ao tamanho da RAM da VM.

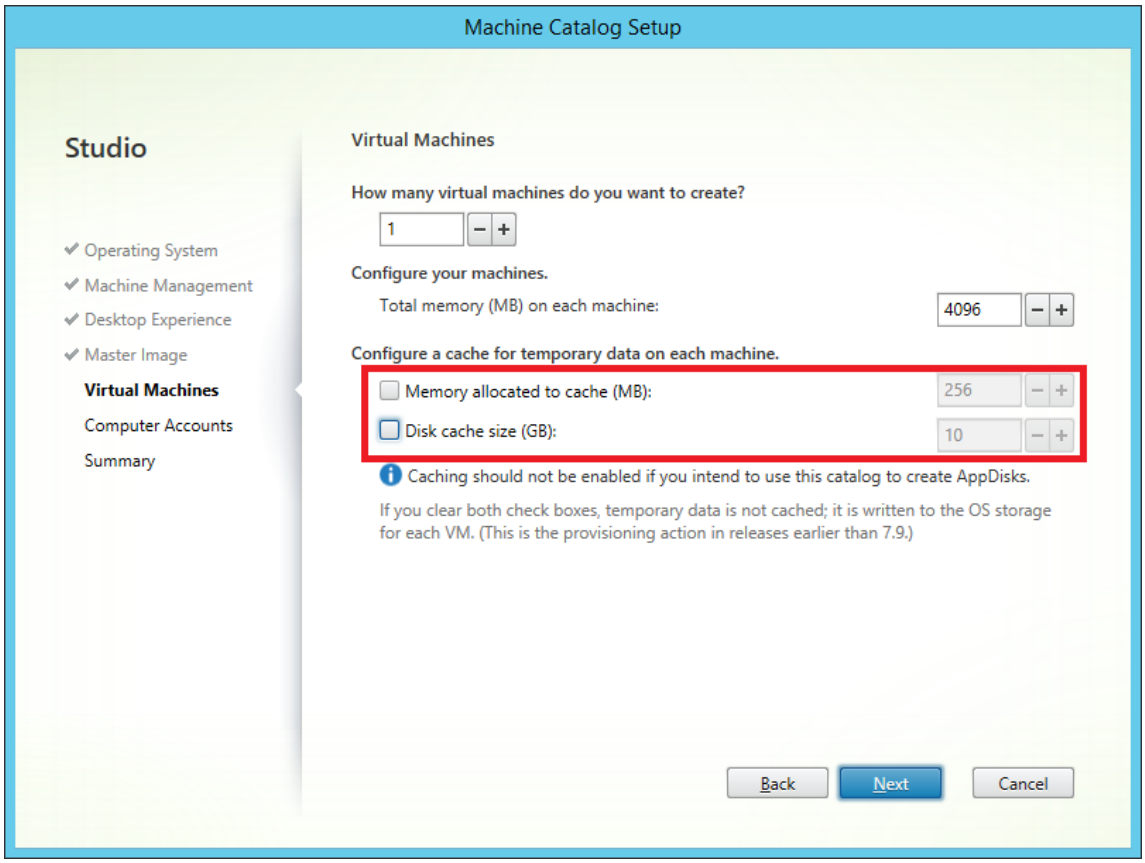
Ativar atualizações de otimização de armazenamento MCS Para ativar a funcionalidade de otimização de armazenamento MCS I/O, atualize o Delivery Controller e o VDA para a versão mais

recente do Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será exigida. O VDA e a atualização do Delivery Controller manipulam a atualização do MCS I/O.

Ao ativar a atualização de otimização de armazenamento MCS, considere o seguinte:

- Ao criar um catálogo de máquinas, o administrador pode configurar a RAM e o tamanho do disco.



- Atualizar um catálogo de máquinas existente para um novo instantâneo de VM contendo um VDA configurado para a versão 1903 resulta no seguinte comportamento: o novo instantâneo continua a usar a configuração de MCS I/O do catálogo existente para RAM e tamanho do disco. O disco bruto existente é formatado.

> **Importante:**
>
> A otimização de armazenamento MCS mudou com o Citrix Virtual Apps and Desktops versão 1903. Essa versão suporta a tecnologia de cache de gravação baseada em arquivo, proporcionando melhor desempenho e estabilidade. A nova funcionalidade fornecida pelo MCS I/O pode ter um

> requisito maior de armazenamento em cache de gravação em comparação com as versões anteriores do Citrix Virtual Apps and Desktops. A Citrix recomenda que você reavalie o tamanho de disco para garantir que tenha espaço em disco suficiente para o fluxo de trabalho alocado e para o tamanho do pagefile extra. O tamanho do pagefile normalmente está relacionado à quantidade de RAM do sistema. Se o tamanho de disco do catálogo existente for insuficiente, crie um catálogo de máquinas e aloque um disco de cache de gravação maior.

Usar PowerShell para criar um catálogo com disco de cache de write-back persistente Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. Esse parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas MCS. A propriedade `PersistWBC` só é usada quando o parâmetro `UseWriteBackCache` é especificado, e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco foi criado.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes do suporte a `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>
<!--NeedCopy-->
```

Ao usar essas propriedades, considere que elas contêm valores padrão se as propriedades forem omitidas do parâmetro `CustomProperties`. A propriedade `PersistWBC` tem dois valores possíveis: **true** ou **false**.

Definir a propriedade `PersistWBC` como **true** não exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Web Studio.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix Virtual Apps and Desktops desliga a máquina usando o Web Studio.

> **Nota:**
>
> Se a propriedade `PersistWBC` for omitida, a propriedade assume o padrão **false** e o cache de write-back é excluído quando a máquina é desligada usando o Web Studio.

Por exemplo, uso do 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>
<!--NeedCopy-->
```

> **Importante:**
>
> A propriedade `PersistWBC` só pode ser definida usando o cmdlet `New-ProvScheme` do PowerShell. Tentar alterar `CustomProperties` em um esquema de provisionamento após a criação não tem impacto no catálogo da máquina e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, definir `New-ProvScheme` para usar o cache de write-back ao definir a propriedade `PersistWBC` como true:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```


Preparar uma imagem mestre

Para obter informações sobre a criação de hosts de conexões, consulte Conexões e recursos.

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

É bom saber:

- Uma imagem mestre também é conhecida como imagem clonada, imagem final, VM base ou imagem base. Os fornecedores de host usam termos diferentes.
- Verifique se o host tem processadores, memória e armazenamento suficientes para acomodar o número de máquinas criadas.
- Configure a quantidade correta de espaço em disco rígido necessário para áreas de trabalho e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo de máquinas.
- Os catálogos de máquinas do Remote PC Access não usam imagens mestre.
- Considerações de ativação do Microsoft KMS ao usar o MCS: se a sua implantação incluir VDAs 7.x com um host XenServer 6.1 ou 6.2, vSphere ou Microsoft System Center Virtual Machine Manager, você não precisa rearmar manualmente o Microsoft Windows ou o Microsoft Office.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para o seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou ferramentas VMware). Se você omitir esta etapa, aplicativos e áreas de trabalho podem não funcionar corretamente.
- Um VDA. A Citrix recomenda a instalação da versão mais recente para permitir o acesso aos recursos novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros, conforme necessárias, como softwares antivírus ou agentes de distribuição eletrônica de software. Defina os serviços com configurações apropriadas para os usuários e o tipo de máquina (por exemplo, atualização de recursos).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda a virtualização de aplicativos. A virtualização reduz os custos eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduz o tamanho dos discos rígidos de imagem mestre, o que economiza nos custos de armazenamento.
- Clientes App-V com as configurações recomendadas, se você planeja publicar aplicativos App-V. O cliente App-V está disponível na Microsoft.
- Quando usar MCS, se você localiza o Microsoft Windows, instale os locais e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam os locais e os pacotes de idiomas instalados.

> **Importante:**
>
> Se você estiver usando o MCS, não execute o Sysprep em imagens mestras.

Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e instale o sistema operacional, além de todos os service packs e atualizações. Especifique o número de CPUs virtuais. Você também pode especificar o valor vCPU se criar o catálogo da máquinas usando o PowerShell. Não é possível especificar o número de vCPUs ao criar um catálogo usando o Web Studio. Configure a quantidade de espaço em disco rígido necessário para áreas de trabalho e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo.
2. Assegure-se de que o disco rígido esteja conectado ao local do dispositivo 0. A maioria dos modelos de imagem mestre padrão configura esse local por padrão, mas alguns modelos personalizados podem não o fazer.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, associe a imagem mestre ao domínio onde aplicativos e áreas de trabalho são membros. Assegure-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas. Se você estiver usando o MCS, não é necessário associar a imagem mestre a um domínio. As máquinas provisionadas são ingressadas no domínio especificado no assistente de criação de catálogo.
5. A Citrix recomenda que você crie e dê um nome a um instantâneo da sua imagem mestre. Se você especificar uma imagem mestre em vez de um instantâneo ao criar um catálogo, o Web Studio criará um instantâneo. Você não pode dar um nome a ele.

Ativação do licenciamento por volume

O MCS oferece suporte à ativação de licenciamento por volume para automatizar e gerenciar a ativação dos sistemas operacionais Windows e do Microsoft Office. Os três modelos que o MCS aceita para ativação de licenciamento por volume são:

- Serviço de gerenciamento de chaves (KMS)
- Ativação baseada no Active Directory (ADBA)
- Chave de ativação múltipla (MAK)

Você pode alterar a configuração de ativação depois de criar o catálogo de máquinas.

Serviço de gerenciamento de chaves (KMS)

O KMS é um serviço leve que não requer um sistema dedicado e pode ser facilmente co-hospedado em um sistema que fornece outros serviços. Essa funcionalidade é suportada em todas as versões

do Windows suportadas pela Citrix. Durante a preparação da imagem, o MCS faz a rearmação do Microsoft Windows e do Microsoft Office KMS. Você pode pular a rearmação executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre o Microsoft Windows KMS Rearm e o Microsoft Office KMS Rearm durante a preparação da imagem, consulte Machine Creation Services: Image Preparation Overview and Fault-Finding. Para obter mais informações sobre a ativação do KMS, consulte Ativar usando o Serviço de Gerenciamento de Chaves.

> **Nota:**
>
> Todos os catálogos de máquinas criados após a execução do comando `Set-Provserviceconfiguration` têm a mesma configuração que a fornecida no comando.

Ativação baseada no Active Directory (ADBA)

O ADBA permite que você ative as máquinas por meio de suas conexões de domínio. As máquinas são ativadas imediatamente quando ingressam no domínio. Essas máquinas permanecem ativadas enquanto permanecerem ingressadas no domínio e em contato com ele. Essa funcionalidade é suportada em todas as versões do Windows suportadas pela Citrix, exceto o Windows Server 2022. Para obter mais informações sobre a ativação baseada no Active Directory, consulte Ativar usando a Ativação baseada no Active Directory.

Chave de ativação múltipla (MAK)

A MAK é uma forma de ativar o volume e autenticar o sistema Windows com a ajuda do servidor Microsoft. Você deve comprar a chave MAK da Microsoft, que é atribuída com um número fixo de contas de ativação. Toda vez que um sistema Windows é ativado, a uma redução na contagem de ativações. Há duas formas de ativar o sistema:

- Ativação on-line: se o sistema Windows que você deseja ativar tiver acesso à Internet, o sistema ativará automaticamente o Windows ao instalar a chave do produto. Esse processo reduz as contas de ativação em 1 da MAK correspondente.
- Ativação offline: se o sistema Windows não conseguir se conectar à Internet para fazer a ativação on-line, o MCS receberá um ID de confirmação e um ID de instalação do servidor Microsoft para ativar o sistema Windows. Essa forma de ativação é útil para catálogos de máquinas não persistentes.

Requisitos principais

- O Delivery Controller deve ter acesso à Internet.
- Crie um novo catálogo se a nova imagem a ser atualizada tiver uma chave MAK diferente da original.

- Instale a chave MAK na imagem mestre. Consulte Deploy MAK Activation para ver as etapas para instalar a chave MAK em um sistema Windows.
- Se você não estiver usando a preparação de imagens:

  1. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
  2. Defina o valor como 1.

Contagens de ativação Para ver o número de ativações restantes para a chave MAK ou verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação de Volume (VAMT). Consulte Instalar a VAMT.

Ativar o sistema Windows usando MAK Para ativar o sistema Windows usando a MAK:

1. Instale a chave do produto na imagem mestre. Essa etapa consome uma conta de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagens:

   a) Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfor\Activation`.
   b) Defina o valor como 1.

   Esse método desativa a opção de ativação on-line.
4. Adicione VMs ao catálogo de máquinas.
5. Ligue as VMs.
6. Dependendo da ativação, se on-line ou offline, o sistema Windows é ativado.

   - Se a ativação estiver on-line, o sistema Windows será ativado após a instalação da chave do produto.
   - Se a ativação estiver offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. Em seguida, o MCS recupera um ID de confirmação e um ID instalado do servidor Microsoft. Esses IDs são usados para ativar o sistema Windows.

Solução de problemas Se a VM provisionada não for ativada com a chave MAK instalada, execute o comando `Get-ProvVM` ou `Get-ProvScheme` em uma janela do PowerShell.

- O comando `Get-ProvScheme`: veja o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS a partir da imagem mestre mais recente.
- O comando `Get-ProvVM`. Veja os parâmetros `WindowsActivationType`, `WindowsActivationSta` , `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Você pode verificar o erro e conferir as etapas para resolver o problema.

Criar um catálogo de máquinas usando o Web Studio

Antes de criar um catálogo:

- Revise esta seção para saber mais sobre as escolhas que você faz e as informações que você fornece.
- Certifique-se de ter criado uma conexão com o hipervisor, serviço de nuvem ou outro recurso que hospeda suas máquinas.
- Se você criou uma imagem mestre para provisionar máquinas, verifique se você instalou um VDA nessa imagem.

Para iniciar o assistente de criação de catálogo:

1. Se este for o primeiro catálogo sendo criado, você será levado para a seleção correta (como "Set up the machines and create machine catalogs to run apps and desktops"). O assistente de criação de catálogo é aberto.
2. Se você já criou um catálogo e deseja criar outro, siga estas etapas:

    a) Entre no Web Studio, selecione **Machine Catalogs** no painel esquerdo e selecione **Create Machine Catalog** na barra de ações.

    b) Para organizar catálogos usando pastas, crie pastas abaixo da pasta **Machine Catalogs** padrão. Para obter mais informações, consulte Criar uma pasta de catálogo.

    c) Selecione a pasta em que você deseja criar o catálogo e clique em **Create Machine Catalog**. O assistente de criação de catálogo é aberto.

O assistente guiará você pelos seguintes itens. As páginas do assistente que você vê são diferentes, dependendo das seleções feitas.

Sistema operacional

Cada catálogo contém máquinas de apenas um tipo. Selecione um.

- **Multi-session OS:** um catálogo de SO multissessão fornece áreas de trabalho compartilhadas hospedadas. As máquinas podem estar executando versões suportadas dos sistemas operacionais Windows ou Linux, mas o catálogo não pode conter os dois. (Consulte a documentação do Linux VDA para obter detalhes sobre o sistema operacional.)
- **Single-session OS:** um catálogo de SO de sessão única fornece áreas de trabalho VDI que você pode atribuir a vários usuários diferentes.
- **Remote PC Access:** um catálogo de Remote PC Access fornece aos usuários acesso remoto a suas áreas de trabalho nas máquinas físicas no escritório. O Remote PC Access não requer uma VPN para fornecer segurança.

Gerenciamento de máquinas

Esta página não aparece quando você está criando catálogos de Remote PC Access.

A página **Machine Management** indica como as máquinas são gerenciadas e qual ferramenta você usa para implantar as máquinas.

Escolha se as máquinas no catálogo são gerenciadas por meio do Web Studio.

- A energia das máquinas é gerenciada pelo Web Studio, por exemplo, VMs ou PCs blade. Essa opção só estará disponível se você já tiver configurado uma conexão a um host.
- A energia das máquinas não é gerenciada pelo Web Studio, por exemplo, máquinas físicas.

Se você indicou que a energia das máquinas é gerenciada pelo Web Studio, escolha qual ferramenta usar para criar VMs.

- **Citrix Machine Creation Services (MCS):** usa uma imagem mestre para criar e gerenciar máquinas virtuais. O MCS não está disponível para máquinas físicas.
- **Other:** uma ferramenta que gerencia máquinas já no data center. A Citrix recomenda que você use o Microsoft System Center Configuration Manager ou outro aplicativo de terceiros para garantir que as máquinas no catálogo sejam consistentes.

Tipos de área de trabalho (experiência de área de trabalho)

Esta página é exibida somente quando você está criando um catálogo contendo máquinas de SO de sessão única.

A página **Desktop Experience** determina o que ocorre cada vez que um usuário faz logon. Selecione um dos seguintes:

- Os usuários se conectam a uma nova área de trabalho (aleatória) cada vez que fazem logon.
- Os usuários se conectam à mesma área de trabalho (estática) cada vez que fazem logon.

Se você escolher a segunda opção e estiver usando o MCS para provisionar as máquinas, poderá configurar como as alterações do usuário à área de trabalho serão tratadas:

- Salvar as alterações do usuário à área de trabalho no disco local.
- Descartar as alterações do usuário e limpar a área de trabalho virtual quando o usuário fizer logoff. Selecione esta opção se você estiver usando a camada de personalização do usuário.

Imagem mestre

Esta página aparece somente quando você está usando o MCS para criar VMs.

Na página **Master image**, selecione a conexão com o host e, em seguida, selecione o instantâneo ou a VM criada anteriormente. Se você estiver criando o primeiro catálogo, a única conexão disponível será aquela que você configurou quando criou o site.

Lembre-se:

- Quando você estiver usando o MCS, não execute o Sysprep em imagens mestras.
- Se você especificar uma imagem mestre em vez de um instantâneo, o Web Studio criará um instantâneo, mas não poderá dar-lhe um nome.

Para permitir o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tem a versão mais recente do VDA instalada. Não altere a seleção de VDA mínimo padrão. No entanto, se você precisar usar uma versão anterior do VDA, consulte Versões do VDA e níveis funcionais.

Uma mensagem de erro será exibida se você selecionar um instantâneo ou VM que não seja compatível com a tecnologia de gerenciamento de máquina selecionada anteriormente no assistente.

Máquinas

Esta página não aparece quando você está criando catálogos de Remote PC Access.

O título desta página depende do que você selecionou na página **Machine Management**: **Machines**, **Virtual Machines** ou **VMs and users**.

Quando usar o MCS:

- Especifique quantas máquinas virtuais criar.
- Escolha a quantidade de memória (em MB) que cada VM tem.
- Cada VM criada tem um disco rígido. Seu tamanho é definido na imagem mestre. Não é possível alterar o tamanho do disco rígido no catálogo.
- Se a sua implantação contém mais de uma zona, você pode selecionar uma zona para o catálogo.

- Se você estiver criando VMs de áreas de trabalho estáticas, selecione um modo de cópia de máquina virtual. Veja Modo de cópia da máquina virtual
- Se você estiver criando VMs de áreas de trabalho aleatórias que não usam vDisks, você pode configurar um cache para ser usado para dados temporários em cada máquina. Veja Configurar cache para dados temporários.

Quando usar outras ferramentas:

Adicione (ou importe uma lista de) nomes de contas de máquinas do Active Directory. Você pode alterar o nome da conta do Active Directory de uma VM depois de adicioná-la ou importá-la. Se você especificou máquinas estáticas na página **Desktop Experience**, poderá, opcionalmente, especificar o nome de usuário do Active Directory para cada VM que você adicionar.

Depois de adicionar ou importar nomes, você pode usar o botão **Remove** para excluir nomes da lista, enquanto ainda estiver na página.

Ao usar outras ferramentas (mas não o MCS):

Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada) ajudam a identificar máquinas que podem não estar qualificadas para serem adicionadas ao catálogo ou que não podem se registrar com um Delivery Controller. Para obter detalhes, consulte Versões do VDA e níveis funcionais.

Adicionar SIDs ao criar máquinas virtuais

Agora você pode adicionar o parâmetro `ADAccountSid` para identificar as máquinas de forma exclusiva ao criar novas máquinas virtuais.

Para isso:

1. Crie um catálogo com o tipo de identidade compatível.
2. Adicione máquinas ao catálogo usando `NewProvVM`. Por exemplo:

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
     )  -RunAsynchronously
2 <!--NeedCopy-->
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta do AD que não está no pool de identidades do catálogo
- Uma conta do AD que não está no estado disponível

Modo de cópia da máquina virtual

O modo de cópia que você especificar na página **Machines** determina se o MCS cria clones thin (cópia rápida) ou thick (cópia completa) a partir da imagem mestre. (Padrão = clones thin)

- Use clones de cópia rápida para uma utilização de armazenamento mais eficiente e criação de máquinas mais rápida.
- Use clones de cópia completa para melhorar o suporte a migração e recuperação de dados, com IOPS potencialmente reduzido após a criação das máquinas.

Versões 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 de produtos requer um novo VDA. Definir um nível funcional disponibiliza todos os recursos introduzidos nessa versão (e posterior, se o nível funcional não for alterado) para as máquinas no catálogo. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não podem ser registradas.

Um menu perto da parte inferior da página **Machines** (ou **Devices**) permite que você selecione o nível mínimo do 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 com a versão mais recente, não será necessário alterar essa seleção. No entanto, se você deve continuar usando versões VDA mais antigas, selecione o valor correto.

Uma versão do Citrix Virtual Apps and Desktops pode não incluir uma nova versão de VDA, ou o novo VDA não afeta o nível funcional. Nesses casos, o nível funcional pode indicar uma versão de VDA que é anterior aos componentes instalados ou atualizados. Por exemplo, embora a versão 7.17 contenha um VDA 7.17, o nível funcional padrão ("7.9 or later") permanece o mais atual. Portanto, após instalar ou atualizar componentes 7.9—7.16 para 7.17, você não precisa alterar o nível funcional padrão. O artigo O que há de novo de cada versão indica as alterações no nível funcional padrão.

O nível funcional selecionado afeta a lista de máquinas acima dele. Na lista, uma dica de ferramenta ao lado de cada entrada indica se o VDA da máquina é compatível com o catálogo naquele nível funcional.

As mensagens são postadas na página se o VDA em cada máquina não atender ou exceder o nível funcional mínimo selecionado. Você pode continuar com o assistente. Essas máquinas provavelmente não serão capazes de 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-los de volta ao catálogo.
- Escolha um nível funcional mais baixo que impeça o acesso aos recursos mais recentes do produto.

Uma mensagem também é postada se uma máquina não for adicionada ao catálogo porque o tipo de máquina não é adequado. Exemplos incluem a tentativa de adicionar um servidor a um catálogo

de SO de sessão única ou adicionar uma máquina de SO de sessão única criada originalmente para alocação aleatória a um catálogo de máquinas estáticas.

> **Importante:**
>
> Na versão 1811, um nível funcional extra foi adicionado: **1811 (or newer)**. Esse nível é destinado ao uso com futuros recursos do Citrix Virtual Apps and Desktops. A seleção **7.9 (or newer)** continua a ser o padrão. Esse padrão é válido para todas as implantações agora.
>
> Se você selecionar **1811 (or newer)**, todas as versões anteriores do VDA no catálogo não conseguirão se registrar em um Controller. No entanto, se o catálogo contiver apenas VDAs 1811 ou versões suportadas posteriores, todos eles estarão qualificados para se registrar. Isso inclui catálogos contendo VDAs configurados para versões posteriores do Citrix Virtual Apps and Desktops, incluindo a versão 1903 e outras versões 19XX anteriores à versão atual.

Configurar cache para dados temporários

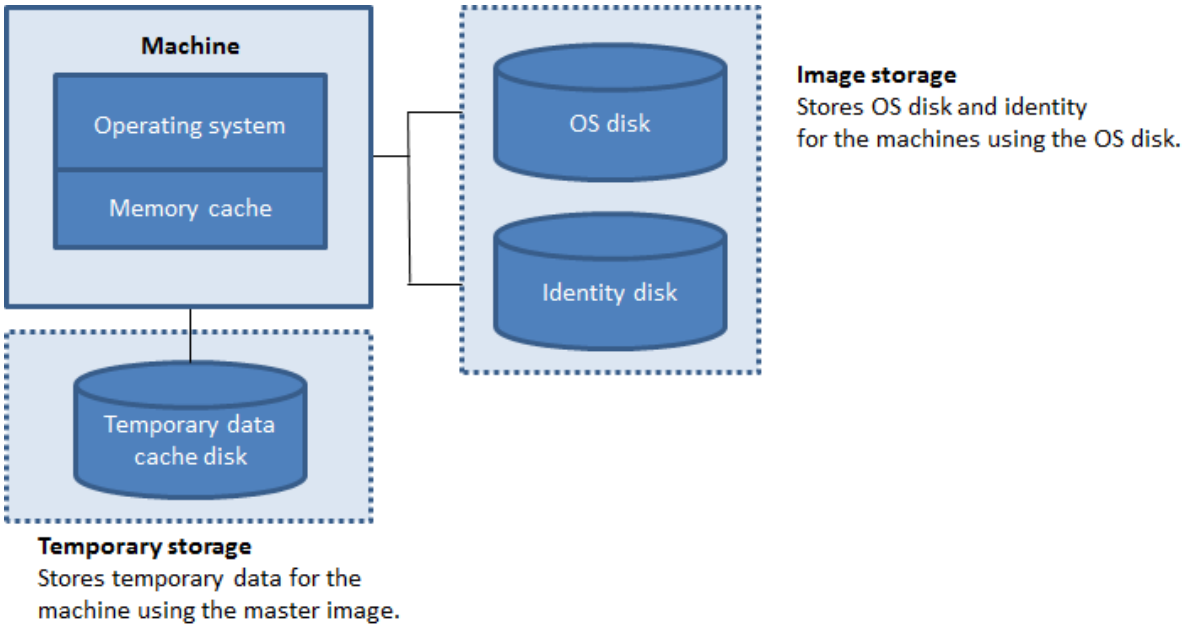
O armazenamento em cache de dados temporários localmente na VM é opcional. Você pode habilitar o uso do cache de dados temporários na máquina quando usar o MCS para gerenciar máquinas em pool (não dedicadas) em um catálogo. Se o catálogo usar uma conexão que especifique armazenamento para dados temporários, você pode ativar e configurar as informações do cache de dados temporários quando criar o catálogo.

> **Importante:**
>
> Esse recurso requer um driver de MCS I/O atual. Instalar esse driver é uma opção quando você instala ou atualiza 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: **Memory allocated to cache (MB)** e **Disk cache size (GB)**. Por padrão, as duas opções estão desmarcadas. Para habilitar a opção Memory allocated to cache (MB), marque a caixa de seleção Disk cache size (GB). Se a caixa de seleção **Disk cache size** não estiver marcada, a opção **Memory allocated to cache** fica acinzentada. Dependendo do tipo de conexão, os valores padrão para essas opções podem ser diferentes. Geralmente, os valores padrão são suficientes para a maioria dos casos. No entanto, leve em consideração o espaço necessário para:

- Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
- Dados de perfil do usuário.
- Dados do ShareFile que são sincronizados com as sessões de usuários.

- Dados que podem ser criados ou copiados por um usuário da sessão ou por qualquer aplicativo que os usuários possam instalar dentro da sessão.



Para configurar um cache para dados temporários em cada máquina, considere os três cenários a seguir:

- Se você não marcar a caixa de seleção Disk cache size e a caixa de seleção Memory allocated to cache, os dados temporários não serão armazenados em cache. Eles serão gravados diretamente no disco de diferença (localizado no armazenamento do sistema operacional) para cada VM. (Esta é a ação de provisionamento na versão 7.8 e anterior.)
- Se você marcar a caixa de seleção Disk cache size e não marcar a caixa de seleção Memory allocated to cache, os dados temporários serão gravados diretamente no disco de cache, usando uma quantidade mínima de cache de memória.
- Se você marcar a caixa de seleção Disk cache size e a caixa de seleção Memory allocated to cache, os dados temporários serão inicialmente gravados no cache de memória. Quando o cache de memória atinge seu limite configurado (o valor em Memory allocated to 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 ficará inutilizável.
> - Esse recurso não está disponível quando você usa uma conexão de host Nutanix.
> - Não é possível alterar os valores de cache em um catálogo de máquinas após a máquina ser criada.
>
> **Nota:**

> - O cache de memória faz parte da quantidade total de memória em cada máquina. Portanto, se você ativar a opção Memory allocated to cache, considere aumentar a quantidade total de memória em cada máquina.
> - Alterar o tamanho do cache em disco em Disk cache size para o 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 quando você está criando catálogos de Remote PC Access.

Na página **Network Interface Cards**, se você planeja usar várias NICs, associe uma rede virtual a cada placa. Por exemplo, você pode atribuir uma placa para acessar uma rede segura específica e outra placa para acessar uma rede mais comumente usada. Você também pode adicionar ou remover NICs a partir dessa página.

Contas de máquina

Esta página é exibida somente ao criar catálogos de Remote PC Access.

Na página **Machine Accounts**, especifique as contas de máquina do Active Directory ou Unidades Organizacionais (UOs) para adicionar que correspondam a usuários ou grupos de usuários. Não use barra (/) no nome de uma unidade organizacional.

Ao adicionar UOs, você pode fazer o seguinte se o domínio não for mostrado na lista:

- Procure por ele usando uma correspondência exata.
- Navegue por todos os domínios para encontrá-lo.

Você pode escolher uma conexão de gerenciamento de energia configurada anteriormente ou optar por não usar o gerenciamento de energia. Se quiser usar o gerenciamento de energia, mas uma conexão adequada ainda não tiver sido configurada, você pode criar essa conexão mais tarde e, então, editar o catálogo de máquinas para atualizar as configurações de gerenciamento de energia.

Contas de computador

Esta página aparece somente ao usar o MCS para criar VMs.

Cada máquina no catálogo deve ter uma conta de computador correspondente do Active Directory. Na página **Computer Accounts**, indique se deseja criar contas ou usar contas existentes, e o local dessas contas.

- Se você criar contas, deverá ter permissão para criar contas de computador na UO em que as máquinas residem.

  Selecione um domínio para essas contas. Se o domínio não for exibido na lista, você pode fazer o seguinte:

  - Procure por ele usando uma correspondência exata.
  - Navegue por todos os domínios para encontrá-lo.

  Especifique o esquema de nomenclatura de conta para a máquina usando marcas de hash para indicar onde os números ou letras sequenciais aparecem. Não use barra (/) no nome de uma unidade organizacional. 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 com os nomes 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 **Import** e especifique o arquivo .csv que contém o nome das contas. O conteúdo do arquivo importado deve usar o formato:

```
[ADComputerAccount]
ADcomputeraccountname.domain
...
<!--NeedCopy-->
```

Certifique-se de que haja contas suficientes para todas as máquinas que você está adicionando. O Web Studio gerencia essas contas, portanto, permita que o Web Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

Para catálogos contendo máquinas físicas ou máquinas existentes, selecione ou importe as contas existentes. Atribua cada máquina a uma conta de computador do Active Directory e a uma conta de usuário.

Resumo, nome e descrição

Na página **Summary**, revise as configurações especificadas. Insira um nome e uma descrição para o catálogo. Essas informações são exibidas no Web Studio.

Quando terminar, clique em **Finish** para iniciar a criação do catálogo.

Localização do arquivo de paginação

Em ambientes do Azure, o arquivo de paginação é configurado no local apropriado quando a VM é criada. A configuração do arquivo de paginação é definida no formato `<page file location>[min size] [max size]` (o tamanho está em MB). Para obter mais informações, consulte o documento da Microsoft Como determinar o arquivo de paginação apropriado.

Quando você cria `ProvScheme` durante a preparação da imagem, o MCS determina a localização do arquivo de paginação com base em determinadas regras. Depois de criar `ProvScheme`:

- A alteração do tamanho da VM será bloqueada se o tamanho da VM de entrada fizer com que a configuração do arquivo de paginação seja diferente.
- A atualização do perfil da máquina será bloqueada se a oferta de serviço for alterada devido à atualização do perfil da máquina que faz com que a configuração do arquivo de paginação seja diferente.
- As propriedades do disco do SO efêmero (EOS) e MCSIO não podem ser alteradas.

Determinação da localização do arquivo de paginação

Os recursos como EOS e MCSIO têm seu próprio local de arquivo de paginação esperado e são exclusivos entre si. A tabela mostra a localização esperada do arquivo de paginação para cada recurso:

Recurso	Local esperado do arquivo de paginação
EOS	Disco do sistema operacional
MCSIO	Disco temporário do Azure primeiro, caso contrário, disco de cache de write-back

> **Nota:**
>
> Mesmo que a preparação da imagem seja dissociada da criação do esquema de provisionamento, o MCS determina corretamente o local do arquivo de paginação. O local padrão do arquivo de paginação é o disco do SO.

Cenários de configuração do arquivo de paginação

A tabela descreve alguns cenários possíveis de configuração do arquivo de paginação durante a preparação da imagem e a atualização do esquema de provisionamento:

Durante	Cenário	Resultado
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco temporário, enquanto o tamanho da VM especificado no esquema de provisionamento não tem disco temporário	O arquivo de paginação é colocado no disco do SO
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco do SO, enquanto o tamanho da VM especificado no esquema de provisionamento tem disco temporário.	O arquivo de paginação é colocado no disco temporário.
Preparação da imagem	O arquivo de paginação de imagem de origem é definido no disco temporário, enquanto o disco de SO efêmero é ativado no esquema de provisionamento.	O arquivo de paginação é colocado no disco do SO
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento, o tamanho original da VM tem disco temporário e a VM de destino não tem disco temporário.	Rejeita a alteração com uma mensagem de erro
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento, o tamanho original da VM não tem disco temporário e a VM de destino tem disco temporário	Rejeita a alteração com uma mensagem de erro

Atualizar configuração do arquivo de paginação

Você também pode especificar a configuração do arquivo de paginação, incluindo o local e o tamanho, usando explicitamente o comando PoSH. Isso substitui o valor determinado pelo MCS. Você pode fazer isso executando o comando `New-ProvScheme` e incluindo as seguintes propriedades person-

alizadas:

- `PageFileDiskDriveLetterOverride`: letra da unidade de disco do local do arquivo de paginação
- `InitialPageFileSizeInMB`: tamanho inicial do arquivo da paginação em MB
- `MaxPageFileSizeInMB`: tamanho máximo do arquivo de paginação em MB

Exemplo de uso das propriedades personalizadas:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

Restrições:

- Você pode atualizar a configuração do arquivo de paginação somente quando cria o esquema de provisionamento executando o comando `New-ProvScheme`, e a configuração do arquivo de paginação não pode ser alterada posteriormente.
- Forneça todas as propriedades relativas da configuração do arquivo de paginação (`PageFileDiskDriveL` , `InitialPageFileSizeInMB` e `MaxPageFileSizeInMB`) nas propriedades personalizadas ou não forneça nenhuma delas.
- O tamanho inicial do arquivo de paginação deve estar entre 16 MB e 16777216 MB.
- O tamanho máximo do arquivo de paginação deve ser maior ou igual ao tamanho inicial do arquivo de paginação e menor que 16777216 MB.
- Esse recurso não é compatível com o Web Studio.

Sincronização de horário do MCS

A sincronização de horário é determinada pela imagem principal e pelo tipo de identidade da máquina ingressada no catálogo. Você obtém o seguinte método de sincronização de horário de acordo com a imagem mestre e o catálogo:

Imagem mestre	Catálogo	Método de sincronização de horário resultante
NDJ	AD ou Azure AD híbrido	Por padrão, NT5DS. Você pode impedir que o MCS altere a configuração de sincronização de horário usando as configurações do registro na imagem mestre
NDJ	NDJ ou Azure AD	Igual à configuração original de sincronização de horário
AD ou Azure AD híbrido	AD ou Azure AD híbrido	Igual à configuração original de sincronização de horário
Azure AD	Azure AD	Igual à configuração original de sincronização de horário

> **Nota:**
>
> A sincronização de horário original é controlada pela seguinte configuração do registro e não pode ser alterada:
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Valor: MaxAllowedPhaseOffset, MaxNegPhaseCorrection and MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> Valor: Type

Para impedir que o MCS altere a configuração de sincronização de horário, defina o valor da seguinte configuração de registro na imagem mestre:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nome: TimeSyncMethodKeep
- Tipo: DWORD
- 0 (Ou valor TimeSyncMethodKeep não configurado): não mantém a configuração original de sincronização de horário.
- 1: Mantém a configuração original de sincronização de horário e os valores dos parâmetros padrão.

Solucionar problemas

> **Importante:**
>
> Depois de criar o catálogo da máquina usando o Web Studio, você não pode mais usar o comando `Get-ProvTask` do PowerShell para recuperar as tarefas associadas à criação do catálogo de máquinas. Essa restrição é resultado da exclusão de tarefas pelo Web Studio após a criação do catálogo de máquinas, independentemente de o catálogo ter sido criado com sucesso.

A Citrix recomenda a coleta de logs para ajudar a equipe de suporte a fornecer soluções. Quando 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 do PowerShell: `Set-ProvServiceConfiguration -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Crie um catálogo com base nesse instantâneo.
5. Quando a VM de preparação for criada no hipervisor, faça login e extraia os seguintes arquivos da raiz de C:\: Image-prep.log e PvsVmAgentLog.txt.
6. Desligue a máquina, momento esse em que ela informa a falha.
7. Execute o seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Problemas de preparação de imagem

Como o MCS cria muitas máquinas a partir de uma única imagem, algumas etapas são executadas para garantir que todas as máquinas sejam exclusivas e licenciadas corretamente. A preparação da imagem faz parte do processo de criação do catálogo. Essa preparação garante que todas as máquinas provisionadas tenham endereços IP exclusivos e se anunciem corretamente ao servidor KMS como instâncias exclusivas. Dentro do MCS, a preparação da imagem ocorre após selecionar o instantâneo da imagem mestre. Uma cópia é feita para permitir que o catálogo se isole da máquina selecionada. A *preparação* da VM é criada, com base na VM original, mas com a conexão de rede desconectada. Desconectar a conexão de rede evita conflitos com outras máquinas, garantindo ao mesmo tempo que a VM preparada seja conectada apenas ao disco recém-copiado.

Um pequeno disco de *instrução*, contendo as etapas necessárias para executar a preparação da imagem, é anexado à VM preparada. A VM preparada é iniciada e o processo de preparação da imagem começa. A preparação da imagem inclui os seguintes processos:

- Ativar DHCP. A ativação de DHCP garante que as máquinas provisionadas não causem conflitos de endereço IP. O DHCP está ativado em todas as placas de rede.
- Rearmar Microsoft Windows KMS. A rearmação de KMS garante que o Microsoft Windows seja licenciado corretamente. O sistema operacional rearmado é invocado de modo que seja corretamente indicado como uma nova instância ao servidor de licenças KMS.
- Rearmar Microsoft Office KMS (se o Microsoft Office estiver instalado). A rearmação do Microsoft Office garante que qualquer versão do Microsoft Office (2010+) seja registrada corretamente no servidor KMS. Depois que a rearmação do Microsoft Office é invocada, ela é indicada como uma nova instância para o servidor de licenças KMS.

> **Dica:**
>
> Quando o processo de preparação da imagem termina, o disco de instruções é obtido a partir do hipervisor. O hipervisor contém as informações obtidas a partir do processo de preparação da imagem.

Existem várias razões pelas quais o estágio de preparação da imagem pode falhar. É exibida uma mensagem de falha semelhante à seguinte: Image Preparation Office Rearm Failed.

Essas falhas são tratadas abaixo.

Ativar DHCP Esses erros são causados por placas de rede que não suportam endereços IP estáticos. Por exemplo, versões anteriores das placas de rede Dell SonicWall. A operação falha porque a placa SonicWall é uma placa de rede de firewall, portanto, definir a placa como DHCP não faz sentido, pois ela só suporta DHCP. Isso foi corrigido em versões posteriores do Citrix Virtual Apps and Desktops. No entanto, se ocorrer com outros tipos de placa de rede, deve ser informado à Citrix por meio dos fóruns ou do seu contato de suporte.

> **Nota:**
>
> A configuração do PowerShell nos exemplos a seguir é aplicada ao site Citrix Virtual Apps and Desktops, por isso afeta todos os novos catálogos e atualizações de imagem executadas em catálogos existentes.

Se você tiver esse problema com outras placas de rede, pode resolvê-lo executando um comando PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Rearmar Microsoft Office Há vários erros de rearmação KMS que podem acontecer durante o estágio de rearmação do Microsoft Office. As principais falhas são:

- Alguns runtimes do Microsoft Office, por exemplo, **Access Runtime**, podem invocar a rearmação do Office, fazendo com que apresente falha.
- Versão KMS do Microsoft Office não instalada.
- Contagem de rearmação excedida.

Se o erro for um falso positivo, você pode resolvê-lo executando o seguinte comando doo PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```

Rearmar Microsoft Windows Várias falhas de KMS podem ocorrer durante o estágio de rearmação do Microsoft Windows. As principais falhas são:

- A versão do Windows instalada não é ativada usando o KMS. Por exemplo, ela está usando uma chave de ativação múltipla (MAK).
- Contagem de rearmação excedida.

Se a versão do Microsoft Windows estiver licenciada corretamente, você poderá limpar a rearmação do sistema operacional executando o seguinte comando PowerShell no Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

Instâncias de falha total A máquina de preparação de imagem não está conectada à rede por design, o que significa que às vezes o estágio de preparação da imagem só pode informar uma falha total. Um exemplo desse tipo de falha lembra: Preparation of the Master VM Image failed. Verifique se a imagem selecionada tem um sistema operacional compatível (por exemplo, Windows 7) e a versão correta do VDA (7.0 ou posterior) instalada.

As principais razões para uma falha total são:

Virtual Delivery Agent (VDA) não está instalado, ou o VDA versão 5.x está instalado Se o VDA 7.x não estiver instalado na imagem mestre, o tempo de preparação da imagem se esgota após 20 minutos e informa o erro acima. Isso ocorre porque não há nenhum software instalado na imagem mestre para executar o estágio de preparação da imagem e informar seu sucesso ou falha. Para resolver isso, verifique se o VDA (versão mínima 7) está instalado no instantâneo selecionado como a imagem mestre.

Política de `DISKPART SAN` Todo o estágio de preparação da imagem pode falhar devido à política `DISKPART SAN` definida na imagem mestre. Se não estiver definida para colocar o disco de in-

struções de preparação da imagem online, a máquina é desligada e a preparação da imagem informa uma falha após 20 minutos. Para verificar isso na imagem mestre, execute os seguintes comandos:

```
C:>; Diskpart.exe
DISKPART>; San
<!--NeedCopy-->
```

Este comando retorna a política atual. Se não for *Online All*, altere o valor executando o seguinte comando:

```
DISKPART>; San policy=OnlineAll
```

Desligue a imagem mestre, crie um instantâneo da máquina e use-o como a imagem base do MCS.

Se a preparação da imagem falhar por outro motivo Se a preparação da imagem apresentar falha e não houver motivo claro para isso, você pode ignorar o processo de preparação da imagem quanto estiver criando um catálogo MCS. No entanto, ignorar o processo pode causar problemas com a licença e a rede de KMS (DHCP) em seu site. Use o seguinte comando do PowerShell:

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
<!--NeedCopy-->
```

Sempre que possível, colete os logs para a equipe de suporte da Citrix, informando o problema à Citrix por meio dos fóruns ou do seu contato de suporte. Para coletar logs:

1. Na imagem mestre, crie a seguinte chave de registro com o valor 1 (como um "valor DWORD (32 bits)"): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Desligue a imagem mestre e crie um instantâneo. No Delivery Controller, inicie o PowerShell com os snap-ins do Citrix PowerShell carregados e execute `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Crie um catálogo com base nesse instantâneo.
4. Quando a VM de preparação for criada no hipervisor, faça login e extraia da raiz de C: os arquivos:

```
Image-prep.log
PvsVmAgentLog.txt
<!--NeedCopy-->
```

Desligue a máquina. Nesse ponto, ela informa a falha.

Execute a partir do seguinte comando PowerShell para reativar o desligamento automático das máquinas de preparação de imagem:

```
Remove-ProvServiceConfigurationData -Name
ImageManagementPrep_NoAutoShutdown
```


O que fazer a seguir

Se este for o primeiro catálogo criado, o Web Studio orientará você para criar um grupo de entrega.

Gerenciar catálogos de máquinas

April 3, 2024

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Você pode adicionar ou remover máquinas a partir de um catálogo de máquinas, renomear, alterar a descrição ou gerenciar contas de computador do Active Directory de um catálogo.

A manutenção de catálogos também pode incluir garantir que cada máquina tenha as atualizações mais recentes do sistema operacional. Inclusive atualizações antivírus, atualizações do sistema operacional ou alterações de configuração.

- Catálogos contendo máquinas em pool aleatórias criadas usando o Machine Creation Services (MCS) fazem a manutenção das máquinas atualizando a imagem mestre usada no catálogo e, depois, atualizando as máquinas. Esse método permite que você atualize eficientemente um grande número de máquinas de usuário.
- Para catálogos contendo máquinas estáticas e permanentemente atribuídas e para catálogos de máquinas de Remote PC Access, as atualizações de máquinas de usuários são realizadas fora do Web Studio. Usando ferramentas de distribuição de software de terceiros, execute a tarefa individualmente ou coletivamente.

Para obter informações sobre como criar e gerenciar conexões com hipervisores de host, consulte Conexões e recursos.

> **Nota:**
>
> O MCS não suporta o Windows 10 IoT Core e Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

Sobre instâncias persistentes

Ao atualizar um catálogo MCS criado usando instâncias persistentes ou dedicadas, as novas máquinas criadas para o catálogo usam a imagem atualizada. As instâncias pré-existentes continuam a usar a instância original. O processo de atualização de uma imagem é feito da mesma maneira para todos os outros tipos de catálogo. Considere o seguinte:

- Em catálogos de discos persistentes, as máquinas pré-existentes não são atualizadas com a nova imagem, mas todas as novas máquinas adicionadas ao catálogo usam a nova imagem.
- Em catálogos de discos não permanentes, a imagem da máquina é atualizada na próxima vez que a máquina for redefinida.
- Em catálogos de máquinas persistentes, atualizar a imagem também atualiza as instâncias do catálogo que usam a imagem.
- Em catálogos que não persistem, se você quiser ter imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

Adicionar máquinas a um catálogo

Antes de começar:

- Certifique-se de que o host de virtualização tem processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- É necessário ter contas de computador do Active Directory não utilizadas em quantidade suficiente. Se estiver usando contas existentes, o número de máquinas que você pode adicionar é limitado pelo número de contas disponíveis.
- Se usar o Web Studio para criar contas de computador do Active Directory para as máquinas adicionais, você precisa ter permissão apropriada de administrador de domínio.

Para adicionar máquinas a um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo de máquinas e, em seguida, selecione **Add Machines** na barra de ações.
4. Selecione o número de máquinas virtuais a serem adicionadas.
5. Se não houver contas existentes do Active Directory suficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas. Especifique um esquema de nomenclatura de conta usando marcas de hash para indicar onde os números ou letras sequenciais aparecem. Não use barra (/) no nome de uma unidade organizacional. 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 com os nomes PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

6. Se você usar contas existentes do Active Directory, navegue até as contas ou clique em **Import** e especifique o arquivo .csv que contém o nome das contas. Verifique se há contas suficientes para todas as máquinas que você está adicionando. O Web Studio gerencia essas contas. Permita que o Web Studio redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

As máquinas são criadas como um processo em segundo plano, podendo levar bastante tempo quando muitas máquinas são criadas. A criação da máquina continua mesmo se você fechar o Web Studio.

Recuperar avisos associados a um catálogo

Você pode receber avisos para entender os problemas com o seu catálogo MCS e corrigi-los. Os avisos, diferentemente dos erros, não fazem com que uma tarefa de provisionamento iniciada falhe.

Usando os comandos do PowerShell, você pode:

- Obter uma lista de avisos
- Alterar o estado do aviso de New para Acknowledged
- Excluir os avisos

Para executar os comandos do PowerShell:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.

Para obter uma lista de avisos:

Execute o comando `Get-ProvSchemeWarning`.

- Sem parâmetros: obtém todos os avisos
- Com o parâmetro `ProvisioningSchemeName` e `ProvisioningSchemeUid`: obtém todos os avisos para esse esquema de provisionamento
- Com o parâmetro `WarningId`: obtém o aviso que corresponde a esse ID de aviso

Para alterar o estado de aviso dos avisos de **New** to **Acknowledged**:

Execute `Set-ProvSchemeWarning`

- Com o parâmetro `WarningId`: define o estado de aviso de um aviso que corresponde a esse ID. Você pode obter o aviso como uma saída do comando `Get-ProvSchemeWarning`
- Com o parâmetro `ProvisioningSchemeName` ou `ProvisioningSchemeUid`: define o estado dos avisos de todos os avisos para esse esquema de provisionamento
- Com o parâmetro `All`: define o estado de todos os avisos como **Acknowledged**.

Para excluir os avisos:

Execute `Remove-ProvSchemeWarning`

- Com o parâmetro `WarningId`: remove um aviso específico que corresponde a esse ID. Você pode obter o aviso como uma saída de Get-ProvSchemeWarning
- Com o parâmetro `ProvisioningSchemeName` ou `ProvisioningSchemeUid`: remove todos os avisos associados a esse esquema de provisionamento.
- Com o parâmetro `All`: remove todos os avisos

Excluir máquinas de um catálogo

Depois de excluir uma máquina de um catálogo de máquinas, os usuários não podem mais acessá-la, portanto, antes de excluir uma máquina, certifique-se de que:

- Foi feito backup dos dados do usuário ou os dados não são mais necessários.
- Todos os usuários fizeram logoff. Ativar o modo de manutenção impede que sejam estabelecidas novas conexões a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **View Machines** na barra de ações.
4. Selecione uma ou mais máquinas e, em seguida, selecione **Delete** na barra de ações.

Escolha se deseja excluir as máquinas que estão sendo removidas. Se você optar por excluir as máquinas, indique se as contas do Active Directory dessas máquinas serão mantidas, desativadas ou excluídas.

Alterar uma descrição de catálogo ou alterar as configurações do Remote PC Access

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Edit Machine Catalog** na barra de ações.
4. Para o catálogo do Remote PC Access, use a página **Power Management** para alterar as configurações de gerenciamento de energia e selecionar uma conexão de gerenciamento de energia. Na página **Organizational Units**, adicione ou remova unidades organizacionais do Active Directory.
5. Na página **Description**, altere a descrição do catálogo.

Renomear um catálogo

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Rename Machine Catalog** na barra de ações.
4. Digite o novo nome.

Mover um catálogo para uma zona diferente

Se a sua implantação tiver mais de uma zona, você pode mover um catálogo de uma zona para outra.

Mover um catálogo para uma zona que não seja a do hipervisor que contém as VMs no catálogo afeta o desempenho.

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Move** na barra de ações.
4. Selecione a zona para onde deseja mover o catálogo.

Excluir um catálogo

Antes de excluir um catálogo, certifique-se de que:

- Todos os usuários fizeram logoff e não há sessões desconectadas em execução.
- O modo de manutenção está ativado para todas as máquinas do catálogo, de modo que novas conexões não possam ser estabelecidas.
- Todas as máquinas do catálogo estão desligadas.
- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Delete Machine Catalog** na barra de ações.
4. Indique se as máquinas no catálogo devem ser excluídas. Se você optar por excluir as máquinas, indique se as contas de computador do Active Directory dessas máquinas serão mantidas, desativadas ou excluídas.

Gerenciar contas de computador do Active Directory em um catálogo

Para gerenciar contas do Active Directory em um catálogo de máquinas, você pode:

- Liberar contas de máquina não utilizadas removendo contas de computador do Active Directory dos catálogos de SO de sessão única e SO multissessão. Essas contas poderão ser usadas para outras máquinas.
- Adicionar contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam em vigor. Não use barra (/) no nome de uma unidade organizacional.

Para gerenciar contas do Active Directory:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Manage AD accounts** na barra de ações.
4. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas das contas: redefinir todas elas ou inserir uma senha que se aplique a todas as contas.

   Você pode redefinir as senhas se não souber as senhas da conta atual, mas deve ter permissão para executar uma redefinição de senha. Ao inserir uma senha, a senha é alterada nas contas à medida que elas são importadas. Ao excluir uma conta, escolha se a conta no Active Directory deve ser mantida, desativada ou excluída.

Indique se as contas do Active Directory serão mantidas, desativadas ou excluídas quando você remover máquinas de um catálogo ou excluir um catálogo.

Atualizar um catálogo

Recomendamos que você salve cópias ou instantâneos de imagens mestre antes de atualizar as máquinas no catálogo. O banco de dados mantém um registro histórico das imagens mestre usadas com cada catálogo de máquinas. Reverta as máquinas em um catálogo para usar a versão anterior da imagem mestre. Execute esta tarefa se os usuários encontrarem problemas com atualizações implantadas em suas áreas de trabalho. Isso minimiza o tempo de inatividade do usuário. Não exclua, mova ou renomeie imagens mestre. Não é possível reverter um catálogo para usá-las.

Depois que uma máquina é atualizada, ela reinicializa automaticamente.

Atualizar ou criar uma imagem mestre

Antes de atualizar o catálogo da máquina, atualize uma imagem mestre existente ou crie uma no hipervisor do host.

1. No hipervisor, tire um instantâneo da VM atual e dê um nome significativo ao instantâneo. Esse instantâneo pode ser usado para reverter máquinas no catálogo, se necessário.
2. Se necessário, ligue a imagem mestre e faça logon.
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 facilmente reconhecido quando o catálogo for atualizado no Web Studio. Embora o Web Studio possa criar um instantâneo, a Citrix recomenda que você o crie usando o console de gerenciamento do hipervisor. Em seguida, selecione o instantâneo no Web Studio. Esse processo permite que você forneça um nome e uma descrição significativos em vez de um nome gerado automaticamente. Para imagens mestre de GPU, você pode alterar a imagem mestre somente por meio do console Citrix Hypervisor.

Alterar a imagem mestre

Para preparar e distribuir a atualização para todas as máquinas em um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione um catálogo e, em seguida, selecione **Change Master Image** na barra de ações.
4. Na página **Master Image**, selecione o host e a imagem que você deseja implantar.

   > **Dica:**
   >
   > Para um catálogo criado pelo MCS, você pode anotar sua imagem adicionando uma nota para a imagem. Uma nota pode conter até 500 caracteres. Cada vez que você altera a imagem mestre, é criada uma entrada relacionada à nota se você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como null (-). Para exibir o histórico de notas da imagem, selecione o catálogo, clique em **Template Properties** no painel inferior e, em seguida, clique em **View note history**.

5. Na página **Rollout Strategy**, escolha quando as máquinas no catálogo de máquinas serão atualizadas com a nova imagem mestre: no próximo desligamento ou imediatamente.

   > **Nota:**
   >
   > A página **Rollout Strategy** não está disponível para VMs persistentes porque a implantação só se aplica a VMs não persistentes.

6. Verifique as informações na página **Summary** e clique em **Finish**. Cada máquina reinicializa automaticamente depois de ser atualizada.

Ao atualizar um catálogo usando o PowerShell SDK diretamente, em vez do Web Studio, especifique um modelo de hipervisor (**VMTemplates**). Use isso como alternativa a uma imagem ou instantâneo de uma imagem.

Estratégia de implantação:

A atualização da imagem no próximo desligamento afetará imediatamente todas as máquinas que não estejam em uso no momento, ou seja, máquinas que não têm uma sessão de usuário ativa. Um sistema que está em uso recebe a atualização quando a sessão ativa atual termina. Considere o seguinte:

- Novas sessões não podem ser iniciadas até que a atualização seja concluída nas máquinas aplicáveis.
- No caso de máquinas de SO de sessão única, as máquinas são imediatamente atualizadas quando não estão em uso ou quando os usuários não estão conectados.
- No caso de um SO de sessão única com máquinas secundárias, as reinicializações não ocorrem automaticamente. Elas devem ser desligadas e reinicializadas manualmente.

> **Dica:**
>
> Limite o número de máquinas reinicializadas usando as configurações avançadas de uma conexão de host. Use essas configurações para modificar as ações tomadas para um determinado catálogo; as configurações avançadas variam dependendo do hipervisor.

Se você quiser ativar o agendamento de reinicialização única usando o PowerShell, use os seguintes comandos `BrokerCatalogRebootSchedule` do PowerShell para criar, modificar e excluir um agendamento de reinicialização:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Por exemplo,

- Para criar um agendamento de reinicialização das VMs no catálogo chamado **BankTellers** para começar em 3 de fevereiro de 2022, entre 2h e 4h.

```
1  C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
       CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
       02:00" -Enabled $true -RebootDuration 120
2  <!--NeedCopy-->
```

- Para criar um agendamento de reinicialização das VMs no catálogo com o UID 17 para começar em 3 de fevereiro de 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM é con-

figurada para exibir uma caixa de mensagem com o título **WARNING: Reboot pending** e a mensagem **Save your work** em cada sessão do usuário.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
<!--NeedCopy-->
```

- Para renomear o agendamento de reinicialização do catálogo chamado **Old Name** para **New Name**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
<!--NeedCopy-->
```

- Para exibir todos os agendamentos de reinicialização do catálogo com o UID 1 e renomear o agendamento de reinicialização do catálogo com o UID 1 para **New name**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Para definir o agendamento de reinicialização do catálogo chamado **Accounting** para exibir uma mensagem com o título **WARNING: Reboot pending** e a mensagem **Save your work** dez minutos antes da reinicialização de cada VM. A mensagem aparece em todas as sessões do usuário nessa VM.

  “‘

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage “Save your work”-WarningDuration 10 -WarningTitle “WARNING: Reboot pending”

- Para exibir todos os agendamentos de reinicialização que estão desativados e habilitar todos os agendamentos de reinicialização desativados.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Para definir o agendamento de reinicialização do catálogo com o UID 17 para exibir a mensagem **Rebooting in %m% minutes** quinze, dez e cinco minutos antes da reinicialização de cada VM.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
<!--NeedCopy-->
```

- Para configurar o fuso horário do catálogo chamado **MyCatalog**.


```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

Reverter a imagem mestre

Depois de implantar uma imagem mestre atualizada ou nova, você pode revertê-la. Esse processo pode ser necessário se ocorrerem problemas com as máquinas recentemente atualizadas. Quando você faz a reversão, as máquinas no catálogo voltam para a última imagem funcional. Os novos recursos que exigem a imagem mais recente não estarão mais disponíveis. Tal como acontece com a implantação, a reversão de uma máquina inclui uma reinicialização.

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione o catálogo e, em seguida, selecione **Roll Back Master Image** na barra de ações.
4. Especifique quando aplicar às máquinas a imagem mestre anterior, conforme descrito na seção anterior sobre a operação de implantação.

A reversão é aplicada apenas a máquinas que precisam ser revertidas. As máquinas que não são atualizadas com a imagem mestre nova ou atualizada não recebem mensagens de notificação e não são forçadas a fazer logoff.

Adicionando descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagens para catálogos de máquinas. Use esse recurso para adicionar uma descrição ao criar um catálogo ou ao atualizar uma imagem mestre existente para um catálogo. Você também pode exibir informações para cada imagem mestre no catálogo. Use os seguintes comandos para adicionar ou exibir descrições de imagens:

- Para adicionar uma nota ao criar um catálogo de máquinas com uma imagem mestre, use o parâmetro `MasterImageNote` no comando `NewProvScheme`. Por exemplo:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
<!--NeedCopy-->
```

- Para atualizar a imagem mestre associada a um catálogo de máquinas, use o parâmetro `MasterImageNote` no comando `Publish-ProvMasterVMImage`. Por exemplo:


```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
<!--NeedCopy-->
```

- Para exibir as informações de cada imagem, use o comando Get-ProvSchemeMasterVMImageHistory. Por exemplo:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
<!--NeedCopy-->
```

Para acompanhar o progresso da reversão, localize o catálogo em **Machine Catalogs** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em determinados cenários, incluindo os seguintes. (A opção **Roll Back Master Image** não fica visível.)

- Você não tem permissão para reverter.
- O catálogo não foi criado usando o MCS.
- O catálogo foi criado usando uma imagem do disco de SO.
- O instantâneo usado para criar o catálogo tornou-se corrompido.
- As alterações do usuário nas máquinas no catálogo não persistem.
- As máquinas no catálogo estão sendo executadas.

Alterar o nível funcional ou desfazer a alteração

Altere o nível funcional do catálogo de máquinas depois de atualizar os VDAs nas máquinas para uma versão mais recente. A Citrix recomenda atualizar todos os VDAs para a versão mais recente para permitir o acesso a todos os recursos novos.

Antes de alterar o nível funcional de um catálogo de máquinas:

- Inicie as máquinas atualizadas para que elas se registrem no Controller. Esse processo permite que o Web Studio determine se as máquinas no catálogo precisam ser atualizadas.

Para alterar o nível funcional de um catálogo:

1. Faça login no Web Studio.
2. Selecione **Machine Catalogs** no painel esquerdo.
3. Selecione o catálogo. A guia **Details** no painel inferior exibe informações da versão
4. Selecione **Change Functional Level**. Se o Web Studio detectar que o catálogo precisa de atualização, ele exibe uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser atualizadas, uma mensagem explica o motivo. Para garantir que todas as máquinas funcionem corretamente, a Citrix recomenda que você resolva o problema com as máquinas antes de clicar em **Change** para prosseguir.

Após a conclusão da alteração do catálogo, você pode reverter as máquinas para suas versões anteriores do VDA selecionando o catálogo e escolhendo **Undo Functional Level Change** na barra de ações.

Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Não é possível alterar as configurações associadas ao sistema operacional e gerenciamento da máquina. O catálogo clonado herda essas configurações do original.
- A clonagem de um catálogo pode levar algum tempo para ser concluída. Se necessário, selecione **Hide progress** para executar a clonagem em segundo plano.
- O catálogo clonado herda o nome do original e tem um sufixo `Copy`. Você pode mudar o nome. Consulte Renomear um catálogo.
- Após a conclusão da clonagem, atribua o catálogo clonado a um grupo de entrega.

1. Entre no Web Studio e selecione **Machine Catalogs** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Clone** na barra de ações.
3. Na janela **Clone Selected Machine Catalog**, exiba as configurações do catálogo clonado e defina as configurações conforme aplicável. Selecione **Next** para prosseguir para a próxima página.
4. Na página **Summary**, exiba um resumo das configurações e selecione **Finish** para iniciar a clonagem.
5. Se necessário, selecione **Hide progress** para executar a clonagem em segundo plano.

Organizar catálogos usando pastas

Você pode criar pastas para organizar catálogos para facilitar o acesso. Por exemplo, você pode organizar catálogos por tipo de imagem ou por estrutura da organização.

Criar uma pasta de catálogo

Antes de começar, primeiro planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas com até cinco níveis de profundidade (excluindo a pasta raiz padrão).
- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós no Web Studio (como os nós **Machine Catalogs** e **Applications**) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outros nós ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nos diferentes nós.

Para criar uma pasta de catálogo, siga estas etapas:

1. Selecione **Machine Catalogs** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Create Folder** na barra **Action**.
3. Insira um nome para a nova pasta e clique em **Done**.

> **Dica:**
>
> Se você criar uma pasta em um local não desejado, poderá arrastá-la para o local correto.

Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. Selecione **Machine Catalogs** no painel esquerdo.
2. Exiba os catálogos por pasta. Você também pode ativar **View all** acima da hierarquia de pastas para exibir todos os catálogos de uma vez só.
3. Clique com o botão direito do mouse em um catálogo e selecione **Move Machine Catalog**.
4. Selecione a pasta para a qual deseja mover o catálogo e clique em **Done**.

> **Dica:**
>
> Você pode arrastar um catálogo para uma pasta.

Gerenciar pastas de catálogo

Você pode excluir, renomear e mover pastas de catálogo.

Você só poderá excluir uma pasta se ela e suas subpastas não contiverem catálogos.

Para gerenciar uma pasta, siga estas etapas:

1. Selecione **Machine Catalogs** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Action**, conforme necessário:
   - Para renomear a pasta, selecione **Rename Folder**.
   - Para excluir a pasta, selecione **Delete Folder**.
   - Para mover a pasta, selecione **Move Folder**.
3. Siga as instruções na tela para concluir as etapas restantes.

Alterar a configuração de rede de um esquema de provisionamento existente

Você pode alterar a configuração de rede de um esquema de provisionamento existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede.

> **Nota:**
>
> Esse recurso é compatível com o 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 chegar ao caminho de rede que deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Execute `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar a nova configuração de rede do esquema de provisionamento existente.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos em cada plataforma. As tags na tabela são representadas como “key”:”value”.

AWS

Nome do recurso	Marca
Disco de identificação	“Name”: “VMName_IdentityDisk”
	“XdConfig”: “XdProvisioned=true”

Nome do recurso	Marca
Imagem	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig”: “XdProvisioned=true”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “Description”: “XD NIC” “XdConfig”: “XdProvisioned=true”
Disco do sistema operacional	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “Name”: “VMName_rootDisk” “XdConfig”: “XdProvisioned=True”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true”
Instantâneo publicado	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
Template	Se não for um instantâneo da AMI do Volume Worker, “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true”

Nome do recurso	Marca
	[quando AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
VM in catalog	“XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [quando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
Volume worker AMI	“XdConfig”: “XdProvisioned=true”
Volume worker bootstraper	“Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [quando AwsCaptureInstanceProperties = true e AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “”
Volume worker instance	“Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true”

Azure

Nome do recurso	Marca
Disco de identificação	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Imagem	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Disco do sistema operacional	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Instantâneo publicado	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Resource group	“CitrixResource”: “Internal” CitrixSchemaVersion: 2.0
Storage account	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Disco WBC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”

> **Nota:**
>
> Uma VM não fica visível no inventário da Citrix se uma tag **CitrixResource** for adicionada para

> identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Google Cloud Platform

Nome do recurso	Marca
Disco de identificação	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Imagem	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disco do sistema operacional	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
PrepVM	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Instantâneo publicado	“CitrixResource”: “internal”
Storage bucket	“Citrixresource”: “internal”
Template	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
VM in catalog	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. O plug-in também adiciona esse rótulo para VMs provisionadas pelo MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. Você pode usar esse rótulo para filtrar por catálogo no console do GCP.
Disco WBC	“CitrixResource”: “internal” CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

> **Nota:**
>
> Uma VM não fica visível no inventário da Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Citrix Hypervisor

Nome do recurso	Marca
Disco básico publicado e sua cópia em cada rede ou armazenamento local	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disco de identificação	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disco do sistema operacional	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Prep VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disco WBC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

SCVMM

Nome do recurso	Marca
Prep VM	Cadeia de caracteres da marca: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Entrada de propriedade personalizada: “XdConfig:”XdProvisioned=True”
VM in catalog	Cadeia de caracteres da marca: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Entrada de propriedade personalizada: “XdConfig:”XdProvisioned=True”

VMware

Nome do recurso	Marca
Prep VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”
VM in catalog	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”

Solucionar problemas

- Para máquinas que apresentam o status “Power State Unknown”, consulte CTX131267 para obter instruções.
- Para corrigir VMs que mostram continuamente um estado de energia desconhecido, consulte How to fix VMs that continuously show an unknown power state.

Criar grupos de entrega

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

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 áreas de trabalho disponíveis para esses usuários.

Criar um grupo de entrega é a próxima etapa na configuração da implantação depois de 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. Há também recursos e configurações que você pode definir somente ao editar um grupo de entrega, não ao criá-lo.

No Remote PC Access, 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 Web Studio o orienta para o local correto para começar a criar um. Se você já criou um grupo de entrega e deseja criar outro, selecione **Grupos de entrega**. Selecione **Create Delivery Group** no painel de ações.
2. O assistente é iniciado em uma página de **introdução**, que você pode remover das futuras inicializações do assistente.
3. Depois, o assistente o orienta pelas páginas descritas na seção a seguir. Quando terminar cada página, clique em **Next** até chegar à página final.

Etapa 1. Máquinas

Na página **Machines**, selecione um catálogo e selecione o número de máquinas que deseja usar desse catálogo.

É bom saber:

- Pelo menos uma máquina deve permanecer não utilizada 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 máquinas (SO multissessão, SO de sessão única ou Remote PC Access). Em outras palavras, você não pode misturar tipos de máquina em um grupo de entrega. Da mesma forma, se a sua implantação tiver catálogos de máquinas Windows e catálogos de máquinas Linux, um grupo de entrega pode conter máquinas de qualquer tipo de sistema operacional, mas não ambos.
- A Citrix recomenda que você instale ou atualize todas as máquinas com a versão VDA mais recente. Atualize catálogos e grupos de entrega conforme necessário. Ao criar um grupo de entrega, se você selecionar máquinas com versões VDA diferentes instaladas, o grupo de entrega será compatível com a versão mais antiga do VDA. 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 somente os recursos que suportados no VDA 7.1. Isso significa que alguns recursos que exigem versões mais recentes do VDA não estarão disponíveis nesse grupo de entrega.
- Cada máquina em um catálogo de Remote PC Access é automaticamente associada a um grupo de entrega. Quando você cria um site do Remote PC Access, 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 com SingleSession
- ProvisioningType deve ser compatível
- PersistChanges deve ser compatível com MCS e Citrix Provisioning
- O catálogo RemotePC só é compatível com o catálogo RemotePC
- Verificação relacionada ao AppDisk

Etapa 2. Tipo de entrega, em Delivery Type

Esta página é exibida somente se você escolher um catálogo contendo máquinas de SO de sessão única estáticas (atribuídas).

Na página **Delivery Type**, escolha **Applications** ou **Desktops**. Você não pode ativar os dois.

Se você selecionou máquinas de um catálogo de SO multissessão ou de SO de sessão única aleatório (em pool), o tipo de entrega será considerado como sendo de aplicativos e áreas de trabalho: você pode entregar aplicativos, áreas de trabalho ou ambos.

Etapa 3. Usuários

Especifique os usuários e grupos de usuários que podem usar os aplicativos e áreas de trabalho no grupo de entrega.

Onde as listas de usuários são especificadas

As listas de usuários do Active Directory são especificadas quando você cria ou edita o seguinte:

- Lista de acesso de usuários a um site, que não é configurada através do Web Studio. Por padrão, a regra de política de direito ao aplicativo inclui todos. Consulte os cmdlets `BrokerAppEntitlementPolicyRule` do SDK do PowerShell para obter detalhes.
- Grupos de 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 determinado departamento, 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 Administração e Finanças acessem aplicativos A através de L.
- Configure as propriedades do aplicativo A para restringir a visibilidade apenas à equipe de Contas a Receber em Administração e Finanças.

Usuários autenticados e não autenticados

Existem dois tipos de usuários: autenticado e não autenticado (não autenticado também é chamado de anônimo). Você pode configurar um ou os dois tipos em um grupo de entrega.

- **Authenticated:** para acessar aplicativos e áreas de trabalho, os usuários e membros do grupo que você especificar por nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha no aplicativo StoreFront ou Citrix Workspace. Para grupos de entrega contendo máquinas de SO de sessão única, você pode importar dados do usuário (uma lista de usuários) posteriormente editando o grupo de entrega.
- **Unauthenticated (anonymous):** para grupos de entrega contendo máquinas de SO multissessão, você pode permitir que os usuários acessem aplicativos e áreas de trabalho sem apresentar credenciais para o aplicativo StoreFront ou Citrix Workspace. Por exemplo, em quiosques, o aplicativo pode exigir credenciais, mas o portal de acesso Citrix e as ferramentas não. Um grupo de usuários anônimos é criado quando você instala o primeiro Delivery Controller.

  Para conceder acesso a usuários não autenticados, cada máquina no grupo de entrega deve ter um VDA para o SO do Windows Server (versão mínima 7.6) instalado. Quando usuários não autenticados estão habilitados, você deve ter um armazenamento StoreFront não autenticado.

  Contas de usuários não autenticados são criadas sob demanda quando uma sessão é iniciada e são chamadas Anon*XYZ*, em que *XYZ* é um valor único de três dígitos.

  As sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desativadas automaticamente quando o cliente se desconecta. Não há suporte para reconexão, roaming entre clientes e controle de espaço de trabalho.

A tabela a seguir descreve as suas escolhas na página **Users**:

Ativar acesso para	Adicionar/atribuir usuários e grupos de usuários?	Ativar a caixa de seleção "Give access to unauthenticated users"?
Somente usuários autenticados	Sim	Não

Ativar acesso para	Adicionar/atribuir usuários e grupos de usuários?	Ativar a caixa de seleção "Give access to unauthenticated users"?
Somente usuários não autenticados	Não	Sim
Usuários autenticados e não autenticados	Sim	Sim

Etapa 4. Aplicativos

É bom saber:

- Não é possível adicionar aplicativos a grupos de entrega de acesso ao PC remoto.
- Por padrão, os novos aplicativos adicionados são colocados em uma pasta chamada Applications. Você pode especificar uma pasta diferente. Para obter detalhes, consulte o artigo 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 outro com o mesmo nome na pasta, você será solicitado a renomear o aplicativo que está adicionando. Se você recusar, o aplicativo é adicionado com um sufixo que o torna exclusivo dentro na pasta de aplicativos.
- Quando você adiciona um aplicativo a mais de um grupo de entrega, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para exibir o aplicativo em todos os grupos de entrega. Nesses casos, consulte um administrador com mais permissões ou estenda o seu escopo para incluir todos os grupos de entrega aos quais o aplicativo foi adicionado.
- Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade Application name (for user) no Web Studio; caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

Clique em **Add** para exibir as origens do aplicativo.

- **Menu From Start:** aplicativos que são detectados em uma máquina criada a partir da imagem mestre no catálogo selecionado. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados; selecione aqueles que deseja adicionar e clique em **OK**.
- **Manually:** aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. Selecionar essa fonte abre uma nova página na qual você especifica um aplicativo a ser adicionado das seguintes formas:
  - Digite o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários.

  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Browse**, insira as credenciais para acessar o VDA, aguarde até ser conectado ao VDA e selecione um aplicativo no VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.

- **Existing**: aplicativos adicionados anteriormente ao site, talvez em outro grupo de entrega. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Adicione os aplicativos e clique em **OK**.
- **App-V:** aplicativos em pacotes App-V. Quando você seleciona essa origem, uma nova página é iniciada na qual você seleciona o servidor App-V ou a biblioteca de aplicativos. Na exibição resultante, selecione os aplicativos que deseja adicionar e clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V.

Se a origem de um aplicativo ou um aplicativo não estiver disponível ou válido, ele não estará visível ou não poderá ser selecionado. Por exemplo, a origem **Existing** não está disponível se nenhum aplicativo tiver sido adicionado ao site. Ou um aplicativo pode não ser compatível com os tipos de sessão com suporte nas máquinas do catálogo selecionado.

Etapa 5. Áreas de trabalho

O título desta página depende do catálogo que você escolheu na página **Machines**:

- Se você escolheu um catálogo contendo máquinas em pool, a página será intitulada **Desktops**.
- Se você escolheu um catálogo contendo máquinas atribuídas e especificou “Desktops”no **Delivery Type** página, a página é intitulada **Desktop User Assignments**.
- Se você escolheu um catálogo contendo máquinas atribuídas e especificou “Applications”no **Delivery Type** página, a página é intitulada **Application Machine User Assignments**.

Clique em **Add**. Na caixa de diálogo:

- Nos campos Display name e Description, digite as informações a serem exibidas no aplicativo Citrix Workspace.
- Para adicionar uma restrição de marca a uma área de trabalho, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca na lista suspensa. Para obter mais informações, consulte Marcadores.
- Use os botões de opção para iniciar uma área de trabalho ou para atribuir uma máquina ao iniciar a área de trabalho. Os usuários podem ser todos que podem acessar esse grupo de entrega ou usuários e grupos de usuários específicos.
- Se o grupo contém máquinas atribuídas, especifique o número máximo de áreas de trabalho por usuário. Esse valor deve ser um ou maior.
- Ative ou desative a área de trabalho (para máquinas em pool) ou a regra de atribuição de área de trabalho (para máquinas atribuídas). Desativar uma área de trabalho interrompe a entrega da

área de trabalho. Desativar uma regra de atribuição de área de trabalho interrompe a atribuição automática da área de trabalho aos usuários.
- Quando terminar com a caixa de diálogo, clique em **OK**.

Máximo de instâncias de uma área de trabalho em um site (somente PowerShell)

Para configurar as instâncias máximas de uma área de trabalho no site (somente PowerShell):

- No PowerShell, use o cmdlet BrokerEntitlementPolicyRule apropriado com o parâmetro Max-PerEntitlementInstances. Por exemplo, o cmdlet a seguir modifica a regra `tsvda-desktop` para definir como dois as instâncias simultâneas máximas de uma área de trabalho permitidas no site. Quando há duas instâncias de área de trabalho em execução, ocorre um erro se um terceiro assinante tentar iniciar uma área de trabalho.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
   2
  ```

- Para obter instruções, use o cmdlet Get-Help. Por exemplo, `Get-Help Set-BrokerEntitlementPoli -Parameter MaxPerEntitlementInstances`.

Etapa 6. Resumo

Insira um nome para o grupo de entrega. Você também pode inserir (opcionalmente) uma descrição, que aparece no aplicativo Citrix Workspace e no Web Studio.

Revise as informações de resumo e clique em **Finish**.

Gerenciar grupos de entrega

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Este artigo descreve os procedimentos para gerenciar grupos de entrega a partir do console de gerenciamento. Além de alterar as configurações especificadas ao criar o grupo, você pode configurar outras configurações que não estão disponíveis quando você cria um grupo de entrega.

As categorias de procedimento incluem: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Prevent users from connecting to machines"é descrito na categoria de máquinas, mas também afeta os usuários. Se você não conseguir encontrar uma tarefa em uma categoria, procure em uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Aplicativos contém informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer permissões relacionadas à função interna de Administrador de grupos de entrega. Para obter detalhes, consulte Administração delegada.

Geral

- Alterar o tipo de entrega
- Alterar endereços do StoreFront
- Alterar o nível funcional
- Gerenciar grupos de entrega de Remote PC Access
- Organizar grupos de entrega usando pastas
- Gerenciar proteção de aplicativo

Alterar o tipo de entrega de um grupo de entrega

O tipo de entrega indica o que o grupo pode entregar: aplicativos, áreas de trabalho ou ambos.

Antes de alterar um tipo de **somente aplicativo** ou **áreas de trabalho e aplicativos** para **somente áreas de trabalho**, exclua todos os aplicativos do grupo.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Delivery Type**, selecione o tipo de entrega desejado.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Alterar endereços do StoreFront

1. Selecione **Delivery Groups** no painel esquerdo.

2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **StoreFront**, selecione ou adicione URLs do StoreFront. Esses URLs são usados pelo aplicativo Citrix Workspace, que é instalado em cada máquina do grupo de entrega.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Você também pode especificar endereços do servidor StoreFront selecionando **StoreFront** no painel esquerdo.

Alterar o nível funcional

Altere o nível funcional do grupo de entrega depois de atualizar os VDAs em suas máquinas e os catálogos de máquinas que contêm as máquinas usadas no grupo de entrega.

Antes de começar:

- Se você usar o Citrix Provisioning (anteriormente Provisioning Services), atualize a versão do VDA no console Citrix Provisioning.
- Inicie as máquinas que contêm o VDA atualizado para que possam se registrar em um Delivery Controller. Esse processo informa o console sobre o que precisa ser atualizado no grupo de entrega.
- Se você tiver que continuar usando versões anteriores do VDA, os novos recursos do produto não estarão disponíveis. Para obter mais informações, consulte a documentação de atualização.

Para atualizar um grupo de entrega:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Upgrade Delivery Group** na barra de ações. A ação **UChange Functional Level** aparece somente se forem detectados VDAs atualizados.

A tela indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Você pode cancelar a ação de alteração, resolver o problema das máquinas e executar a ação de alteração novamente.

Após a conclusão da alteração, você pode reverter as máquinas para seus estados anteriores. Selecione o grupo de entrega e selecione **Undo Functional Level Change** na barra de ações.

Gerenciar grupos de entrega de Remote PC Access

Se uma máquina em um catálogo de máquinas Remote PC Access não 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 catálogo de máquinas a grupos de entrega tem um valor de prioridade. A prioridade determina o grupo de entrega atribuído à máquina quando ele se registra no sistema ou quando um usuário precisa de uma atribuição de máquina. Quanto menor o valor, maior a prioridade. Se um catálogo de máquinas Remote PC Access tiver várias atribuições de grupo de entrega, o software seleciona a correspondência com a prioridade mais alta. Use o SDK do PowerShell para definir o valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas Remote PC Access são associados a um grupo de entrega. Contas de máquina ou unidades organizacionais adicionadas ao catálogo posteriormente podem ser adicionadas ao grupo de entrega. Esta associação pode ser ativada ou desativada.

Para adicionar ou remover uma associação de catálogo de máquinas Remote PC Access com um grupo de entrega:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo Remote PC Access.
3. Na seção **Details**, clique na guia **Machine Catalogs** e selecione um catálogo Remote PC Access.
4. Para adicionar ou restaurar uma associação, clique em **Add Desktops**. Para remover uma associação, clique em **Remove Association**.

Organizar grupos de entrega usando pastas

Você pode criar pastas para organizar grupos de entrega e facilitar o acesso. Por exemplo, você pode organizá-los por finalidade ou pela estrutura organizacional.

Para criar e gerenciar pastas de grupos de entrega, use a barra de ações ou o menu do botão direito do mouse. Você também pode arrastar um grupo de entrega ou uma pasta para o local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas com até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de entrega e subpastas. Você só pode excluir uma pasta se ela e suas subpastas não contiverem grupos de entrega.
- Todos os recursos (como catálogos de máquinas, grupos de entrega, aplicativos e grupos de aplicativos) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outras pastas de recursos ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nas diferentes árvores de pastas.

Gerenciar proteção de aplicativo

As informações a seguir complementam a proteção do aplicativo. Veja os seguintes detalhes:

- Você deve ter um direito de proteção de aplicativos válido. Para comprar o recurso de proteção de aplicativos, entre em contato com o seu representante de vendas da Citrix.
- A proteção de aplicativos exige confiança em XML. Para ativar a confiança em XML, vá para **Settings > Enable XML trust**.
- Em relação à proteção contra captura de tela:
  - No Windows e no macOS, somente a janela do conteúdo protegido fica em branco. A proteção de aplicativo fica ativa quando uma janela protegida não é minimizada.
  - No Linux, toda a captura fica em branco. A proteção de aplicativo fica ativa independentemente de uma janela protegida ser minimizada ou não.

Para escolher um método de proteção de aplicativos para um grupo de entrega, siga estas etapas:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **App Protection**, você pode ativar **Anti-keylogging** e **Anti-screen-capturing**.

Usuários

- Alterar configurações do usuário
- Adicionar ou remover usuários

Alterar as configurações do usuário em um grupo de entrega

O nome dessa página aparece como **User Settings** ou **Basic Settings**.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **User Settings** (ou **Basic Settings**), altere qualquer uma das configurações na tabela a seguir.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Definição	Descrição
Descrição	O texto que o Citrix Workspace (ou StoreFront) usa e que os usuários veem.
Enable delivery group	Se o grupo de entrega está ativado ou não.

Definição	Descrição
Time zone	O fuso horário no qual as máquinas desse grupo de entrega devem residir. A opção lista os fusos horários suportados pelo site.
Enable Secure ICA	Protege comunicações de e para máquinas no grupo de entrega usando SecureICA, que criptografa o protocolo ICA. O nível padrão é 128 bits. O nível pode ser alterado usando o SDK. A Citrix recomenda o uso de mais métodos de criptografia, como a criptografia TLS, ao atravessar redes públicas. Além disso, SecureICA não verifica a integridade dos dados.

Adicionar ou remover usuários em um grupo de entrega

Para obter informações detalhadas sobre usuários, consulte Usuários.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Users**:
   - Para adicionar usuários, clique em **Add** e, em seguida, especifique os usuários que deseja adicionar.
   - Para remover usuários, selecione um ou mais usuários e clique em **Remove**.
   - Marque ou desmarque a caixa de seleção para permitir o acesso por usuários não autenticados.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Importar ou exportar listas de usuários Para grupos de entrega contendo máquinas físicas de SO de sessão única, você pode importar informações do usuário de um arquivo .csv depois de criar o grupo de entrega. Você também pode exportar informações do usuário para um arquivo .csv. O arquivo .csv pode conter dados de uma versão anterior do produto.

A primeira linha no arquivo CSV deve conter dois cabeçalhos de coluna, separados por uma vírgula. Certifique-se de que o primeiro cabeçalho seja `Machine Account` e o segundo cabeçalho seja `User Names`. (Você pode incluir cabeçalhos adicionais, mas eles não são suportados.) As linhas

subsequentes no arquivo contêm dados separados por vírgulas. As entradas `Machine Account` podem ser o SID do computador, o FQDN ou pares de domínio e nome de computador.

Para importar ou exportar informações de usuário:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Machine Allocation**, selecione a lista **Import** ou **Export** e navegue até o local do arquivo.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

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 marca para uma área de trabalho
- Remover uma máquina
- Restringir o acesso a máquinas
- Impedir que usuários se conectem a uma máquina (modo de manutenção)
- Desligar e reiniciar máquinas
- Criar e gerenciar agendamentos de reinicialização de máquinas
- Carregar máquinas gerenciadas
- Máquinas com gerenciamento de energia

Alterar atribuições de máquinas para usuários em um grupo de entrega

Você pode alterar as atribuições de máquinas de SO de sessão única provisionadas com MCS. Não é possível alterar atribuições de máquinas com SO multissessão ou máquinas provisionadas com o Citrix Provisioning.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Desktops** ou **Desktop Assignment Rules** (o título da página depende do tipo de catálogo de máquinas que o grupo de entrega usa), especifique os novos usuários.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Alterar o número máximo de máquinas por usuário em um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Desktop Assignment Rules**, defina o valor máximo de áreas de trabalho por usuário.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Atualizar uma máquina em um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **View Machines** na barra de ações.
3. Selecione uma máquina e clique em **Update Machines** na barra de ações.

Para escolher uma imagem diferente, selecione **Master Image** e, em seguida, selecione um instantâneo.

Para aplicar alterações e notificar os usuários da máquina, selecione **Rollout notification to end-users**. Em seguida, especifique:

- Quando atualizar a imagem mestre: agora ou na próxima reinicialização
- A hora de distribuição de reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados sobre a reinicialização ou não
- A mensagem que os usuários recebem

Adicionar, alterar ou remover uma restrição de marca para uma área de trabalho

Adicionar, alterar e remover restrições de marca pode ter efeitos imprevisíveis sobre quais áreas de trabalho são consideradas para a inicialização. Consulte as considerações e precauções em Marcas.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Desktops**, selecione a área de trabalho e clique em **Edit**.
4. Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca.
5. Para alterar ou remover uma restrição de marca siga, escolha uma ação:
    - Selecione uma marca diferente.
    - Remova a restrição de marca desmarcando **Restrict launches to machines with this tag**.

6. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Remover uma máquina de um grupo de entrega

A remoção de uma máquina a exclui de um grupo de entrega. Ela não a exclui do catálogo de máquinas usado pelo grupo de entrega. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes que possam ser removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto ela está sendo removida, coloque a máquina no modo de manutenção antes de desligá-la.

As máquinas podem conter dados pessoais, portanto, seja cauteloso antes de alocar a máquina para outro usuário. Considere refazer a imagem da máquina.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **View Machines** na barra de ações.
3. Assegure-se de que a máquina está desligada.
4. Selecione a máquina e clique em **Remove from Delivery Group** na barra de ações.

Você também pode remover uma máquina de um grupo de entrega através da conexão que a máquina usa.

Restringir o acesso a máquinas em um grupo de entrega

Quaisquer alterações que você fizer para restringir o acesso a máquinas em um grupo de entrega substituem as configurações anteriores, independentemente do método usado. Você pode:

- **Restringir o acesso de administradores que usam escopos de administração delegada:** crie e atribua um escopo que permita que os administradores acessem todos os aplicativos e outro escopo que forneça acesso a apenas determinados aplicativos. Para obter detalhes, consulte Administração delegada.
- **Restringir o acesso de usuários por meio de expressões de política SmartAccess:** use expressões de política para filtrar conexões de usuário realizadas por meio do Citrix Gateway.

  1. Selecione **Delivery Groups** no painel esquerdo.
  2. Selecione um grupo e clique em **Edit** na barra de ações.
  3. Na página da **política de acesso**, selecione **Connections through NetScaler Gateway**.
  4. Para escolher um subconjunto dessas conexões, selecione **Connections meeting any of the following filters**. Em seguida, defina o site Citrix Gateway e adicione, edite ou remova as expressões de política do SmartAccess para os cenários permitidos de acesso do usuário. Para obter detalhes, consulte a documentação do Citrix Gateway.

5. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

- **Restringir o acesso de usuários por meio de filtros de exclusão:** use filtros de exclusão nas políticas de acesso que você definiu no SDK. As políticas de acesso são aplicadas a grupos de entrega para refinar as conexões. Por exemplo, você pode restringir o acesso da máquina a um subconjunto de usuários e especificar dispositivos de usuário permitidos. Os filtros de exclusão refinam ainda mais as políticas de acesso. Por exemplo, por segurança, você pode negar o acesso a um subconjunto de usuários ou dispositivos. Por padrão, os filtros de exclusão são desativados.

  Por exemplo, um laboratório de ensino na sub-rede de uma rede corporativa que impede o acesso do laboratório a um grupo de entrega específico. Independentemente de quem está usando as máquinas no laboratório, use o comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

  Use o asterisco (*) como curinga para corresponder a todas as marcas que começam com a mesma expressão de política. Por exemplo, se você adicionar a marca `VPDesktops_Direct` a uma máquina e `VPDesktops_Test` a outra, definir a marca no script `Set-BrokerAccessPolicy` como `VPDesktops_*` aplica o filtro às duas máquinas.

  Se você estiver conectado usando um navegador da Web ou com o recurso de experiência do usuário do aplicativo Citrix Workspace ativado na loja, não será possível usar um filtro de exclusão de nome cliente.

Impedir que os usuários se conectem a uma máquina (modo de manutenção) em um grupo de entrega

Quando precisar interromper temporariamente novas conexões às máquinas, você pode ativar o modo de manutenção de uma ou de todas as máquinas em um grupo de entrega. Você pode fazer isso antes de aplicar patches ou usar ferramentas de gerenciamento.

- Quando uma máquina com SO multissessão está no modo de manutenção, os usuários podem se conectar a sessões existentes, mas não podem iniciar novas sessões.
- Quando uma máquina de SO de sessão única (ou um computador usando Remote PC Access) está no modo de manutenção, os usuários não podem se conectar ou reconectar. As conexões atuais permanecem ativas até que se desconectem ou seja feito logoff.

Para ativar ou desativar o modo de manutenção:

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo.

3. Para ativar o modo de manutenção para todas as máquinas do grupo de entrega, clique em **Turn On Maintenance Mode** na barra de ações.

   Para ativar o modo de manutenção para uma máquina, clique em **View Machines** na barra de ações. Selecione uma máquina e clique em **Turn On Maintenance Mode** na barra de ações.

4. Para desativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega, siga as instruções anteriores, mas clique em **Turn Off Maintenance Mode** na barra de ações.

As configurações da Conexão de Área de Trabalho Remota (RDC) do Windows também afetam se uma máquina com SO multissessão está ou não no modo de manutenção. O modo de manutenção é ativado quando ocorre uma das seguintes circunstâncias:

- O modo de manutenção é definido como ativado, conforme descrito anteriormente.
- A RDC está definida como **Não permitir conexões com este computador**.
- A RDC não está definida como **Não permitir conexões com este computador**. A configuração do **modo de logon do usuário da configuração do host remota** é **Permitir reconexões, mas impedir novos logons** ou **Permitir reconexões, mas impedir novos logons até que o servidor seja reiniciado**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, o que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, o que afeta as máquinas nesse catálogo.

Desligar e reiniciar máquinas em um grupo de entrega

Este procedimento não é suportado para máquinas de Remote PC Access.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **View Machines** na barra de ações.
3. Selecione a máquina e clique em uma das seguintes entradas na barra de ações:

   - **Force shut down:** força o desligamento da máquina e atualiza a lista de máquinas.
   - **Restart:** solicita que o sistema operacional seja desligado e, em seguida, inicializa a máquina novamente. Se o sistema operacional não conseguir, a máquina permanecerá em seu estado atual.
   - **Force restart:** força o desligamento do sistema operacional e, em seguida, reinicializa a máquina.
   - **Suspend:** pausa a máquina sem desligá-la e atualiza a lista de máquinas.
   - **Shut down:** solicita que o sistema operacional seja desligado.

Para ações não forçadas, se a máquina não for desligada em 10 minutos, ela será encerrada. Se o Windows tentar instalar atualizações durante o desligamento, existe o risco de a máquina ser encerrada antes do término das atualizações.

A Citrix recomenda que você evite que usuários de máquinas de SO de sessão única selecionem **Desligar** de dentro de uma sessão. Consulte a documentação da política da Microsoft para obter detalhes.

Você também pode desligar e reinicializar máquinas em uma conexão.

Criar e gerenciar agendamentos de reinicialização de máquinas em um grupo de entrega

O agendamento de reinicialização especifica a periodicidade de reinicialização das máquinas em um grupo de entrega. Você pode criar um ou mais agendamentos para um grupo de entrega. Um agendamento pode afetar:

- Todas as máquinas no grupo.
- Uma ou mais máquinas (mas não todas) no grupo. As máquinas são identificadas por uma marca que você aplica à máquina. Isso é chamado de restrição de marca, porque a marca restringe uma ação a apenas os itens que têm a marca.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você quer que cada máquina seja reinicializada uma vez por semana e que as máquinas usadas pelo pessoal da contabilidade sejam reinicializadas diariamente. Para isso, configure um cronograma para todas as máquinas e outro cronograma apenas para as máquinas da contabilidade.

Um agendamento inclui o dia e a hora em que a reinicialização começa e a duração.

Você pode ativar ou desativar um agendamento. Desabilitar um agendamento pode ser útil durante a realização de testes, durante intervalos especiais ou quando você estiver preparando o cronograma de agendamentos antes de precisar deles.

Não é possível usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reinicializar.

Sobreposição de agendamentos Pode acontecer de os agendamentos se sobreporem. No exemplo acima, os dois agendamentos afetam as máquinas da contabilidade. Essas máquinas podem ser reinicializadas duas vezes aos domingos. O código de agendamento foi projetado para evitar a reinicialização da mesma máquina com mais frequência do que o desejado, mas não é garantido.

- Se os agendamentos coincidirem precisamente na hora de início e na duração, é mais provável que as máquinas sejam reinicializadas apenas uma vez.
- Quanto mais diferentes forem a hora de início e a duração nos agendamentos, maior a probabilidade de que ocorram várias reinicializações.

- O número de máquinas afetadas por um agendamento também afeta a probabilidade de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário das máquinas do departamento de contabilidade, dependendo da duração especificada para cada.

Para uma análise detalhada dos agendamentos de reinicialização, consulte Reboot schedule internals.

Exibir agendamentos de reinicialização

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Selecione a página **Restart Schedule**.

A página **Restart Schedule** contém as seguintes informações sobre cada agendamento configurado:

- Nome do agendamento.
- Restrição de marca usada, se houver.
- Com que frequência as reinicializações da máquina ocorrem.
- Se os usuários da máquina recebem uma notificação.
- Se o agendamento está habilitado.

Adicionar (aplicar) marcas Quando você configura um agendamento de reinicialização que usa uma restrição de marca, verifique se a marca foi adicionada às máquinas afetadas pelo agendamento. No exemplo acima, cada uma das máquinas usadas pelo pessoal de contabilidade tem uma marca aplicada. Para obter detalhes, consulte Marcas.

Embora você possa aplicar mais de uma marca a uma máquina, um agendamento de reinicialização pode especificar apenas uma marca.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione o grupo que contém as máquinas controladas pelo agendamento.
3. Clique em **View Machines** e, em seguida, selecione as máquinas às quais você deseja adicionar uma marca.
4. Clique em **Manage Tags** na barra de ações.
5. Se a marca existir, ative a caixa de seleção ao lado do nome da marca. Se a marca não existir, clique em **Create** e, em seguida, especifique o nome da marca. Depois que a marca é criada, ative a caixa de seleção ao lado do nome da marca recém-criada.
6. Clique em **Save** na caixa de diálogo **Manage Tags**.

Criar um agendamento de reinicialização

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Restart Schedule**, clique em **Add**.
4. Na página **Add Restart Schedule**:
    - Digite um nome e uma descrição do agendamento.
    - Se você estiver usando uma restrição de marca, selecione a marca.
    - Em **Restart frequency**, selecione com que frequência ocorre a reinicialização: diariamente, dias úteis, fim de semana ou um dia específico da semana.
    - Usando o relógio de 24 horas, especifique a hora do dia para iniciar a reinicialização.
    - Em **Restart duration**, escolha se todas as máquinas são reinicializadas ao mesmo tempo ou o período total de tempo para começar a reinicializar todas as máquinas afetadas. Um algoritmo interno determina quando cada máquina é reinicializada durante esse intervalo.

      > **Nota:**
      >
      > Outra opção de duração de reinicialização está disponível usando o PowerShell. Consulte Reinicializar após o esvaziamento.

    - Em **Send notification to users**, escolha se deseja exibir uma mensagem de notificação nas máquinas afetadas antes de iniciar uma reinicialização. Por padrão, nenhuma mensagem é exibida.
    - Se optar por exibir uma mensagem 15 minutos antes do início da reinicialização, você pode escolher (em Notification frequency) para repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não é repetida.
    - Insira o título e o texto da notificação. Não há texto padrão.

      Se quiser que a mensagem inclua o número de minutos antes da reinicialização, inclua a variável **%m%**. Por exemplo: "Aviso: seu computador será reinicializado automaticamente em %m% minutos". O valor diminui em cinco minutos a cada mensagem repetida. A menos que você opte por reinicializar todas as máquinas ao mesmo tempo, a mensagem é exibida em cada máquina no momento apropriado antes da reinicialização, calculada pelo algoritmo interno.
    - Para ativar o agendamento, marque a caixa de seleção. Para desativar o agendamento, desmarque a caixa de seleção.
5. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Reinicializar após o esvaziamento Outro valor de duração da reinicialização está disponível usando o PowerShell para criar ou atualizar um cronograma de agendamento de reinicialização de máquina (`New-BrokerRebootSchedulev2` ou `Set-BrokerRebootSchedulev2`).

Quando você habilita o recurso de reinicialização após o esvaziamento com o parâmetro `-UseNaturalReboot <Boolean>`, todas as máquinas são reinicializadas depois de esvaziar todas as sessões. Quando o horário de reinicialização é atingido, as máquinas são colocadas no estado de esvaziamento e, em seguida, reinicializadas quando todas as sessões forem desligadas.

Esse recurso é suportado para grupos de entrega que contêm máquinas de sessão única ou multissessão. Você pode usar essa opção para máquinas com gerenciamento de energia e também para máquinas que não são gerenciadas por energia.

Em um ambiente local, esse recurso é suportado somente ao usar o PowerShell. O recurso não está disponível no Web Studio.

Editar, remover, ativar ou desativar um agendamento de reinicialização

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit** na barra de ações.
3. Na página **Restart Schedule**, marque a caixa de seleção de um agendamento.

    - Para editar um agendamento, clique em **Edit**. Atualize a configuração do agendamento, usando as orientações em Criar um agendamento de reinicialização.
    - Para ativar ou desativar um agendamento, clique em **Edit**. Marque ou desmarque a caixa de seleção **Enable restart schedule**.
    - Para remover um agendamento, clique em **Remove**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma marca aplicada às máquinas nas máquinas afetadas.

Reinicializações programadas atrasadas devido à interrupção do banco de dados

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

Se ocorrer uma interrupção do banco de dados do site antes da reinicialização agendada começar para as máquinas (VDAs) em um grupo de entrega, as reinicializações iniciam quando a interrupção termina. Isso pode ter resultados inesperados.

Por exemplo, digamos que você agendou as reinicializações de um grupo de entrega para ocorrer durante um horário fora do período de produção (começando às 3h). Uma interrupção do banco de dados do site ocorre uma hora antes do início da reinicialização agendada (2h). A interrupção dura seis horas (até as 8h). O cronograma de reinicialização começa quando a conexão entre o Delivery Controller e o banco de dados do site é restaurada. Agora, a reinicialização do VDA começa cinco

horas após sua programação original, resultando na reinicialização dos VDAs durante as horas de produção.

Para ajudar a evitar esta situação, você pode usar o parâmetro `MaxOvertimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além da hora de início programada que um agendamento de reinicialização pode começar.

- Se a conexão do banco de dados for restaurada dentro desse tempo (horário agendado + `MaxOvertimeStartMins`), a reinicialização do VDA começa.
- Se a conexão do banco de dados não for restaurada dentro desse período de tempo, as reinicializações de VDA não começam.
- Se esse parâmetro for omitido ou tiver valor zero, a reinicialização agendada começará quando a conexão com o banco de dados for restaurada, independentemente da duração da interrupção.

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell. Você não pode definir esse valor quando configura um agendamento de reinicialização no Web Studio.

Reinicializações agendadas para máquinas no modo de manutenção

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell. A opção `IgnoreMaintenanceMode` é compatível com o Citrix Virtual Apps and Desktops 7 2006 e posterior.

Para indicar se um agendamento de reinicialização afeta máquinas que estão no modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria um agendamento que reinicializa máquinas que estão no modo de manutenção (além de máquinas que não estão no modo de manutenção).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

O cmdlet a seguir modifica um agendamento de reinicialização existente.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell.

Carregar máquinas gerenciadas em grupos de entrega

Você pode gerenciar a carga somente de máquinas com SO multissessão.

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as atuais condições do ambiente. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor:** uma máquina com SO multissessão é considerada para balanceamento de carga somente quando o modo de manutenção está desativado.
- **Índice de carga do servidor:** determina a probabilidade de um servidor que fornece máquinas com SO multissessão receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações de métricas de desempenho, como CPU, disco e uso de memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga.

  Um índice de carga de servidor de 10000 indica que o servidor está totalmente carregado. Se nenhum outro servidor estiver disponível, os usuários poderão receber uma mensagem informando que a área de trabalho ou o aplicativo não está disponível quando iniciarem uma sessão.

  Você pode monitorar o índice de carga na pesquisa no Director (Monitor), Web Studio (Manage) e no SDK.

  Nas exibições do console, para exibir a coluna **Server Load Index** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse em um cabeçalho de coluna e selecione **Select Column**. Em **Machine category**, selecione **Load Index**.

  No SDK, use o cmdlet `Get-BrokerMachine`. Para obter detalhes, consulte CTX202150.

- **Concurrent logon tolerance policy setting**: o número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões XenApp 6.x.)

  Quando todos os servidores superam ou se encontram no limite da configuração de tolerância de logon simultâneo, a próxima solicitação de logon é atribuída ao servidor com o menor número de logons pendentes. Se mais de um servidor atender a esses critérios, o servidor com o menor índice de carga é selecionado.

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 máquinas físicas (incluindo máquinas Remote PC Access). Máquinas com SO de sessão única com recursos de GPU não podem ser suspensas, portanto, as operações de desligamento falham. Para máquinas com SO multissessão, você pode criar um agendamento de reinicialização.

Em grupos de entrega contendo máquinas em pool, as máquinas virtuais com SO de sessão única podem estar em um dos seguintes estados:

- Aleatoriamente alocadas e em uso
- Não alocadas e não conectadas

Em grupos de entrega contendo máquinas estáticas, as máquinas virtuais com SO de sessão única podem estar:

- Permanentemente alocadas e em uso
- Permanentemente alocadas e desconectadas (mas prontas)
- Não alocadas e não conectadas

Durante o uso normal, os grupos de entrega estáticos normalmente contêm máquinas alocadas permanentemente e não alocadas. Inicialmente, todas as máquinas estão no estado não alocadas, exceto as alocadas manualmente quando o grupo de entrega foi criado. Conforme os usuários se conectam, as máquinas ficam alocadas permanentemente Você pode gerenciar totalmente a energia das máquinas não alocadas nesses grupos de entrega, mas gerenciar apenas parcialmente as máquinas alocadas permanentemente.

- **Polls e buffers:** para grupos de entrega em pool e grupos de entrega estáticos com máquinas não alocadas, um pool (nesta instância) é um conjunto de máquinas não alocadas ou temporariamente alocadas que são mantidas em um estado ativo, pronto para que os usuários se conectem. O usuário recebe uma máquina imediatamente após o login. O tamanho do pool (o número de máquinas mantidas ativas) é configurável pela 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 que se mantêm no modo de espera e que são ativadas quando o número de máquinas no pool cai abaixo de um limite. O limite é uma porcentagem do tamanho do grupo de entrega. Para grandes grupos de entrega, um número significativo de máquinas pode ser ativado quando o limite for excedido. Portanto, planeje cuidadosamente o tamanho dos grupos de entrega ou use o SDK para ajustar o tamanho padrão do buffer.

- **Timers de estado de energia:** você pode usar timers de estado de energia para suspender máquinas depois que os usuários tiverem se desconectado por um período de tempo especificado. Por exemplo, as máquinas são suspensas automaticamente fora do horário de expediente se os usuários ficarem desconectados por pelo menos 10 minutos.

  Você pode configurar timers 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 timers de estado de energia, mas não pools ou buffers. As máquinas são ativadas no início de cada período de pico e desativadas

no início de cada período fora de pico. Você não tem o mesmo controle preciso que tem de máquinas não alocadas sobre o número de máquinas que ficam disponíveis para compensar as máquinas que são consumidas.

Gerenciar a energia de máquinas virtuais de SO de sessão única

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit Delivery Group** na barra de ações.
3. Na página **Power Management**, selecione **Weekdays** em **Power manage machines**. Por padrão, os dias da semana são de segunda a sexta-feira.
4. Para grupos de entrega aleatórios, em **Machines to be powered on**, clique em **Edit** e especifique o tamanho do pool durante os dias úteis. Em seguida, selecione o número de máquinas para ativar.
5. Em **Peak hours**, defina as horas de pico e fora de pico para cada dia.
6. Defina os timers de estado de energia para horas de pico e não pico durante os dias da semana: em **During peak hours > When disconnected**, especifique o atraso (em minutos) antes de suspender uma máquina desconectada no grupo de entrega e selecione **Suspend**. Em **During off-peak hours > When disconnected**, especifique o atraso antes de desligar máquinas desconectadas no grupo de entrega e selecione **Shutdown**. Este timer não está disponível para grupos de entrega com máquinas aleatórias.
7. Selecione **Weekend** em **Power manage machines** e configure as horas de pico e os timers de estado de energia para fins de semana.
8. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta. Ou clique em **Save** para aplicar as alterações e fechar a janela.

Use o SDK para:

- Desligar máquinas, em vez de suspendê-las, em resposta a timers de estado de energia; ou se preferir que os timers sejam baseados em logoffs, em vez de desconexões.
- Alterar as definições padrão do dia da semana e fim de semana.
- Desativar o gerenciamento de energia. Veja CTX217289.

Gerenciar a energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas

> **Importante:**
>
> Esta melhoria aplica-se somente às máquinas VDI com sessões desconectadas. Não se aplica às máquinas VDI com sessões em logoff.

Em versões anteriores, uma máquina VDI fazendo a transição para um período em que era necessária uma ação (ação de desconexão=”**Suspend**”ou “**Shutdown**”) tinha que permanecer ligada. Esse

cenário ocorria se a máquina se desconectasse durante um período de tempo (horários de pico ou fora de pico) em que não era necessária nenhuma ação (ação de desconexão="**Nothing**").

A partir do Citrix Virtual Apps and Desktops 7 1909, a máquina é suspensa ou desligada quando o tempo de desconexão especificado é decorrido, dependendo da ação de desconexão configurada para o período de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega VDI:

- Definir `PeakDisconnectAction` como "Nothing"
- Definir `OffPeakDisconnectAction` como "Shutdown"
- Definir `OffPeakDisconnectTimeout` como "10"

Para obter mais informações sobre a ação de desconexão na política de energia, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy e https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Em versões anteriores, uma máquina VDI com uma sessão desconectada durante os horários de pico permanecia ligada quando fazia a transição de pico para não 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 o horário fora de pico.

Se você quiser reverter para o comportamento anterior (ou seja, não aplicar nenhuma ação em máquinas que fazem a transição de horário de pico para não pico ou de horário de não pico para pico com sessões desconectadas), execute um destes procedimentos:

- Defina o valor do registro `LegacyPeakTransitionDisconnectedBehaviour` como `1`, o equivalente a *true*, o que permite o comportamento anterior. Por padrão, o valor é `0`, ou *false*, o que dispara ações da política de energia de desconexão na transição do período.
  - Caminho: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Nome: `LegacyPeakTransitionDisconnectedBehaviour`
  - Tipo: `REG_DWORD`
  - Dados: `0x00000001 (1)`
- Configure o parâmetro usando o comando `Set-BrokerServiceConfigurationData` do PowerShell. Por exemplo:
  - ```
    PS C:\> Set-BrokerServiceConfigurationData HostingManagement.
    LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true
    ```

Uma máquina deve atender aos seguintes critérios antes que as ações de política de energia possam ser aplicadas a ela na transição do período:


    ```

- Ter uma sessão desconectada.
- Não ter ações pendentes de energia.
- Pertencer a um grupo de entrega VDI (sessão única) que transita para um período de tempo diferente.
- Ter uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e transita para um período em que uma ação de energia é atribuída.

**Alterar a porcentagem de VDAs em um estado de energia para catálogos**

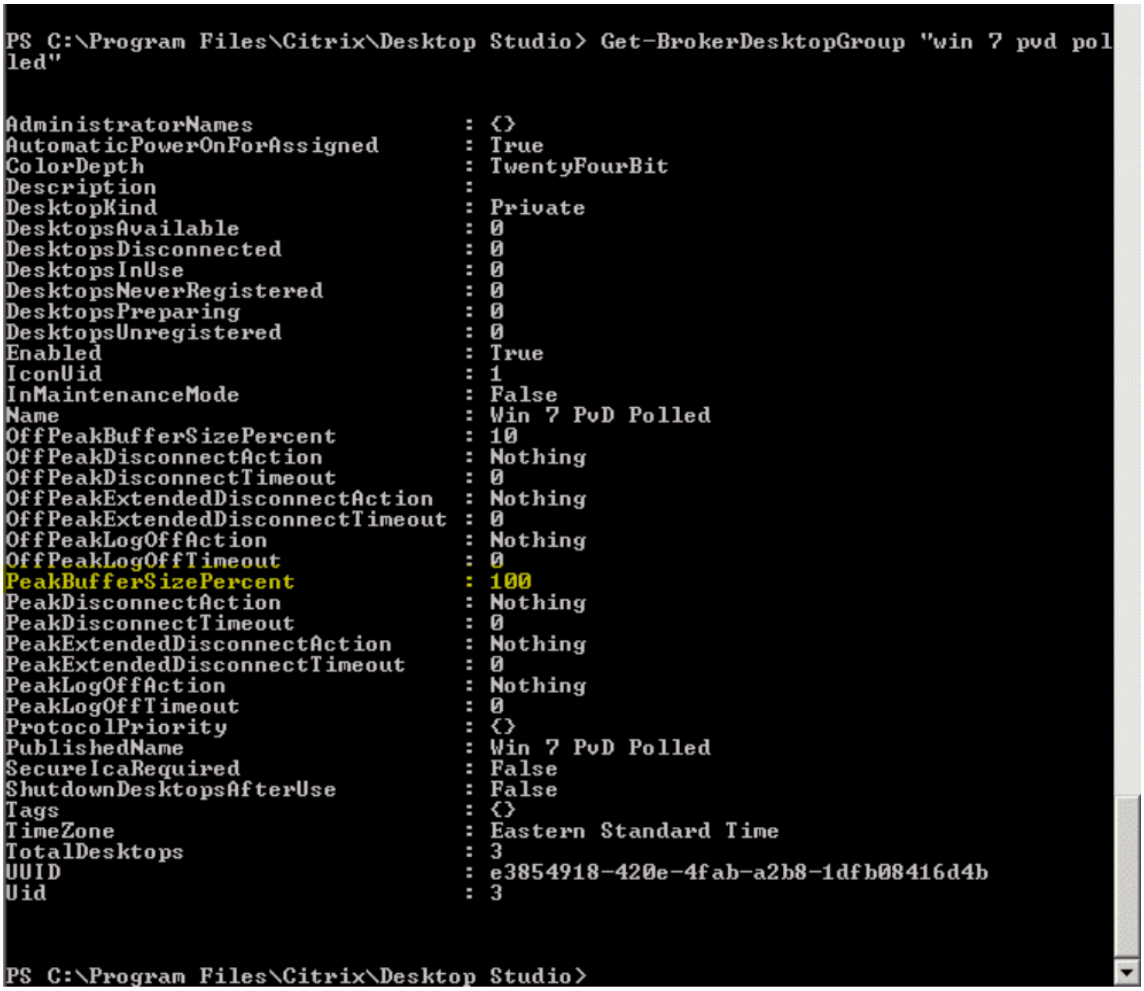
1. Ajuste as horas de pico para o grupo de entrega na seção de **gerenciamento de energia** do grupo de entrega.
2. Anote o nome do grupo de área de trabalho.
3. Com privilégios de administrador, inicie o PowerShell e execute os seguintes comandos. Substitua "Desktop Group Name"pelo nome do seu grupo 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 prontos.
4. Verifique a solução executando:

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```

Pode levar até uma hora para que as mudanças entrem em vigor.

Para desligar os VDAs depois que o usuário faz logoff, digite:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

Para reinicializar os VDAs durante o horário de pico, de modo que estejam prontos para os usuários após fazerem logoff, insira:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

Sessões

- Fazer logoff ou desconectar uma sessão ou enviar uma mensagem aos usuários
- Configurar o pré-lançamento da sessão e o prolongamento da sessão
- Reconexão da sessão de controle quando desconectada da máquina no modo de manutenção
- Configurar roaming de sessão

Fazer logoff ou desconectar uma sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e selecione **View Machines** na barra de ações.
3. No painel central, selecione a máquina, selecione **View Sessions** na barra de ações e, em seguida, selecione uma sessão.
    - Alternativamente, no painel central, selecione a guia **Session** e, em seguida, selecione uma sessão.
4. Para fazer logoff de uma sessão, selecione **Log off** na barra de ações. A sessão fecha e o usuário é desconectado. A máquina fica disponível para outros usuários, a menos que esteja alocada para um usuário específico.
5. Para desconectar uma sessão, selecione **Disconnect** na barra de ações. Os aplicativos continuam sendo executados na sessão e a máquina permanece alocada para o usuário. O usuário pode se reconectar à mesma máquina.

Você pode configurar timers de estado de energia para máquinas de SO de sessão única para lidar automaticamente com sessões não utilizadas. Para obter detalhes, consulte Máquinas com gerenciamento de energia.

Enviar uma mensagem para um grupo de entrega

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega e selecione **View Machines** na barra de ações.
3. No painel central, selecione uma máquina para a qual deseja enviar uma mensagem.
4. Na barra de ações, selecione **View Sessions**.
5. No painel central, selecione todas as sessões e, em seguida, selecione **Send Message** na barra de ações.
6. Digite sua mensagem e clique em **OK**. Você pode especificar o nível de severidade, se necessário. As opções incluem **Critical**, **Question**, **Warning** e **Information**.

Como alternativa, você pode enviar uma mensagem usando o Citrix Director. Para obter mais informações, consulte Enviar mensagens para usuários.

Configurar a pré-inicialização de sessão e o prolongamento de sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas com SO multissessão.

Os recursos de pré-inicialização de sessão e de prolongamento de sessão ajudam os usuários especificados a acessar aplicativos rapidamente, iniciando as sessões antes de serem solicitadas (pré-inicialização de sessão) e mantendo as sessões de aplicativos ativas depois que o usuário feche todos os aplicativos (prolongamento de sessão).

Por padrão, a pré-inicialização de sessão e o prolongamento de sessão não são usados. Uma sessão é inicializada quando o usuário inicia um aplicativo e permanece ativa até que o último aplicativo aberto na sessão seja fechado.

Considerações:

- O grupo de entrega deve oferecer suporte a aplicativos e as máquinas devem estar executando um VDA de SO multissessão, versão mínima 7.6.
- Esses recursos são compatíveis apenas ao usar o aplicativo Citrix Workspace para Windows e também exigem configuração extra do aplicativo Citrix Workspace. Para obter instruções, procure por pré-inicialização de sessão na documentação do produto para a sua versão do aplicativo Citrix Workspace para Windows.
- O aplicativo Citrix Workspace para HTML5 não é suportado.
- Ao usar a pré-inicialização de sessão, se a máquina de um usuário for colocada no modo suspender ou hibernar, a pré-inicialização não funciona (independentemente das configurações de pré-inicialização da sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário fizer logoff do aplicativo Citrix Workspace, a sessão será encerrada e a pré-inicialização não se aplica mais.
- Ao usar a pré-inicialização de sessão, as máquinas cliente físicas não podem usar as funções de gerenciamento de energia suspender ou hibernar. Usuários de máquinas cliente podem bloquear suas sessões, mas não devem fazer logoff.
- Sessões pré-inicializadas e prolongadas consomem uma licença simultânea, mas somente quando conectadas. Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. As sessões pré-inicializadas e prolongadas não utilizadas se desconectam após 15 minutos por padrão. Esse valor pode ser configurado no PowerShell (cmdlet `New`/`Set-BrokerSessionPreLaunch`).
- O planejamento e monitoramento minuciosos dos padrões de atividade de seus usuários são essenciais para adaptar esses recursos para complementarem uns aos outros. A configuração ideal equilibra os benefícios da disponibilidade mais rápida de aplicativos para os usuários em relação ao custo de manter as licenças em uso e os recursos alocados.
- Você também pode configurar a pré-inicialização da sessão para um horário agendado do dia no aplicativo Citrix Workspace.

Quanto tempo as sessões pré-inicializadas e prolongadas não utilizadas permanecem ativas
Existem várias maneiras de especificar quanto tempo uma sessão não utilizada permanece ativa se o usuário não iniciar um aplicativo: um tempo limite configurado e limites de carga do servidor. Você pode configurar todos eles. O evento que ocorre primeiro faz com que a sessão não utilizada termine.

- **Tempo limite:** um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-inicializada ou prolongada não utilizada permanece ativa. Se você configurar

um tempo limite muito curto, as sessões pré-inicializadas terminarão antes que ofereçam ao usuário o benefício do acesso rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário recebidas poderão ser negadas porque o servidor não tem recursos suficientes.

Você pode ativar o tempo limite somente a partir do SDK (cmdlet `New`/`Set-BrokerSessionPreLaunch`), não do console de gerenciamento. Se você desativar o tempo limite, ele não aparecerá na exibição do console do grupo de entrega ou nas páginas **Edit Delivery Group**.

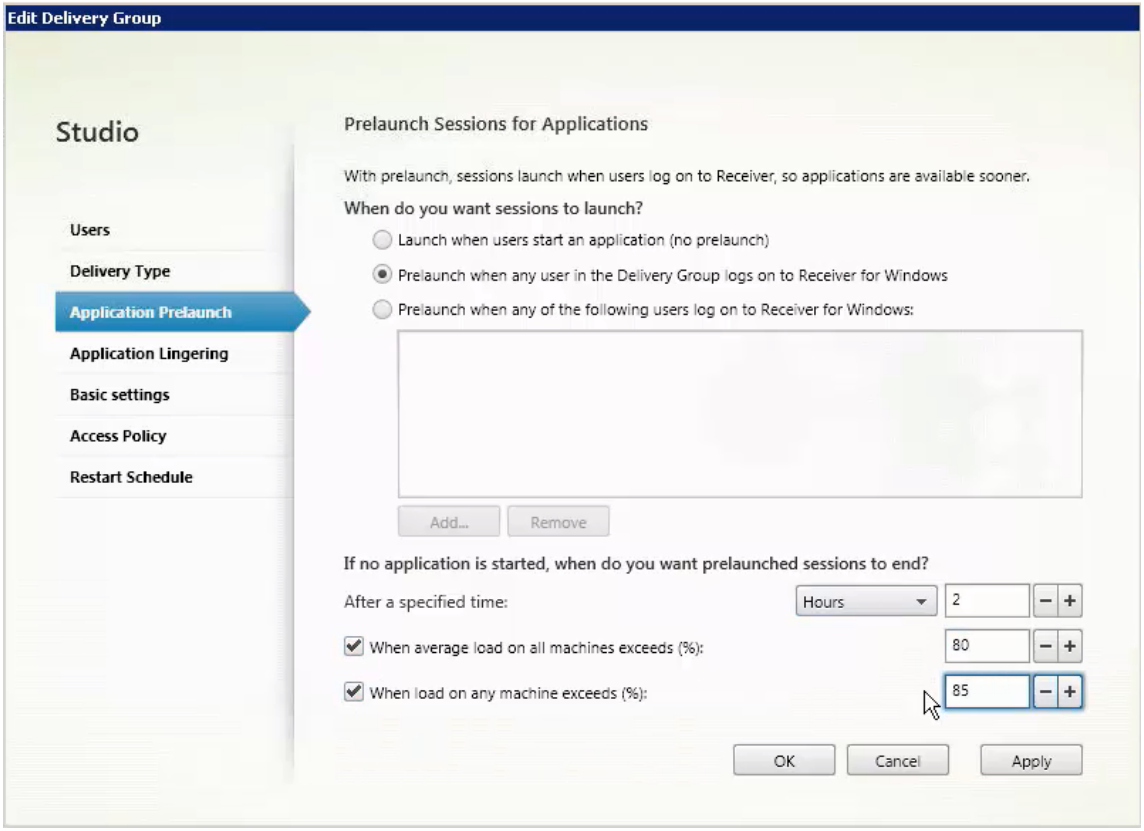
- **Limites:** o encerramento automático de sessões pré-inicializadas e prolongadas com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, pressupondo-se que os recursos do servidor estejam disponíveis. Sessões pré-inicializadas e prolongadas não utilizadas não causam conexões negadas porque elas são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

  Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-inicialização ou prolongada por mais tempo são encerradas. As sessões são encerradas uma por uma em intervalos de minutos até que a carga caia abaixo do limite. Enquanto o limite for excedido, nenhuma nova sessão de pré-inicialização será iniciada.

Os servidores com VDAs que não se registraram no Controller e os servidores no modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-inicialização e prolongadas terminem automaticamente para liberar capacidade.

Para ativar a pré-inicialização da sessão

1. Selecione um grupo e clique em **Edit Delivery Group** na barra de ações.
2. Na página **Application Prelaunch**, ative a pré-inicialização da sessão escolhendo quando as sessões são iniciadas:
   - Quando um usuário inicia um aplicativo. Essa é a configuração padrão. A pré-inicialização da sessão está desativada.
   - Quando um usuário no grupo de entrega faz logon no aplicativo Citrix Workspace para Windows.
   - Quando uma pessoa em uma lista de usuários e grupos de usuários faz logon no aplicativo Citrix Workspace para Windows. Certifique-se de especificar também usuários ou grupos de usuários se escolher essa opção.



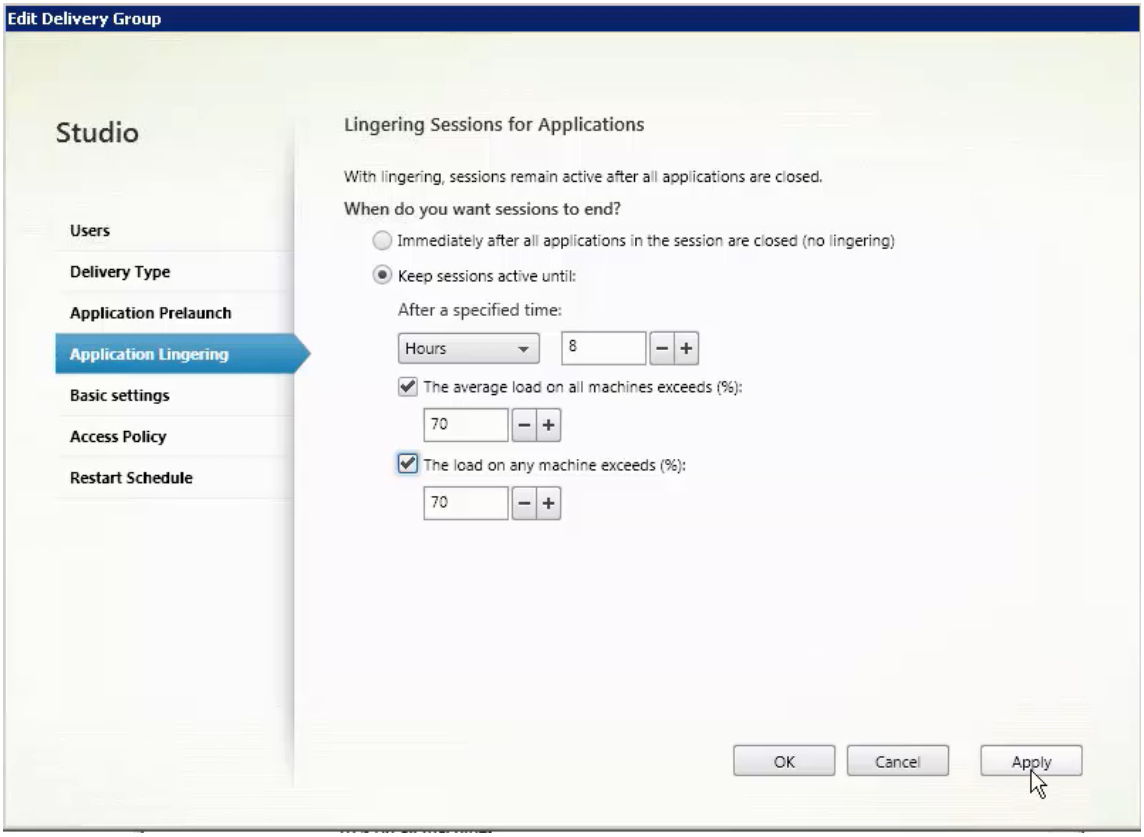
3. Uma sessão pré-inicializada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-inicializada não for utilizada), as configurações a seguir afetarão quanto tempo a sessão permanece ativa.

    - Quando um intervalo de tempo especificado se esgotar. Você pode alterar o intervalo de tempo (1—99 dias, 1—2376 horas ou 1—142.560 minutos).
    - Quando a carga média em todas as máquinas no grupo de entrega exceder uma porcentagem especificada (1—99%).
    - Quando a carga em qualquer máquina no grupo de entrega exceder uma porcentagem especificada (1—99%).

    Recapitulando, uma sessão pré-inicializada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado se esgota ou um limite de carga especificado é excedido.

Para ativar o prolongamento de sessão

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e clique em **Edit Delivery Group** na barra de ações.
3. Na página **Application Lingering**, ative a o prolongamento da sessão selecionando **Keep sessions active until**.



4. Várias configurações afetam quanto tempo uma sessão prolongada permanece ativa se o usuário não iniciar outro aplicativo.

    - Quando um intervalo de tempo especificado se esgotar. Você pode alterar o intervalo de tempo: 1—99 dias, 1—2376 horas ou 1—142.560 minutos.
    - Quando a carga média em todas as máquinas no grupo de entrega exceder uma porcentagem especificada: 1—99%.
    - Quando a carga em qualquer máquina no grupo de entrega exceder uma porcentagem especificada: 1—99%.

    Recapitulando, uma sessão prolongada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado se esgota ou um limite de carga especificado é excedido.

Reconexão da sessão de controle quando desconectada da máquina no modo de manutenção

> **NOTA:**
>
> Este recurso está disponível apenas no PowerShell.

Você pode controlar se as sessões desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes da versão 2106, a reconexão não era permitida para sessões de desktop em pool de sessão única que tinham desconectado das máquinas no modo de manutenção. A partir da versão 2106, você pode configurar um grupo de entrega para permitir ou proibir reconexões (independentemente do tipo VDA) após a desconexão de uma máquina no modo de manutenção.

Ao criar ou editar um grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use o `-AllowReconnectInMaintenanceMode <boolean>` parâmetro para permitir ou proibir reconexões para máquinas que foram desconectadas de uma máquina no modo de manutenção.

- Quando definido como true, as sessões podem se reconectar a máquinas no grupo.
- Quando definido como false, as sessões não podem se reconectar a máquinas no grupo.

Valores padrão:

- Sessão única: Desativado
- Multissessão: Ativado

Configurar roaming de sessão

Por padrão, o roaming de sessão está habilitado para grupos de entrega. As sessões se movem entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos ficam disponíveis nos dois dispositivos simultaneamente. Você pode exibir os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo, ou se existem ou não sessões atuais. Muitas vezes, as impressoras e outros recursos atribuídos ao aplicativo também seguem. Como alternativa, você pode usar o PowerShell. Para obter mais informações, consulte Roaming de sessão.

Configurar roaming de sessão para aplicativos Para configurar o roaming de sessão para aplicativos, siga estas etapas:

1. No console, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit Delivery Group** na barra de ações.
3. Na página **Users**, ative o roaming de sessão marcando a caixa de seleção **Sessions roam with users as they move between devices**.
    - Quando ativada, se um usuário iniciar uma sessão de aplicativo e depois se mover para outro dispositivo, a mesma sessão será usada e ficará disponível nos dois dispositivos. Quando desativada, a sessão não fará mais o roaming entre dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

Configurar o roaming de sessão para áreas de trabalho Para configurar o roaming de sessão para uma área de trabalho, siga estas etapas:

1. No console, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Desktops**, selecione a área de trabalho e selecione **Edit**.
4. Ative o roaming de sessão marcando a caixa de seleção **Session roaming**.

- Quando ativada, se o usuário iniciar uma área de trabalho e depois se mover para outro dispositivo, a mesma sessão é usada e os aplicativos ficam disponíveis nos dois dispositivos. Quando desativada, a sessão não fará mais o roaming entre dispositivos.

Selecione **OK** para aplicar as alterações e fechar a janela.

Solução de problemas

- Os VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização dos recursos disponíveis. Há várias razões para que um VDA não possa ser registrado, muitas das quais um administrador pode resolver. A exibição de detalhes fornece informações sobre solução de problemas no assistente de criação de catálogo e depois de adicionar um catálogo a um grupo de entrega.

  Depois de criar um grupo de entrega, o painel de detalhes de um grupo de entrega indica o número de máquinas que podem ser registradas, mas que não estão. Por exemplo, uma ou mais máquinas estão ligadas e não estão no modo de manutenção, mas, no momento, não estão registradas em um Controller. Ao visualizar uma máquina "não registrada, mas que deveria estar", consulte a guia **Troubleshoot** no painel de detalhes para ver as possíveis causas e as ações corretivas recomendadas.

  Para mensagens sobre o nível funcional, consulte Versões e níveis funcionais do VDA.

  Para obter informações sobre a solução de problemas de registro VDA, consulte CTX136668.

- Na exibição de um grupo de entrega, a **versão instalada do VDA** no painel de detalhes pode diferir da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas que apresentam o status **Power State Unknown**, consulte CTX131267 para obter instruções.

Criar grupos de aplicativos

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Crie grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega. Ou aplicativos usados por um subconjunto de usuários dentro de grupos de entrega. Os grupos de aplicativos são opcionais; eles oferecem uma alternativa para adicionar os mesmos aplicativos a vários grupos de entrega. Associe grupos de entrega a mais de um grupo de aplicativos e associe um grupo de aplicativos a mais de um grupo de entrega.

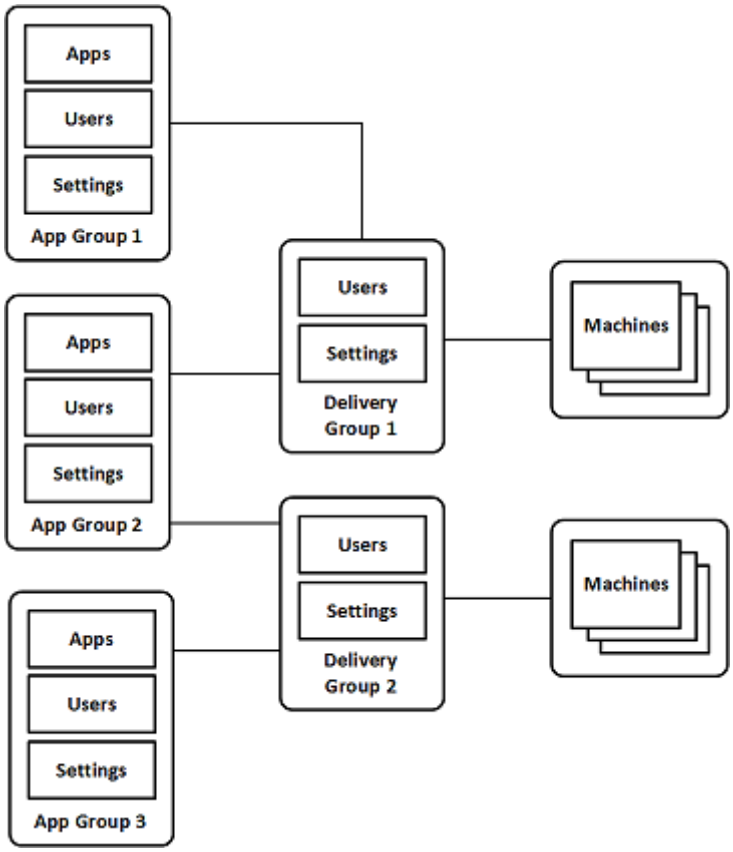
Usar grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em comparação com o uso de mais grupos de entrega:

- O agrupamento lógico de aplicativos e suas configurações permite gerenciar esses aplicativos como uma única unidade. Por exemplo, você não precisa adicionar (publicar) o mesmo aplicativo a grupos de entrega individuais um de cada vez.
- O compartilhamento de sessão entre grupos de aplicativos pode economizar no consumo de recursos. Em outros casos, desativar o compartilhamento de sessões entre grupos de aplicativos pode ser benéfico.
- Você pode usar o recurso de restrição de marca para publicar aplicativos a partir de um grupo de aplicativos, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Com as restrições de marcas, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando nos custos associados com a implantação e gerenciamento de máquinas extras. Uma restrição de marca pode ser considerada como uma subdivisão (ou partição) de máquinas em um grupo de entrega. Usar um grupo de aplicativos ou áreas de trabalho com restrição de marca pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Exemplo de configurações

Exemplo 1:

O gráfico a seguir mostra uma implantação 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 sejam mostradas, as máquinas estão em catálogos de máquinas.)

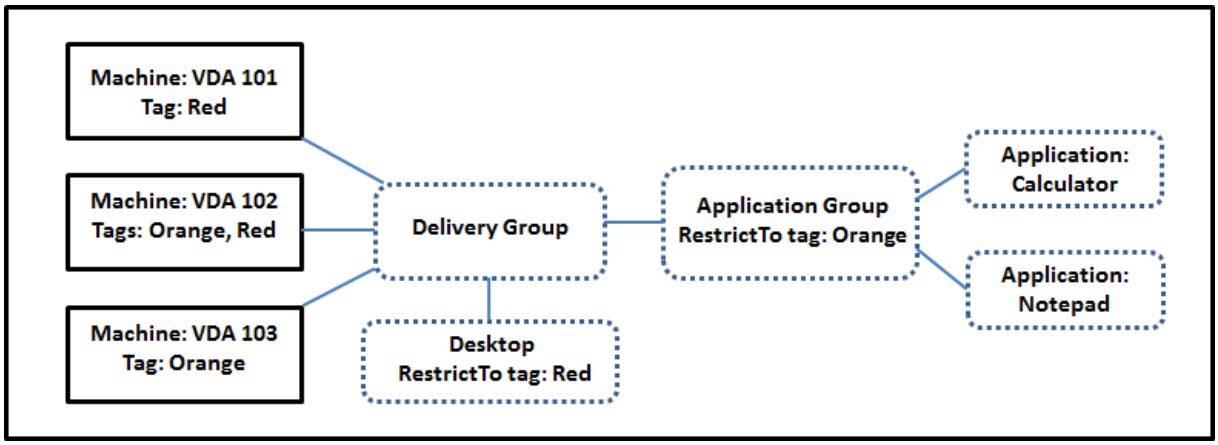
O grupo de aplicativos 1 está associado ao grupo de entrega 1. Acesse os aplicativos no grupo de aplicativos 1 com os usuários especificados no grupo de aplicativos 1. Esses grupos só aparecem enquanto também estão na lista de usuários do grupo de entrega 1. Essa configuração segue a orientação de que a lista de usuários de um grupo de aplicativos é um subconjunto (uma restrição) das listas de usuários dos grupos de entrega associados. As configurações no grupo de aplicativos 1 (como o compartilhamento de sessão de aplicativos entre grupos de aplicativos, grupos de entrega associados) se aplicam a aplicativos e usuários no grupo. As configurações no grupo de entrega 1 se aplicam aos usuários nos grupos de aplicativos 1 e 2, porque esses grupos de aplicativos foram associados ao grupo de entrega.

O grupo de aplicativos 2 está associado a dois grupos de entrega: 1 e 2. Cada um desses grupos de entrega 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 a prioridade igual têm suas cargas balanceadas. Acesse os aplicativos no grupo de aplicativos 2 com os usuários especificados no grupo de aplicativos 2. No entanto, eles também devem aparecer nas listas de usuários do

grupo de entrega 1 e grupo de entrega 2.

Exemplo 2:

Este layout simples usa as restrições de marca para limitar quais máquinas são consideradas para determinadas inicializações de área de trabalho e aplicativo. O site tem um grupo de entrega compartilhado, uma área de trabalho publicada e um grupo de aplicativos configurado com dois aplicativos.



As marcas foram adicionadas a cada uma das três máquinas (VDA 101—103).

O grupo de aplicativos foi criado com a restrição de marca "Orange". Cada um de seus aplicativos é lançado apenas em máquinas no grupo de entrega que têm a marca "Orange", VDA 102 e 103.

Para obter exemplos e orientações mais abrangentes sobre o uso de restrições de marcas em grupos de aplicativos (e áreas de trabalho), consulte Tags.

Orientação e considerações

A Citrix recomenda adicionar aplicativos a grupos de aplicativos ou grupos de entrega, mas não a ambos. Caso contrário, a complexidade adicional de ter aplicativos em dois tipos de grupo pode dificultar o gerenciamento.

Por padrão, um grupo de aplicativos está ativado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Veja Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativos entre grupos de aplicativos está ativado. Veja Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. O processo requer:

1. Atualização dos VDAs nas máquinas usadas no grupo de entrega.
2. Atualização dos catálogos de máquinas que contêm as máquinas.
3. Atualização do grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ter a versão mínima 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna Administrador do Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo refere-se a "associar"um aplicativo com mais de um grupo de aplicativos. Ele diferencia essa ação da adição de instâncias do aplicativo a partir de uma origem disponível. Da mesma forma, os grupos de entrega estão associados a grupos de aplicativos, em vez de serem adições ou componentes um do outro.

Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão do aplicativo está ativado, todos os aplicativos são iniciados na mesma sessão do aplicativo. Isso economiza os custos associados com a inicialização de mais sessões de aplicativos e permite o uso de recursos do aplicativo que envolvem a área de transferência, como operações de copiar e colar. No entanto, em algumas situações, você pode limpar o compartilhamento de sessão.

Quando você usa grupos de aplicativos, você pode configurar o compartilhamento de sessão de aplicativo das três maneiras a seguir, que estendem o comportamento padrão de compartilhamento de sessão disponível quando você está usando apenas grupos de entrega:

- Compartilhamento de sessão ativado entre grupos de aplicativos.
- Compartilhamento de sessão ativado somente entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desativado.

Compartilhamento de sessão entre grupos de aplicativos

Você pode ativar o compartilhamento de sessão de aplicativo entre grupos de aplicativos ou desativá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo da utilidade de ativar o compartilhamento de sessão entre grupos de aplicativos:**

  O grupo de aplicativos 1 contém aplicativos do Microsoft Office, como Word e Excel. O grupo de aplicativos 2 contém outros aplicativos, como Bloco de Notas e Calculadora, e ambos os grupos de aplicativos são anexados ao mesmo grupo de entrega. Um usuário que tem acesso aos dois grupos de aplicativos inicia uma sessão de aplicativo iniciando o Word e, em seguida, inicia o Bloco de Notas. Se o controlador achar 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 marca excluir a máquina em que a sessão está sendo executada —, uma nova sessão em uma máquina adequada será criada, em vez de usar o compartilhamento de sessão.

- **Um exemplo da utilidade de desativar o compartilhamento de sessão entre grupos de aplicativos:**

  Uma configuração com um conjunto de aplicativos que não interoperam bem com outros aplicativos instalados nas mesmas máquinas. Como duas versões diferentes do mesmo pacote de software ou duas versões diferentes do mesmo navegador da Web. Você vai preferir não permitir que um usuário inicie ambas as versões na mesma sessão.

  Crie um grupo de aplicativos para cada versão do pacote de software e adicione os aplicativos para cada versão do pacote de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desativado para cada um desses grupos de aplicativos, um usuário especificado nesses grupos poderá executar aplicativos da mesma versão na mesma sessão. O usuário ainda pode executar outros aplicativos ao mesmo tempo, mas não na mesma sessão. Ao iniciar um dos aplicativos com versão diferente ou qualquer aplicativo que não esteja contido em um grupo de aplicativos, esse aplicativo é iniciado em uma nova sessão.

Esse recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de área restrita de segurança. Não é infalível e tampouco pode impedir que os usuários iniciem aplicativos em suas sessões através de outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver na capacidade máxima, não serão iniciadas novas sessões nela. Novos aplicativos são iniciados em sessões existentes na máquina, conforme necessário, usando o compartilhamento de sessão.

Você só pode disponibilizar sessões pré-iniciadas para grupos de aplicativos que têm o compartilhamento de sessão de aplicativos permitido. (As sessões que usam o recurso de prolongamento de sessão estão disponíveis para todos os grupos de aplicativos.) Esses recursos devem ser ativados e configurados em cada um dos grupos de entrega associados ao grupo de aplicativos. Não é possível configurá-los nos grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativos entre grupos de aplicativos é ativado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Veja Gerenciar grupos de aplicativos.

Desativar o compartilhamento de sessão em um grupo de aplicativos

Você pode impedir o compartilhamento de sessão do aplicativo entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo da utilidade de desativar o compartilhamento de sessão em grupos de aplicativos:**

  Você deseja que seus usuários acessem várias sessões simultâneas de um aplicativo em tela cheia em monitores separados.

  Você cria um grupo de aplicativos e adiciona os aplicativos a ele.

Por padrão, o compartilhamento de sessão de aplicativos é ativado quando você cria um grupo de aplicativos. Não é possível alterar essa configuração ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Veja Gerenciar grupos de aplicativos.

Criar um grupo de aplicativos

Para criar um grupo de aplicativos:

1. Faça login no Web Studio.
2. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
3. Selecione **Create Application Group** na barra de ações.
4. O assistente é iniciado em uma página de **introdução**, que você pode remover das futuras inicializações do assistente.
5. O assistente o orienta pelas páginas descritas na seção a seguir. Quando terminar cada página, clique em **Next** até chegar à página Summary.

Etapa 1. Grupos de entrega

A página **Delivery Groups** lista todos os grupos de entrega, com o número de máquinas que cada grupo contém.

- A lista **Compatible Delivery Groups** contém grupos de entrega que você pode selecionar. Grupos de entrega compatíveis contêm máquinas de SO multissessão ou de sessão única aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Incompatible Delivery Groups** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como, por exemplo, por conter máquinas atribuídas estaticamente.

Um grupo de aplicativos pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam somente áreas de trabalho, se as duas condições a seguir forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.
- Você tem a permissão Edit Delivery Group

O tipo de grupo de entrega é automaticamente convertido em "áreas de trabalho e aplicativos" quando o assistente de criação do grupo de aplicativos é confirmado.

Embora você possa criar um grupo de aplicativos que não tenha grupos de entrega associados (talvez para organizar aplicativos ou para servir como armazenamento para aplicativos não utilizados no momento), o grupo de aplicativos não pode ser usado para entregar aplicativos até especificar pelo menos um grupo de entrega. Além disso, você não pode adicionar aplicativos ao grupo de aplicativos a partir da origem do menu **From Start** se não houver grupos de entrega especificados.

Os grupos de entrega que você seleciona especificam as máquinas usadas para entregar aplicativos. Marque as caixas de seleção ao lado dos grupos de entrega que deseja associar com o grupo de aplicativos.

Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca na lista suspensa.

Etapa 2. Usuários

Especifique os usuários do aplicativo no grupo de aplicativos. Dê permissão a todos os usuários e grupos de usuários nos grupos de entrega selecionados 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, o grupo de aplicativos, poderão acessar os aplicativos nesse grupo. Essencialmente, a lista de usuários no grupo de aplicativos fornece um filtro nas listas de usuários nos grupos de entrega.

A ativação ou desativação do uso do aplicativo por usuários não autenticados está disponível somente em grupos de entrega, não em grupos de aplicativos.

Para obter informações sobre onde as listas de usuários são especificadas em uma implantação, consulte Onde as listas de usuários são especificadas.

Etapa 3. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos adicionados são colocados em uma pasta chamada **Applications**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e já existir outro com o mesmo nome na pasta, você será solicitado a renomear o aplicativo que está adicionando. Se você concordar com o nome exclusivo sugerido, o aplicativo será adicionado com esse novo nome. Caso contrário, você deve renomeá-lo para que possa ser adicionado. Para obter detalhes, consulte Gerenciar pastas de aplicativos.
- Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Veja Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Application name (for user)** no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.
- Quando você adiciona um aplicativo a mais de um grupo de aplicativos, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para exibir o aplicativo em todos os grupos. Nesses casos, consulte um administrador com mais permissões ou estenda o seu escopo para incluir todos os grupos aos quais o aplicativo foi adicionado.

Clique no botão **Add** no menu suspenso para exibir as origens do aplicativo.

- **From Start menu:** aplicativos que são detectados em uma máquina nos grupos de entrega selecionados. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Essa origem não pode ser selecionada se você selecionou um dos seguintes:

  - Grupos de aplicativos que não têm grupos de entrega associados.
  - Grupos de aplicativos com grupos de entrega associados que não contêm máquinas.
  - Um grupo de entrega que não contém máquinas.

- **Manually defined:** aplicativos localizados no site ou em outro lugar na sua rede. Quando você seleciona essa origem, uma nova página é iniciada onde você digita o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Depois de inserir essas informações, clique em **OK**.

- **Existing**: aplicativos adicionados anteriormente ao site. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**. Essa origem não pode ser selecionada se o site não tiver aplicativos.

- **App-V**: aplicativos em pacotes App-V. Quando você seleciona essa origem, uma nova página é iniciada onde você seleciona **App-V Server** ou **Application Library**. Na exibição resultante, marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V. Esta origem não pode ser selecionada (ou pode não aparecer) se o App-V não estiver configurado para o site.

Como observado, certas entradas no menu suspenso **Add** não são selecionáveis se não houver uma origem válida desse tipo. As origens incompatíveis não são listadas (por exemplo, não é possível adicionar grupos de aplicativos a grupos de aplicativos, de modo que a origem não é listada quando você cria um grupo de aplicativos).

Etapa 4. Escopos

Esta página só aparece se você tiver criado anteriormente um escopo personalizado. Por padrão, o escopo **All** é selecionado. Para obter mais informações, consulte Administração delegada.

Etapa 5. Resumo

Insira um nome para o grupo de aplicativos. Você também pode (opcionalmente) inserir uma descrição.

Revise as informações de resumo e clique em **Finish**.

Gerenciar grupos de aplicativos

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Este artigo descreve como gerenciar os grupos de aplicativos que você criou.

Consulte Aplicativos para obter informações sobre o gerenciamento de aplicativos em grupos de aplicativos ou grupos de entrega, incluindo como:

- Adicionar ou remover aplicativos em um grupo de aplicativos.
- Alterar associações de grupos de aplicativos.

O gerenciamento de grupos de aplicativos requer as permissões de administrador delegado da função interna Delivery Group Administrator. Consulte Administração delegada para obter detalhes.

Ativar ou desativar um grupo de aplicativos

Quando um grupo de aplicativos está ativado, ele pode entregar os aplicativos que foram adicionados a ele. A desativação de um grupo de aplicativos desativa cada aplicativo naquele grupo. No entanto, se esses aplicativos também estiverem associados a outros grupos de aplicativos ativados, eles poderão ser entregues a partir desses outros grupos. Se o aplicativo foi explicitamente adicionado aos grupos de entrega associados ao grupo de aplicativos, a desativação do grupo de aplicativos não afetará os aplicativos nesses grupos de entrega.

Um grupo de aplicativos é ativado quando você o cria. Você não pode alterar essa configuração quando cria o grupo.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Na página **Settings**, marque ou desmarque a caixa de seleção**Enable Application Group**.
4. Clique em **Apply**, para manter a janela aberta, ou clique em **Save** para aplicar alterações e fechar a janela.

Ativar ou desativar o compartilhamento de sessão do aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é ativado quando você cria um grupo de aplicativos. Você não pode alterar essa configuração quando cria o grupo. Para obter mais informações, consulte Compartilhamento de sessão com grupos de aplicativos.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Na página **Settings**, marque ou desmarque a caixa de seleção **Enable application session sharing between Application Groups**.
4. Clique em **Apply**, para manter a janela aberta, ou clique em **Save** para aplicar alterações e fechar a janela.

Desativar o compartilhamento de sessão do aplicativo em um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é ativado por padrão quando você cria um grupo de aplicativos. Se você desativar o compartilhamento de sessão do aplica-

tivo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanece ativado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão do aplicativo desativado entre os aplicativos que eles contêm. Em algumas circunstâncias, esta opção é desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não integrados em janelas de aplicativos em tamanho real em monitores separados.

Quando você desativa o compartilhamento de sessão do aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão do aplicativo. Se uma sessão desconectada adequada estiver disponível, e que esteja executando o mesmo aplicativo, ela será reconectada. Por exemplo, ao iniciar o Bloco de Notas com uma sessão desconectada com o Bloco de Notas em execução, a sessão é reconectada em vez de uma ser criada. Quando várias sessões desconectadas adequadas estão disponíveis, uma das sessões é escolhida para a reconexão, de forma aleatória, mas determinística. Quando a situação ocorre novamente nas mesmas circunstâncias, a mesma sessão é escolhida, mas a sessão não é necessariamente previsível de outra forma.

Use o SDK do PowerShell para desativar o compartilhamento de sessão do aplicativo para todos os aplicativos em um grupo de aplicativos existente ou para criar um grupo com compartilhamento de sessão do aplicativo desativado.

Exemplos de cmdlet do PowerShell

Para desativar o compartilhamento de sessão, use os cmdlets do Broker PowerShell `New-BrokerApplicationGroup` ou `Set-BrokerApplicationGroup` com o parâmetro `SessionSharingEnabled` definido como `False` e o parâmetro `SingleAppPerSession` definido como `True`.

- Por exemplo, para criar um grupo de aplicativos com compartilhamento de sessão do aplicativo desativado para todos os aplicativos do grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Por exemplo, para desativar o compartilhamento de sessão do aplicativo entre todos os aplicativos em um grupo de aplicativos existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

Considerações

- Para ativar a propriedade `SingleAppPerSession` você deve definir a propriedade `SessionSharingEnabled` como False. As duas propriedades não devem ser ativadas ao

mesmo tempo. O parâmetro `SessionSharingEnabled` refere-se ao compartilhamento de sessões entre grupos de aplicativos.
- O compartilhamento de sessão do aplicativo funciona apenas para aplicativos associados a grupos de aplicativos, mas que não estão associados a grupos de entrega. Todos os aplicativos associados diretamente a um grupo de entrega compartilham a sessão por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, verifique se os grupos não têm configurações conflitantes. Por exemplo, um grupo com a opção definida como `True` e outro grupo com a opção definida como `False` resulta em um comportamento imprevisível.

Renomear um grupo de aplicativos

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Rename Application Group** na barra de ações.
3. Especifique o novo nome exclusivo e clique em **OK**.

Adicionar, remover ou alterar a prioridade das associações de grupos de entrega com um grupo de aplicativos

Um grupo de aplicativos pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam somente áreas de trabalho, se as duas condições a seguir forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão anterior a 7.9.
- Você tem a permissão Edit Delivery Group

O tipo de grupo de entrega é automaticamente convertido em "áreas de trabalho e aplicativos" quando a caixa de diálogo **Edit Application Group** é confirmada.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Delivery Groups**.
4. Para adicionar grupos de entrega, clique em **Add**. Marque as caixas de seleção dos grupos de entrega disponíveis. (Grupos de entrega incompatíveis não podem ser selecionados.) Quando terminar suas seleções, clique em **OK**.

5. Para remover grupos de entrega, marque as caixas de seleção dos grupos que deseja remover e clique em **Remove**. Confirme a exclusão quando solicitado.
6. Para alterar a prioridade dos grupos de entrega, marque a caixa de seleção do grupo de entrega e clique em **Edit Priority**. Digite a prioridade (0 = mais alta) e clique em **OK**.
7. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Save** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover uma restrição de marca em um grupo de aplicativos

Adicionar, alterar e remover restrições de marca pode ter efeitos imprevisíveis sobre quais máquinas são consideradas para a inicialização do aplicativo. Consulte as considerações e precauções em Marcas.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Delivery Groups**.
4. Para adicionar uma restrição de marca, selecione **Restrict launches to machines with the tag** e, em seguida, selecione a marca na lista suspensa.
5. Para alterar ou remover uma restrição de marca, selecione uma marca diferente ou remova a restrição de marca completamente desmarcando **Restrict launches to machines with this tag**.
6. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Save** para aplicar as alterações e fechar a janela.

Adicionar ou remover usuários em um grupo de aplicativos

Para obter informações detalhadas sobre usuários, consulte Criar grupos de aplicativos.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Users**. Indique se deseja permitir que todos os usuários nos grupos de entrega associados usem aplicativos no grupo de aplicativos ou apenas usuários e grupos específicos. Para adicionar usuários, clique em **Add** e, em seguida, especifique os usuários que deseja adicionar. Para remover usuários, selecione um ou mais usuários e clique em **Remove**.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Save** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover um ícone de aplicativo em um grupo de aplicativos

Execute as etapas a seguir para adicionar, alterar ou remover um ícone de aplicativo.

1. Selecione **Applications** no painel esquerdo.
2. Na guia **Applications**, selecione um aplicativo e, em seguida, selecione **Properties**.

   Para fazer alterações no nível de um grupo de aplicativos, navegue para a guia **Application Groups**, selecione um aplicativo em um grupo e selecione **Properties**.
3. Selecione a página **Delivery** e, em seguida, selecione **Change**. A janela **Select Icon** é exibida.
4. Na janela **Select Icon**, siga um destes procedimentos:

   - Para adicionar um ícone, selecione **Add** e, em seguida, navegue até o ícone.
   - Para remover um ícone, selecione-o e selecione **Remove**.
   - Para alterar um ícone, selecione-o para o aplicativo.

   > **Importante:**
   >
   > - Não é possível adicionar um ícone cujo tamanho seja maior que 200 KB.
   > - Você pode adicionar apenas arquivos .icon.
   > - Você não pode remover ícones internos.
   > - Não é possível remover um ícone de um aplicativo que está em uso.

5. Selecione **Save** para aplicar as alterações e fechar a janela.

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (não é possível editar o escopo All). Para obter mais informações, consulte Administração delegada.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Scopes**. Marque ou desmarque a caixa de seleção ao lado de um escopo.
4. Clique em **Apply** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Save** para aplicar as alterações e fechar a janela.

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (não é possível editar o escopo All). Para obter mais informações, consulte Administração delegada.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Edit Application Group** na barra de ações.
3. Selecione a página **Scopes**. Marque ou desmarque a caixa de seleção ao lado dos escopos que você deseja alterar.
4. Selecione **Apply** para aplicar as alterações feitas e manter a janela aberta, ou selecione **Save** 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 faz com que um ou mais aplicativos não mais pertençam a um grupo, você será avisado de que a exclusão do grupo também removerá os aplicativos. Você pode então confirmar ou cancelar a exclusão.

A exclusão de um aplicativo não o exclui de seu local de origem. No entanto, se quiser torná-lo disponível novamente, você deve adicioná-lo novamente.

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione a guia **Application Groups**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Delete Group** na barra de ações.
3. Confirme a exclusão quando solicitado.

Organizar grupos de aplicativos usando pastas

Você pode criar pastas para organizar grupos de aplicativos e facilitar o acesso. Para criar e gerenciar pastas de grupos de aplicativos, você pode usar a barra de ações ou o menu ativado pelo botão direito do mouse. Você também pode arrastar um grupo de aplicativos ou uma pasta para o local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas com até cinco níveis (excluindo a pasta raiz padrão).
- Uma pasta pode conter grupos de aplicativos e subpastas. Você pode excluir uma pasta somente se ela e suas subpastas não contiverem grupos de aplicativos.
- Todos os recursos (como catálogos de máquinas, grupos de entrega, aplicativos e grupos de aplicativos) compartilham uma árvore de pastas no backend. Para evitar conflitos de nome com outras pastas de recursos ao renomear ou mover pastas, recomendamos que você atribua nomes diferentes às pastas de primeiro nível nas diferentes árvores de pastas.

Remote PC Access

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O Remote PC Access é um recurso do Citrix Virtual Apps and Desktops que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

O Remote PC Access usa os mesmos componentes do Citrix Virtual Apps and Desktops que entregam áreas de trabalho e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Remote PC Access são os mesmos que os necessários para implantar o Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

O recurso consiste em um catálogo de máquinas do tipo **Remote PC Access** que proporciona a essa funcionalidade:

- Capacidade de adicionar máquinas especificando unidades organizacionais. Essa capacidade facilita a adição de PCs em massa.
- Atribuição automática do usuário com base no usuário que faz login no PC Windows do escritório. Oferecemos suporte a atribuições de usuário único e multiusuário. Por padrão, atribuímos automaticamente vários usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, entre no Web Studio, vá para **Settings** e desative a configuração **Enable automatic assignment of multiple users for Remote PC Access**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs físicos Linux
- PCs físicos em pool (isto é, aleatoriamente atribuídos, não dedicados)

> **Observações:**
>
> Para obter detalhes sobre as versões do SO com suporte, consulte os requisitos do sistema para o VDA para SO de sessão única e Linux VDA.
>
> Para implantações locais, o Remote PC Access é válido apenas para licenças do Citrix Virtual Apps and Desktops Advanced ou Premium. As sessões consomem licenças da mesma maneira que outras sessões do Citrix Virtual Desktops. No caso do Citrix Cloud, o Remote PC Access é válido para o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) e Workspace Premium Plus.

Considerações

Embora todos os requisitos e considerações técnicas que se aplicam ao Citrix Virtual Apps and Desktops em geral também se apliquem ao Remote PC Access, alguns podem ser mais relevantes ou exclusivos para casos de uso de PC físico.

> **Importante:**
>
> Os sistemas físicos do Windows 11 (e alguns que executam o Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software do VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:
>
> - Use a opção "/physicalmachine"juntamente com a opção "/remotepc"como parte da instalação da linha de comando do VDA
> - Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada acima não tenha sido usada
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - Nome: ForceEnableRemotePC
>   - Tipo: DWORD
>   - Dados: 1

Considerações sobre implantação

Ao planejar a implantação do Remote PC Access, adote algumas medidas gerais.

- Você pode adicionar o Remote PC Access a uma implantação existente do Citrix Virtual Apps and Desktops. Antes de escolher essa opção, considere o seguinte:
  - Os Delivery Controllers ou os Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?

  - Os bancos de dados locais do site e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os VDAs existentes e os novos VDAs do Remote PC Access ultrapassam o número máximo de VDAs suportados por site?

- Você deve implantar o VDA em PCs no escritório por meio de um processo automatizado. A seguir estão as opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instale VDAs usando SCCM.
  - Scripts de implantação: Instale VDAs usando scripts.
- Veja as Considerações de segurança do Remote PC Access.

> **Nota:**
>
> Ao projetar o acesso ao PC remoto, você deve considerar o número de monitores físicos conectados à GPU no PC remoto e atualmente configurados/operacionais. Mesmo que o monitor não seja usado na sessão Citrix, mas seja detectado pela GPU, a presença do monitor é computada no limite máximo de monitores suportados pela GPU.

Considerações do catálogo de máquinas

O tipo de catálogo de máquinas exigido depende do caso de uso:

- Catálogo de máquinas de Remote PC Access
  - PCs Windows dedicados
  - PCs Windows multiusuário dedicados Esse caso de uso se aplica a PCs físicos de escritório que vários usuários podem acessar remotamente em turnos diferentes.
  - PCs Windows em pool. Esse caso de uso se aplica a PCs físicos que vários usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas com SO de sessão única
  - Estático - PCs Linux dedicados
  - Aleatório - PCs Linux em pool

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.

- Ao escolher as UOs em que as contas da máquina residem, selecione UOs de nível inferior para obter maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de bancos/caixas/guichês, selecione **Tellers** para obter maior granularidade. Caso contrário, você pode selecionar **Officers** ou **Bank** baseado nas exigências.
- Mover ou excluir UOs depois de atribuídas a um catálogo de máquinas de Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Portanto, tenha o cuidado de planejar adequadamente para que as atualizações de atribuição da unidade organizacional a catálogos de máquina sejam contabilizadas no plano de alteração do Active Directory.
- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas por causa da estrutura de unidade organizacional, você não precisa selecionar nenhuma UO. Você pode usar o PowerShell para adicionar máquinas ao catálogo posteriormente. As atribuições automáticas de usuário continuam funcionando se a atribuição da área de trabalho estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo da máquina juntamente com as atribuições do usuário está disponível em GitHub.
- Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Remote PC Access**.

Considerações do Linux VDA

Estas considerações são específicas para o Linux VDA:

- Use o Linux VDA em máquinas físicas somente no modo não 3D. Devido a limitações do driver do NVIDIA, a tela local do PC não pode ser desligada e exibe as atividades da sessão quando o modo HDX 3D está ativado. Mostrar essa tela é um risco de segurança.
- Use catálogos de máquina do tipo SO de sessão única para máquinas físicas Linux.
- A atribuição automática de usuário não está disponível para máquinas Linux.
- Se os usuários já estiverem conectados em seus PCs localmente, as tentativas de iniciar os PCs a partir do StoreFront falharão.
- Opções de economia de energia não estão disponíveis para máquinas Linux.

Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e as considerações para PCs físicos.

- Não há suporte para:
  - Chaveadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo notebooks e PCs All-in-One e NVIDIA Optimus.

  - Máquinas de inicialização dupla.

- Conecte o teclado e o mouse diretamente ao PC. Esses periféricos poderão se tornar indisponíveis se forem conectados ao monitor ou a outros componentes que podem ser desligados ou desconectados. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desative os componentes.
- Os PCs devem ser ingressados em um domínio do Active Directory Domain Services
- A Inicialização Segura é suportada apenas no Windows 10 e Windows 11.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é recomendada para ter-se maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:

  1. Defina as configurações de energia para deixar o adaptador sem fio ligado.
  2. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registra até que o usuário faça logon. O PC não está disponível para acesso remoto até que um usuário tenha feito logon.
  3. Certifique-se de que os Delivery Controllers ou os Cloud Connectors possam ser acessados da rede Wi-Fi.

- Você pode usar o Remote PC Access em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:

  1. Desative o recurso de hibernação.
  2. Desative o recurso de suspensão.
  3. Defina a ação de fechar a tampa como **Não fazer nada**.
  4. Defina a ação "pressionar o botão de energia"como **Desligar**.
  5. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Remote PC Access é suportado em dispositivos Surface Pro com Windows 10. Siga as mesmas instruções para laptops mencionadas anteriormente.
- Se estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixa o laptop, o VDA se registra novamente nos Delivery Controllers ou Cloud Connectors por Wi-Fi. No entanto, quando você reencaixa o laptop, o VDA não muda para a conexão com fio, a menos que você desconecte o adaptador de conexão sem fio. Alguns dispositivos fornecem funcionalidade interna para desconectar o adaptador de conexão sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador de conexão sem fio. Revise as considerações de Wi-Fi mencionadas anteriormente.

Faça o seguinte para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

1. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão**, e defina **Suspender** como **Nunca**.
2. Em **Gerenciador de dispositivos > Adaptadores de rede > Adaptador Ethernet** vá para **Gerenciamento de energia** e desmarque **O computador pode desligar o dispositivo para economizar energia**. Assegure que **Permitir que este dispositivo acorde o computador** esteja selecionado.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, o recurso aparece como indisponível se já estiver sendo usado por outro usuário.
- Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

Sequência de configuração

Esta seção contém uma visão geral de como configurar o Remote PC Access ao usar o catálogo da máquinas do tipo **Remote PC Access**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquina.

1. Somente site local –Para usar o recurso Wake on LAN integrado, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para o Remote PC Access:

   a) Selecione o tipo de site **Remote PC Access**.
   b) Em **Power Management**, escolha se deseja ativar ou desabilitar o gerenciamento de energia para o catálogo de máquinas Remote PC Access. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.
   c) Forneça as informações nas páginas **Users** e **Machine Accounts**

   Ao concluir essas etapas, é criado um catálogo de máquinas chamado **Remote PC Access Machines** e um grupo de entrega chamado **Remote PC Access Desktops**.
3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a) Crie um catálogo de máquinas do tipo **Remote PC Access** (página Operating System do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Tenha o cuidado de atribuir a unidade organizacional correta para que os PCs de destino sejam disponibilizados para uso com o Remote PC Access.

b) Crie um grupo de entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um grupo de entrega, consulte Criar grupos de entrega. Certifique-se de atribuir o grupo de entrega a um grupo do Active Directory que contém os usuários que exigem acesso a seus PCs.

4. Implantar o VDA nos PCs do escritório.

   - Recomendamos usar o instalador de VDA básico de SO de sessão única (VDAWorkstationCoreSetup.exe).
   - Você também pode usar o instalador de VDA completo de sessão única (VDAWorkstationSetup.exe) com a opção `/remotepc/physicalmachine`, que chega ao mesmo resultado que o uso do instalador de VDA básico.

     > **Nota:**
     >
     > Para a instalação do RemotePC, use o argumento `/physicalmachine` com `/remotepc` para que o VDA se comporte conforme o esperado em determinados cenários de usuário.

   - Ative a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto por meio do Citrix Director. Para isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para poder ver as informações de duração de logon no Director, você deve usar o instalador de VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Para incluir esse componente, use a opção `/includeadditional`. Para obter detalhes, consulte Instalar usando a linha de comando.
   - Para obter informações sobre como implantar o VDA usando o SCCM, consulte Instalar VDAs usando SCCM.
   - Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

   Depois que você concluir com êxito as etapas 2 a 4, os usuários são atribuídos automaticamente às suas próprias máquinas quando fazem logon localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente usado para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace está disponível em `https://www.citrix.com/downloads/` ou nas lojas de aplicativos para dispositivos móveis com suporte.

Recursos gerenciados através do registro

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

Desativar atribuições automáticas de multiusuário

Em cada Delivery Controller, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nome: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Dados: 0

Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina Remote PC Access entre em um estado de suspensão, adicione a configuração de registro ao VDA e reinicialize a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra no modo de suspensão depois que o timer pré-configurado de inatividade expira. Depois que a máquina acorda, ela se registra novamente no Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Dados: 1

Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é desconectada automaticamente quando um usuário local inicia uma sessão na máquina (pressionando CTRL+ATL+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e reinicialize a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Dados: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é confirmada dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Dados:
  - 1 - O usuário remoto sempre tem prioridade se não responder à mensagem na interface do usuário dentro do período de tempo limite especificado. Esse comportamento é o padrão se esse parâmetro não estiver configurado.
  - 2 - O usuário local tem prioridade.

O tempo limite padrão para impor o modo Remote PC Access é de 30 segundos. Você pode configurar esse tempo limite, mas não o defina abaixo de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout
- Tipo: DWORD
- Dados: número de segundos do tempo limite em valores decimais

Quando um usuário quiser forçar o acesso ao console, o usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local da sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon no PC enquanto estiver em uso por um usuário remoto, o usuário remoto receberá uma mensagem. A mensagem pergunta se deve permitir ou negar a conexão do usuário local. Permitir que a conexão desconecta a sessão do usuário remoto.

Log de gerenciamento de sessão

O Remote PC Access agora tem recursos de log que registram quando alguém tenta acessar um PC com uma sessão ativa do ICA. Isso permite que você monitore seu ambiente em busca de atividades indesejadas ou inesperadas e seja capaz de auditar esses eventos se precisar investigar incidentes.

Os eventos são registrados no log usando o Visualizador de Eventos do Windows e estão em **Applications and Services > Citrix > HostCore > ICA Service > Admin**.

Há três eventos distintos que são registrados no log ao usar o Remote PC Access.

Evento Ctrl+Alt+Del

Este evento aparece quando o usuário local pressiona Ctrl+Alt+Del no teclado do console com uma sessão remota ativa.

Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 43, 44, 45
- Fonte: ICA Service

ID do evento 43 Este ID de evento aparece quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:

```
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 é desconectada por diferentes motivos.

Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 46, 47, 48
- Fonte: ICA Service

ID do evento 46 Este ID de evento aparece quando a sessão remota é desconectada e quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:

```
The remote session for <remoteUserName> has been
   disconnected.
```

ID do evento 47 Este ID de evento aparece quando o usuário remoto concorda em desconectar a sessão e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode é 2 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
The remote session for <remoteUserName> has been
   disconnected because the user accepted the request to
   disconnect the session.
```

ID do evento 48 Este ID de evento aparece quando o usuário remoto não recusa a solicitação de desconexão dentro do período de tempo limite específico e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
The remote session for <remoteUserName> has been
   disconnected because the user did not decline the
   disconnection request within the configured timeout
   period (<timeout period>).
```

Evento Ctrl+Alt+Del pressionado duas vezes Este evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 49
- Fonte: ICA Service

ID do evento 49 Este ID de evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

- Mensagem:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

Wake on LAN

O Remote PC Access suporta Wake on LAN, o que dá aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs no escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina for desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede em que o PC reside quando instruído pelo Delivery Controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura extras ou soluções de terceiros para a entrega dos pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN legado baseado em SCCM. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN —SCCM integrado.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes sobre a capacidade de suporte, consulte os Requisitos do sistema para VDA.
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows

Configurar o Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops no local, a configuração do Wake on LAN integrado só será suportada usando o PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas Remote PC Access se ainda não tiver um.
2. Crie a conexão de host Wake on LAN se ainda não tiver uma.

   > **Nota:**
   >
   > Para usar o recurso Wake on LAN, se você tiver uma conexão de host do tipo "Microsoft Configuration Manager Wake on LAN", crie uma nova conexão de host.

3. Obtenha o identificador exclusivo da conexão de host Wake on LAN.
4. Associe a conexão de host Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host Wake on LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```


Quando a conexão do host estiver pronta, execute os seguintes comandos para obter o identificador exclusivo de conexão do host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Depois de obter o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo da máquinas do Remote PC Access:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

Considerações de design

Ao planejar o uso do Wake on LAN com Remote PC Access, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host Wake on LAN.
- Para que um PC acorde outro PC, os dois PCs devem estar na mesma sub-rede e usar a mesma conexão de host Wake on LAN. Não importa se os PCs estão no mesmo catálogo de máquinas ou em catálogos diferentes.
- As conexões de host são atribuídas a zonas específicas. Se a sua implantação contém mais de uma zona, você precisa de uma conexão de host Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Os pacotes mágicos são transmitidos usando o endereço de transmissão global 255.255.255.255. Certifique-se de que o endereço não esteja bloqueado.
- Deve haver pelo menos um PC ligado na sub-rede –para cada conexão Wake on LAN –para conseguir acordar as máquinas nessa sub-rede.

Considerações operacionais

Veja as considerações a seguir para usar o recurso Wake on LAN:

- O VDA deve se registrar pelo menos uma vez antes que o PC possa ser ativado usando o recurso Wake on LAN integrado.
- Wake on LAN só pode ser usado para acordar PCs. Ele não suporta outras ações de energia, como reinicializar ou desligar.
- Depois que a conexão Wake on LAN é criada, ela fica visível no Web Studio. No entanto, a edição de suas propriedades no Web Studio não é suportada se você estiver usando o Citrix Virtual Apps and Desktops no local.
- Os pacotes mágicos são enviados de uma destas duas maneiras:

1. Quando um usuário tenta iniciar uma sessão no PC e o VDA não está registrado
2. Quando um administrador envia manualmente um comando de envio de energia a partir do Web Studio ou do PowerShell

- Como o Delivery Controller não tem conhecimento do estado de energia de um PC, o Web Studio exibe **Not Supported** sob o estado de energia. O Delivery Controller usa o estado de registro do VDA para determinar se um PC está ligado ou desligado.

Wake on LAN —Integrado a SCCM

O Wake on LAN integrado a SCCM é uma opção alternativa de Wake on LAN para Remote PC Access que só está disponível com o Citrix Virtual Apps and Desktops local.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN integrado a SCCM:

- Citrix Virtual Apps and Desktops 1912 ou posterior
- PCs físicos:
  - VDA versão 1912 ou posterior
  - Windows 10. Para obter detalhes sobre a capacidade de suporte, consulte os Requisitos do sistema para VDA.
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou posterior

Configurar Wake on LAN integrado a SCCM

Conclua os seguintes pré-requisitos:

1. Configure o SCCM 2012 R2, 2016 ou 2019 dentro da organização. Em seguida, implante o cliente SCCM em todas as máquinas de Remote PC Access, dando tempo suficiente para que o ciclo de inventário do SCCM agendado seja executado, ou force um manualmente, se necessário.
2. Para dar suporte ao proxy de ativação, ative a opção no SCCM. Para cada sub-rede na organização que contém PCs que usam o recurso Remote PC Access Wake on LAN, certifique-se de que três ou mais máquinas possam servir como máquinas sentinelas.
3. Para obter suporte a pacotes mágicos, configure roteadores de rede e firewalls para permitir que os pacotes mágicos sejam enviados usando uma transmissão direcionada por sub-rede ou unicast.

4. Configure o Wake on LAN nas configurações BIOS/UEFI de cada PC.
5. Implante o VDA nos PCs físicos se ainda não tiver feito.

Depois de tratar dos pré-requisitos, execute as seguintes etapas para permitir que o Delivery Controller se comunique com o SCCM:

1. Crie uma conexão de host para o SCCM. Para obter mais informações, consulte Conexões e recursos.
    - Selecione **Microsoft Configuration Manager Wake on LAN** como o tipo de conexão.
    - As credenciais inseridas devem ter acesso às coleções no escopo e devem ter a função **Remote Tools Operator**.
2. Selecione a conexão no Web Studio e, em seguida, selecione **Edit Connection** e clique em **Advanced**.
3. Selecione a opção apropriada para lidar com Wake on LAN:
    - Se estiver usando o proxy de ativação, selecione a primeira opção: **Microsoft System Center Configuration Manager Wake-up proxy**.
    - Se estiver usando pacotes mágicos, selecione a segunda opção: **Wake on LAN packets transmitted by the Delivery Controller**.
        - Selecione o método de transmissão apropriado: **subnet-directed boradcasts** ou **unicast**.

Depois de criar a conexão de host, associe a conexão a um catálogo Remote PC Access:

- Se você estiver criando um novo catálogo Remote PC Access, na página **Operating System** do assistente de criação de catálogo, selecione **Remote PC Access** como o tipo de catálogo e escolha a conexão apropriada na lista suspensa.
- Para adicionar Wake on LAN a um catálogo Remote PC Access existente:
    1. No Web Studio, vá para o nó **Machine Catalogs**, selecione o catálogo da máquinas e, em seguida, selecione **Edit Machine Catalog**.
    2. Selecione a guia **Power Management** e escolha **Yes** para permitir o gerenciamento de energia do catálogo de máquinas.
    3. Selecione a conexão apropriada na lista suspensa e clique em **OK**.

Solução de problemas

Desligamento do monitor não funciona

Se o monitor local do PC Windows não for desligado enquanto houver uma sessão HDX ativa (o monitor local exibir o que está acontecendo na sessão), é provável que seja devido a problemas com o

driver do fornecedor da GPU. Para resolver o problema, dê prioridade maior ao Citrix Indirect Display Driver (IDD) do que ao driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para obter mais detalhes sobre as prioridades do adaptador de exibição e criação de monitor, consulte o artigo CTX237608 do Knowledge Center.

A sessão desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão ativada

A notificação de gerenciamento de sessão controlada pelo valor do registro **SasNotification** funciona somente quando o modo Remote PC Access está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Informações de diagnóstico

As informações de diagnóstico sobre o Remote PC Access são gravadas no log de Eventos de Aplicativos do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas, descartando-se as mensagens duplicadas.

- 3300 (informativo): máquina adicionada ao catálogo
- 3301 (informativo): máquina adicionada ao grupo de entrega
- 3302 (informativo): máquina atribuída ao usuário
- 3303 (erro): exceção

Gerenciamento de energia

Se o gerenciamento de energia do Remote PC Access estiver ativado, as transmissões direcionadas por sub-rede não iniciarão máquinas que estejam em uma sub-rede diferente daquela do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando transmissões direcionadas por sub-rede e o suporte AMT não estiver disponível, tente o método Wake-up proxy ou Unicast. Certifique-se de que essas configurações estejam ativadas nas propriedades avançadas para a conexão de gerenciamento de energia.

A sessão remota ativa registra a entrada local da tela sensível ao toque

Quando o VDA habilita o modo Remote PC Access, a máquina ignora a entrada local da tela sensível ao toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Mais recursos

Veja a seguir outros recursos para Remote PC Access:

- Orientação sobre o projeto da solução: Remote PC Access Design Decisions
- Exemplos de arquiteturas do Remote PC Access: Reference Architecture for Citrix Remote PC Access Solution.

Publicar conteúdo

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles

> de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Você pode publicar um aplicativo que seja simplesmente um caminho UNC ou URL para um recurso, como um documento do Microsoft Word ou um link da Web. Esse recurso é conhecido como conteúdo publicado. A capacidade de publicar conteúdo adiciona flexibilidade à forma como você entrega conteúdo aos usuários. Você se beneficia do controle de acesso e gerenciamento de aplicativos existentes. Você também pode especificar se deseja usar aplicativos locais ou publicados para abrir o conteúdo.

O conteúdo publicado aparece como os outros aplicativos no StoreFront e o aplicativo Citrix Workspace. Os usuários o acessam da mesma forma que acessam aplicativos. No cliente, o recurso abre como de costume.

- 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 o conteúdo usando o SDK do PowerShell. Você não pode usar o Web Studio para publicar conteúdo. No entanto, você pode usar o Web Studio para editar as propriedades do aplicativo mais tarde, depois que elas forem publicadas.

Visão geral e preparação da configuração

Publicar conteúdo usa o cmdlet `New-BrokerApplication` com as seguintes propriedades de chave. (Consulte a ajuda do cmdlet para obter descrições de todas as propriedades do cmdlet.)

```
1 New-BrokerApplication –ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

A propriedade `ApplicationType` deve ser `PublishedContent`.

A propriedade `CommandLineExecutable` especifica a localização do conteúdo publicado. Os seguintes formatos são suportados, com um limite de 255 caracteres.

- Endereço do 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 do arquivo UNC (por exemplo, `file://myServer/myShare/myFile.asf` ou `\\myServer\myShare\myFile.asf`)

Certifique-se de ter o SDK correto.

- Para implantações do Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), faça o download e instale o Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- Para implantações locais do Citrix Virtual Apps and Desktops, use o PowerShell SDK instalado com o Delivery Controller. Adicionar um aplicativo de conteúdo publicado requer a versão mínima 7.11 do Delivery Controller.

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 com SO multissessão do catálogo. O aplicativo WordPad foi adicionado ao grupo.
- São feitas atribuições ao nome do grupo de entrega, à localização `CommandLineExecutable` e ao nome do aplicativo.

Introdução

Na máquina que contém o PowerShell SDK, abra o PowerShell.

O cmdlet a seguir adiciona o snap-in apropriado do PowerShell SDK e atribui o registro retornado do grupo de entrega.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Se você estiver usando o Citrix DaaS, autentique-se inserindo suas credenciais do Citrix Cloud. Se houver mais de um cliente, escolha um.

Publicar um URL

Depois de atribuir o local e o nome do aplicativo, o cmdlet a seguir publica a página inicial da Citrix como um aplicativo.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication –ApplicationType PublishedContent –
     CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
     Uid
```



```
<!--NeedCopy-->
```

Verifique o resultado:

- Abra o StoreFront e faça logon como um usuário que pode acessar aplicativos no grupo de entrega PublishedContentApps. A exibição inclui o aplicativo recém-criado com o ícone padrão. Para saber mais sobre como personalizar o ícone, consulte https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Clique no aplicativo **Citrix Home Page**. O URL é iniciado em uma nova guia em uma instância executada localmente do seu navegador padrão.

Publicar recursos localizados em caminhos UNC

Neste exemplo, o administrador já criou um compartilhamento chamado `PublishedResources`. Depois de atribuir os locais e os nomes dos aplicativos, os seguintes cmdlets publicam um arquivo RTF e um DOCX no 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
<!--NeedCopy-->
```

Verifique o resultado:

- Atualize a 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.

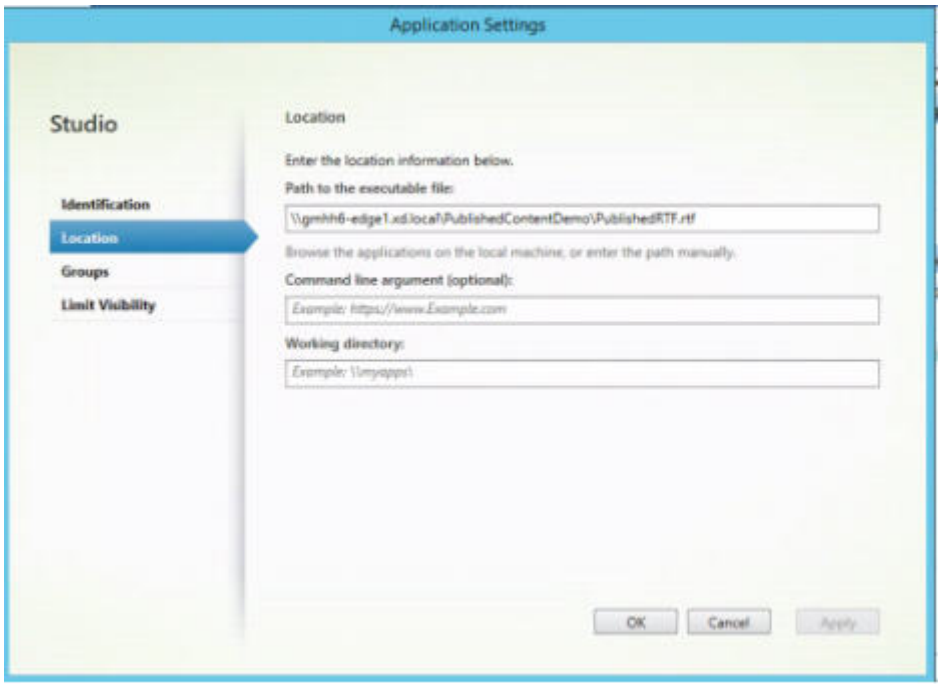
Visualizar e editar aplicativos PublishedContent

Você gerencia o conteúdo publicado usando os mesmos métodos que você usa para outros tipos de aplicativos.

Para visualizar e editar aplicativos `PublishedContent`, siga estas etapas:

1. Entre no Web Studio e selecione **Applications** no painel esquerdo.
2. Na guia **Applications**, selecione um aplicativo PublishedContent e, em seguida, selecione **Properties**.

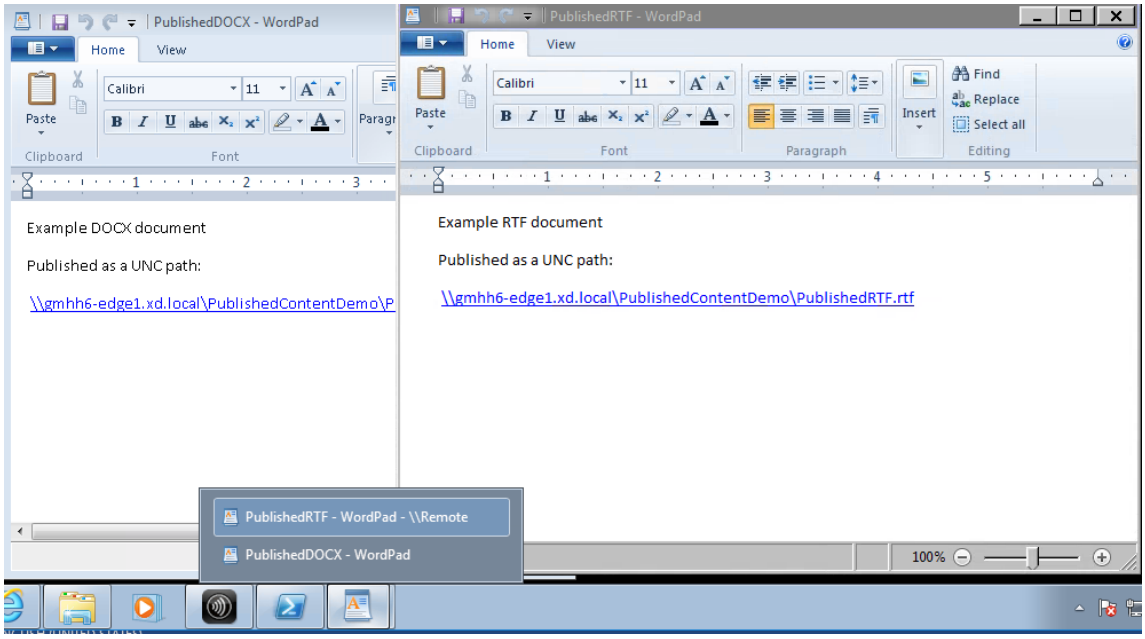
   As propriedades do aplicativo (como visibilidade do usuário, associação de grupo e atalho) se aplicam ao conteúdo publicado. No entanto, você não pode alterar o argumento da linha de comando ou as propriedades do diretório de trabalho na página **Location**.
3. Para alterar o recurso, modifique o campo **Path to the executable file** na página.



4. Para usar um aplicativo publicado para abrir um aplicativo `PublishedContent` (em vez de um aplicativo local), siga estas etapas:

   Neste exemplo, o aplicativo WordPad publicado é editado para criar uma associação de tipo de arquivo para arquivos .rtf.

   a) Ative o modo de manutenção para o grupo de entrega.
   b) Edite a propriedade **File Type Association**.
   c) Desative o modo de manutenção quando terminar.
   d) Atualize o StoreFront para carregar as alterações feita em File Type Association e, em seguida, clique nos aplicativos **PublishedRTF** e **PublishedDOCX**. Observe a diferença. **PublishedDOCX** ainda abre no WordPad local. No entanto, **PublishedRTF** agora abre no WordPad publicado devido à associação de tipo de arquivo.



Para obter mais informações

- Criar catálogos de máquinas
- Criar grupos de entrega
- Alterar propriedades do aplicativo

Server VDI

June 28, 2023

Use o recurso Server VDI (Virtual Desktop Infrastructure) para fornecer uma área de trabalho a partir de um sistema operacional de servidor para um único usuário.

- Os administradores Enterprise podem entregar sistemas operacionais de servidor como áreas de trabalho VDI, o que pode ser valioso para usuários como engenheiros e designers.
- Os provedores de serviços podem oferecer áreas de trabalho a partir da nuvem. Essas áreas de trabalho estão em conformidade com o Contrato de Licença de Provedor de Serviços (SPLA) da Microsoft.

Suporte:

- Nas implantações do Citrix Virtual Apps and Desktops e Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), o Server VDI é suportado no Windows Server 2022, Windows Server 2019 e Windows Server 2016.

- Todas as implantações do Server VDI são compatíveis com a tecnologia da camada de personalização do usuário.
- Para que o Server VDI funcione com dispositivos TWAIN, como scanners, o recurso Experiência Desktop do Windows Server deve ser instalado.
- Os seguintes recursos não podem ser usados com o Server VDI:
  - Aplicativos hospedados
  - Acesso a aplicativo local
  - Conexões de área de trabalho diretas (não agenciadas)
  - Remote PC Access

Instalar e configurar Server VDI

1. Prepare o servidor Windows para instalação.
   - Use o Windows Server Manager para garantir que os serviços da função Serviços de Área de Trabalho Remota não sejam instalados. Se foram instalados anteriormente, remova-os. A instalação do VDA falhará se esses serviços de função estiverem instalados.
   - Assegure-se de que a propriedade **Restringir cada usuário a uma sessão** esteja ativada. No servidor Windows, edite o registro da 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 ou imagem mestre de servidor compatível, especificando as opções `/quiet` e `/servervdi`. (Por padrão, a interface gráfica do instalador bloqueia o VDA do SO de sessão única Windows no sistema operacional de um servidor. Usar a linha de comando substitui esse comportamento.) Use um dos seguintes comandos:
   - Implantações do Citrix Virtual Apps and Desktops:
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Implantações do Citrix DaaS:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   Outras opções:
   - Use `/controllers` para especificar Delivery Controllers ou Cloud Connectors.

- Use `/enable_hdx_ports` para abrir portas no firewall, a menos que o firewall seja configurado manualmente.
- Use `/mastermcsimage` (ou `/masterimage`) se estiver instalando o VDA em uma imagem e for usar o MCS para criar VMs do servidor a partir dessa imagem.
- Para obter todos os detalhes da opção, consulte Instalar usando a linha de comando.

3. Crie um catálogo de máquinas para o Server VDI. No assistente de criação de catálogo:

   - Na página **Operating System**, selecione **Single-session OS**.
   - Na página **Summary**, especifique um nome ao catálogo de máquina e uma descrição para que administradores o identifiquem claramente como Server VDI. Este é o único indicador no Studio de que o catálogo suporta Server VDI.

   Ao usar a pesquisa no Studio, o catálogo Server VDI é exibido na guia **Single-session OS Machines**, mesmo que o VDA esteja instalado em uma máquina multissessão.

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 de usuário

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O recurso de camada de personalização do usuário do Citrix Virtual Apps and Desktops amplia os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e aplicativos instalados localmente em todas as sessões. Equipado com a tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e Machine Creation Services (MCS) em catálogos de máquinas não persistentes.

Você instala os componentes da camada de personalização do usuário juntamente com o Virtual Delivery Agent dentro da imagem mestre. Um arquivo VHD armazena localmente os aplicativos instalados pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

> **Importante:**
>
> Você pode implantar camadas de personalização de usuário no Citrix Virtual Apps and Desktops ou camadas de usuário do App Layering ativadas em um modelo de imagem, não as duas. Não instale o recurso da camada de personalização do usuário em uma camada dentro do App Layering.

Esse recurso substitui o Personal vDisk (PvD), além de fornecer uma experiência de espaço de trabalho persistente para usuários em um ambiente de área de trabalho não persistente (em pool).

Para implantar o recurso de camada de personalização do usuário, instale-o e configure-o usando as etapas detalhadas no artigo.

Suporte a aplicativos

Além das exceções a seguir, todos os aplicativos que um usuário instala localmente na área de trabalho são suportados na camada de personalização do usuário.

Exceções

Os seguintes aplicativos são a exceção e não são suportados na camada de personalização do usuário:

- Aplicativos empresariais, como MS Office e Visual Studio.
- Aplicativos que modificam a pilha de rede ou hardware. Exemplo: um cliente VPN.
- Aplicativos que possuem drivers de nível de inicialização. Exemplo: um verificador de vírus.
- Aplicativos com drivers que usam o repositório de drivers. Exemplo: um driver de impressora.

  > **Nota:**
  >
  > Você pode disponibilizar impressoras usando objetos de política de grupo (GPOs) do Windows.

Não permita que os usuários instalem aplicativos não suportados localmente. Em vez disso, instale os aplicativos diretamente na imagem mestre.

Aplicativos que exigem uma conta de usuário ou administrador local

Quando um usuário instala um aplicativo localmente, o aplicativo vai para a sua camada de usuário. Se o usuário adicionar ou editar um usuário ou grupo local, as alterações não persistirão além da sessão.

> **Importante:**
>
> Adicione os usuários ou grupos locais necessários na imagem mestre.

Requisitos

O recurso da camada de personalização do usuário requer os seguintes componentes:

- Citrix Virtual Apps and Desktops 7 1909 ou posterior
- Virtual Delivery Agent (VDA), versão 1912 ou posterior
- Citrix Provisioning, versão 1909 ou posterior
- Compartilhamento de arquivos do Windows (SMB) ou arquivos do Azure com autenticação do AD no local ativada

Você pode implantar o recurso de camada de personalização de usuário nas seguintes versões do Windows com sistema operacional implantado como uma única sessão. O suporte é limitado a um único usuário em uma única sessão.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versão 1607 ou posterior
- Windows 10 multissessão (arquivos do Azure suportados)
- Windows Server 2016 (arquivos do Azure suportados)
- Windows Server 2019 (arquivos do Azure suportados)

Para o Citrix Virtual Apps and Desktops 7, o uso de arquivos do Azure com camadas de personalização de usuário é suportado no Windows Server 2019, Windows Server 2016v e no cliente Windows 10.

> **Nota:**
>
> Se você estiver usando um SO de servidor, somente o Server VDI é aceito. Para obter detalhes de implantação, consulte o artigo Server VDI.
>
> A camada de personalização do usuário suporta apenas um usuário por vez por máquina, e a máquina precisa ser reinicializada para reiniciar os discos. Você não pode usar a camada de personalização do usuário com sistemas operacionais de servidor multissessão, apenas com sistemas de servidor de sessão única. A camada de personalização do usuário funciona apenas com áreas de trabalho não persistentes.

Desinstale o recurso da camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

Configurar o compartilhamento de arquivos

O recurso da camada de personalização do usuário requer o armazenamento SMB (Server Message Block) do Windows. Para criar um compartilhamento de arquivos do Windows, siga as etapas habituais para o sistema operacional Windows em que você está.

Para obter mais informações sobre como usar os Arquivos do Azure com catálogos baseados no Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

Recomendações, em Recommendations

Siga as recomendações nesta seção para uma implantação bem-sucedida da camada de personalização do usuário.

Microsoft System Center Configuration Manager (SCCM)

Se você estiver usando o SCCM com o recurso de camada de personalização do usuário, siga as instruções da Microsoft para preparar a imagem em um ambiente VDI. Consulte este artigo do Microsoft TechNet para obter mais informações.

Tamanho da camada do usuário

Uma camada de usuário é um disco thin provisionado que se expande à medida que o espaço em disco é utilizado. O tamanho padrão permitido para uma camada de usuário é 10 GB, o mínimo que recomendamos.

> **Nota:**
>
> Durante a instalação, se o valor for definido como zero (0), o tamanho da camada de usuário padrão será definido como 10 GB.

Se quiser alterar o tamanho da camada do usuário, insira um valor diferente na política **User Layer Size**. Consulte, na **Etapa 5: Criar políticas personalizadas de grupo de entrega**, **Opcional: clique em Select ao lado de User Layer Size in GB.**

Ferramentas para substituir o tamanho da camada de usuário (opcional)

Você pode substituir o tamanho da camada de usuário usando uma ferramenta Windows para definir uma cota no compartilhamento de arquivos da camada do usuário.

Use uma das seguintes ferramentas de cota da Microsoft para definir uma cota fixa no diretório da camada de usuário chamado **Users**:

- Gerenciador de Recursos do Servidor de Arquivos (FSRM)
- Gerente de cota

> **Nota:**
>
> Aumentar a cota afeta as novas camadas de usuário e expande as existentes. Diminuir a cota afeta apenas as novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

Implantar uma camada de personalização de usuário

Ao implantar o recurso de personalização do usuário, você define as políticas no Web Studio. Depois, você atribui as políticas ao grupo de entrega vinculado ao catálogo de máquinas, onde o recurso é implantado.

Se você deixar a imagem mestre sem configuração de camada de personalização de usuário, os serviços permanecem inativos e não interferem nas atividades de criação.

Se você definir as políticas na imagem mestre, os serviços tentam realizar a execução e montar uma camada de usuário dentro da imagem mestre. A imagem mestre poderá exibir comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, execute as seguintes etapas nesta ordem:

- Etapa 1: verifique a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Passo 2: prepare sua imagem mestre.
- Etapa 3: crie um catálogo de máquinas.
- Etapa 4: crie um grupo de entrega.
- Etapa 5: crie políticas personalizadas do grupo de entrega.

> **Nota:**
>
> Fazer logon pela primeira vez após atualizar o Windows 10 na imagem leva mais tempo do que o normal. A camada do usuário precisa ser atualizada para a nova versão do Windows 10, o que aumenta o tempo de login.

Etapa 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

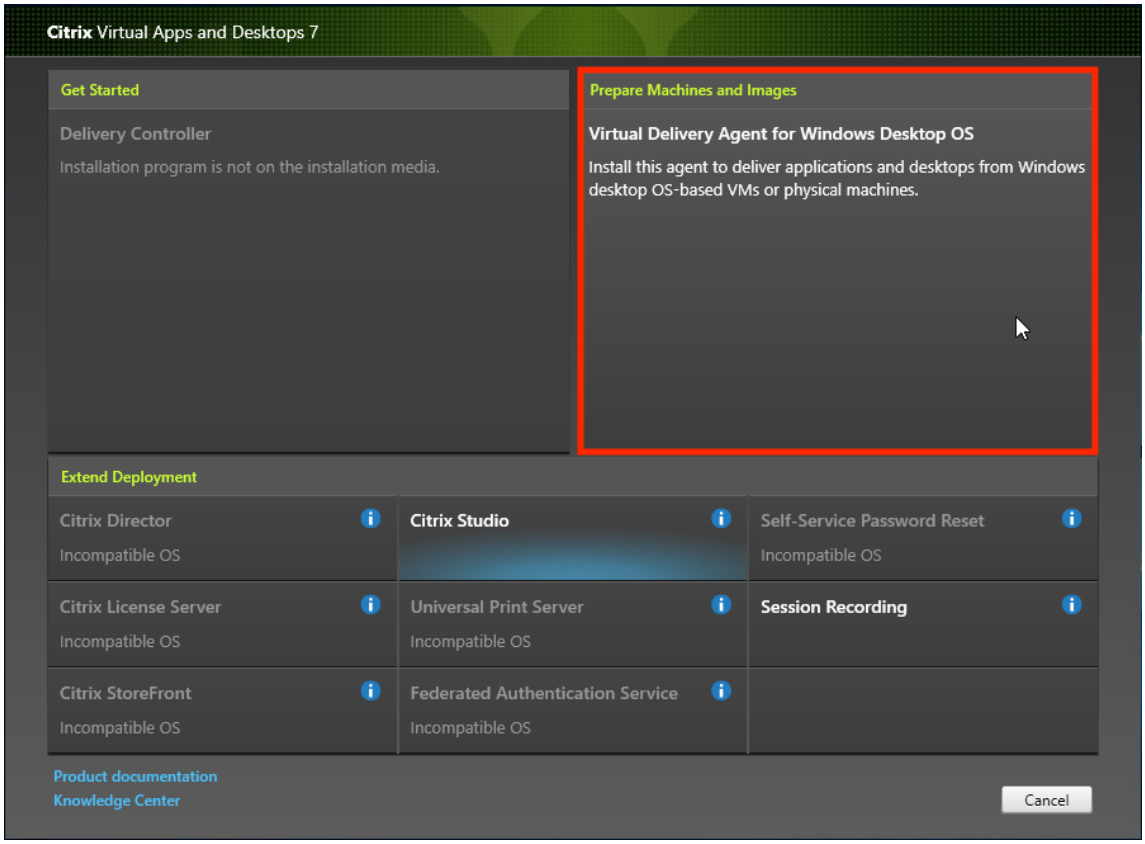
Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops está disponível para usar com o novo recurso. Para obter detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

Etapa 2: Prepare sua imagem mestre

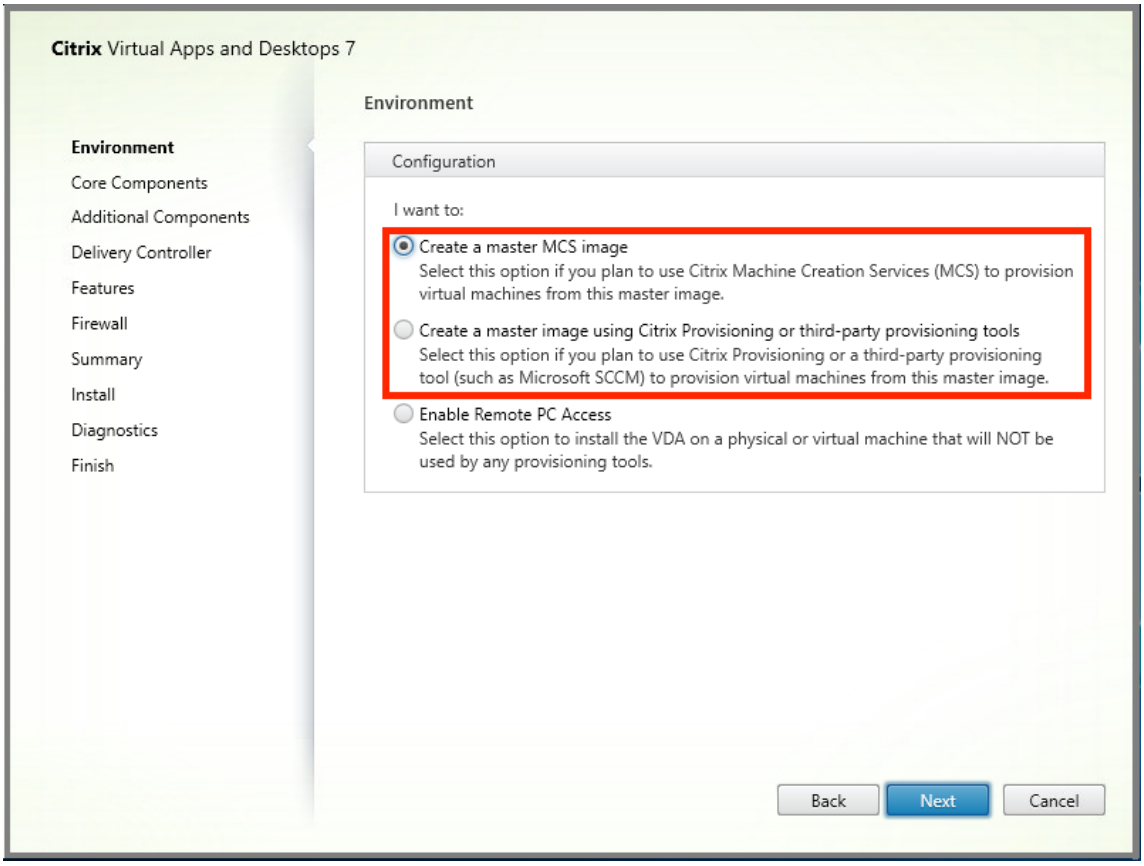
Para preparar a sua imagem mestre:

1. Localize a imagem mestre. Instale os aplicativos empresariais da sua organização e outros aplicativos que os usuários geralmente acham úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Lembre-se de incluir o componente opcional **User personalization layer**. Para obter detalhes, consulte as opções de linha de comando para instalar um VDA.
3. Se estiver usando o Windows 10, instale o Virtual Delivery Agent (VDA) 1912 ou posterior. Se uma versão mais antiga do VDA já estiver instalada, desinstale a versão antiga primeiro. Quando instalar a nova versão, certifique-se de selecionar e instalar o componente opcional **Citrix User Personalization Layer** como se segue:

    a) Clique no bloco **Virtual Delivery Agent for Windows Desktop OS**:

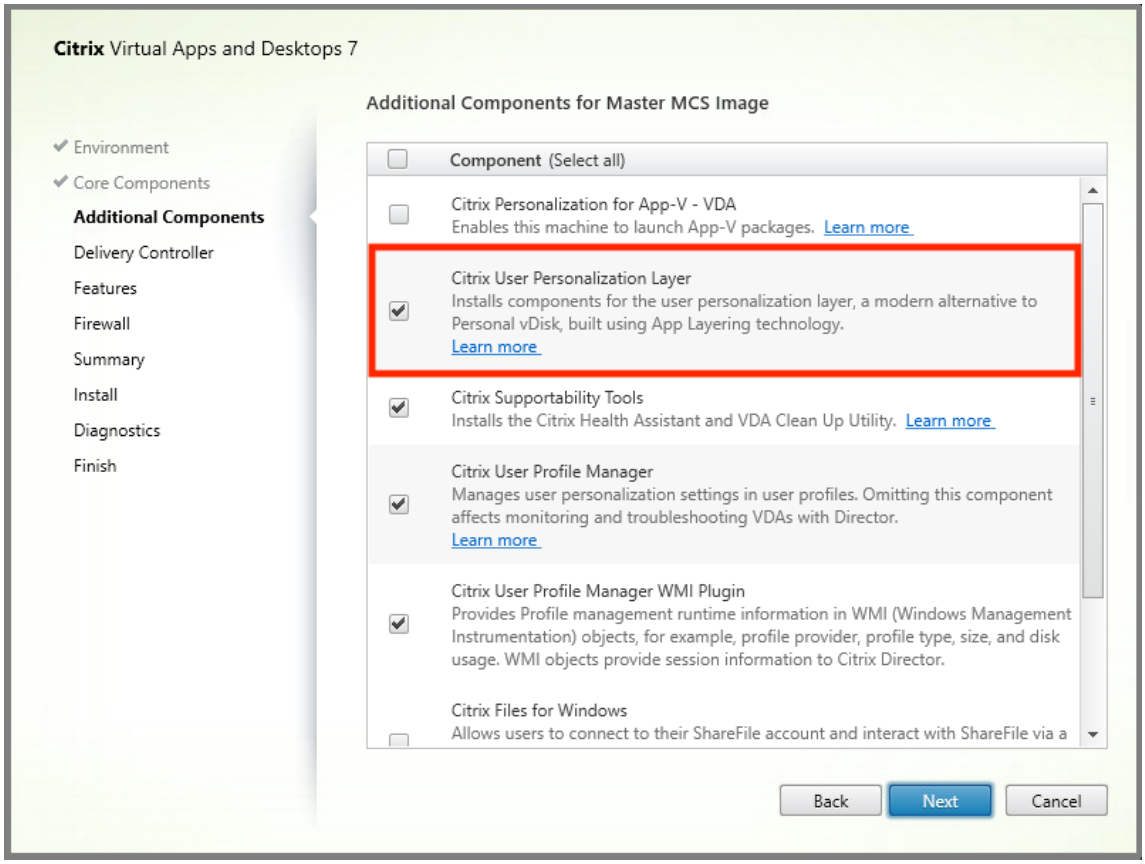


    a) **Environment:** selecione **Create a master MCS image** ou **Create a master image using Citrix Provisioning or third-party provisioning tools**.



a) **Core Components:** clique em **Next**.

b) **Additional Components:** selecione **Citrix User Personalization Layer**.



a) Clique nas telas de instalação restantes, configurando o VDA conforme necessário, e clique em **Install**. A imagem é reinicializada uma ou mais vezes durante a instalação.

4. Deixe **Windows updates** desativado. O instalador da camada de personalização do usuário desativa as atualizações do Windows na imagem. Deixe as atualizações desativadas.

A imagem está pronta para você carregar no Web Studio.

> **Nota:**
>
> Se deseja simplesmente atualizar a camada de personalização do usuário (UPL), você pode fazer isso com uma versão mais recente da UPL e o pacote autônomo. Você não precisa atualizar o VDA.

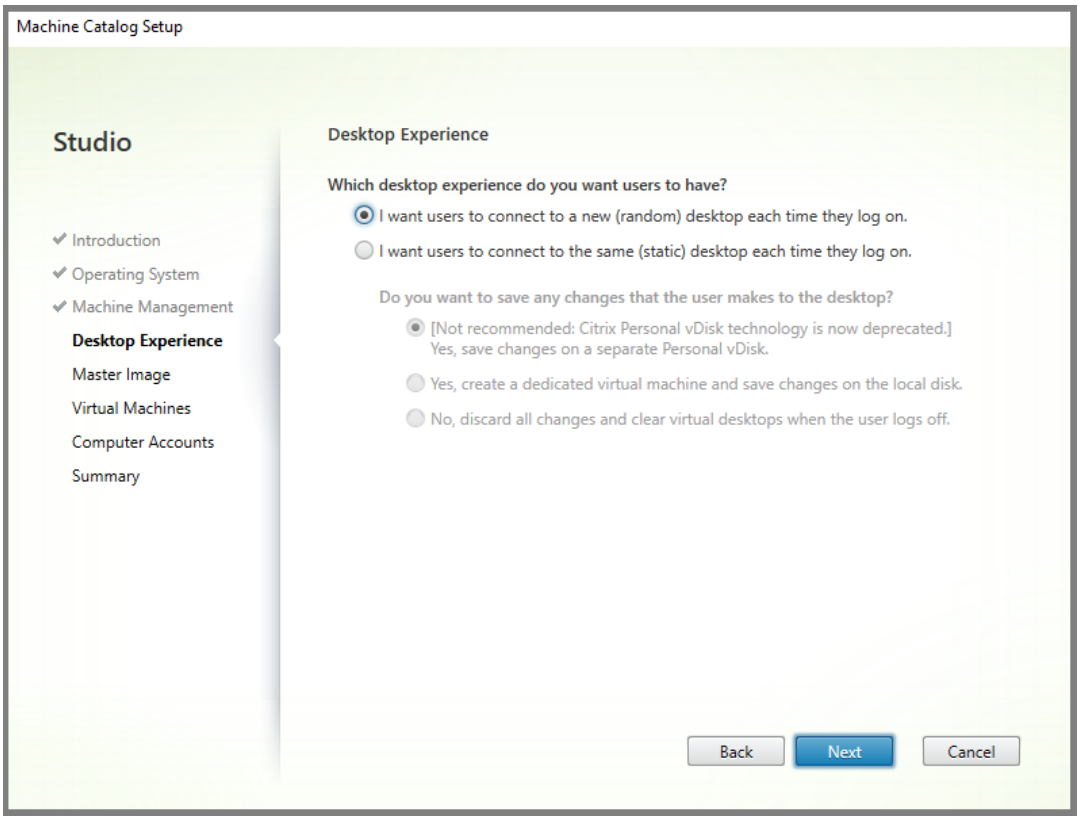
Etapa 3: Crie um catálogo de máquinas

No Web Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

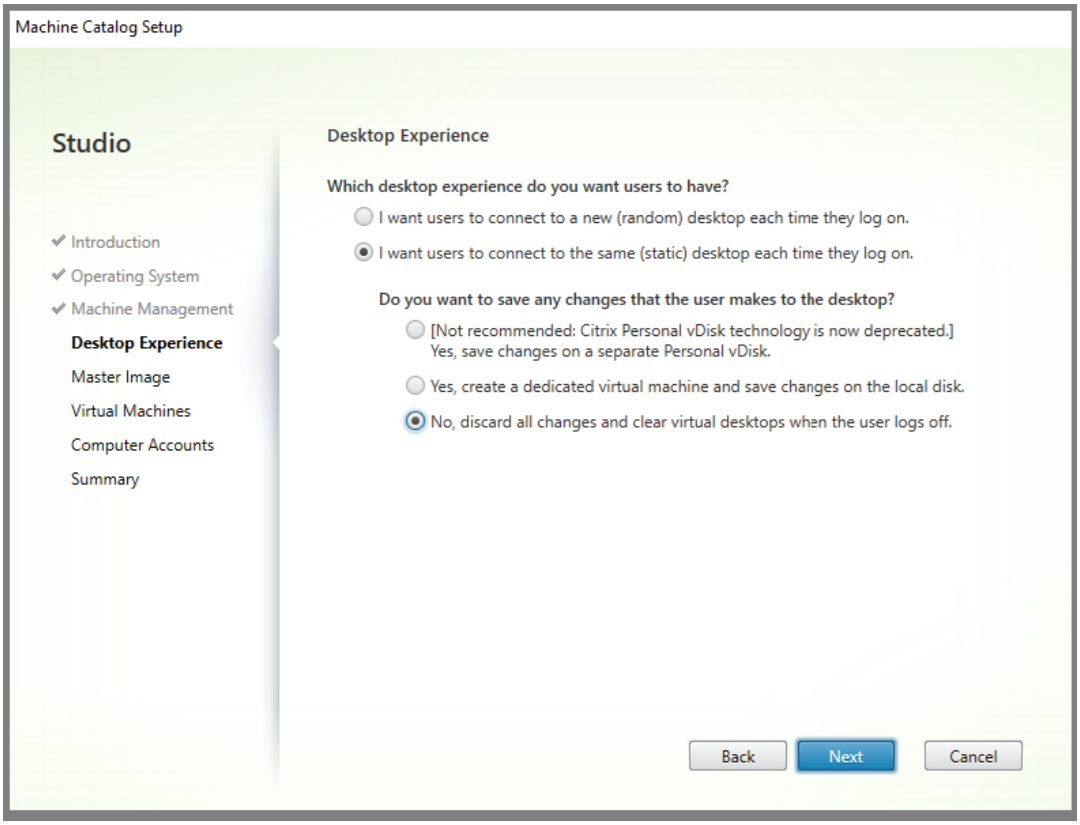
1. Selecione **Operating System** e defina como **Single-session OS**.
2. Selecione **Machine Management** e defina como **Machines that are power managed**. Por exemplo, máquinas virtuais ou PCs blade.

3. Selecione **Desktop Experience** e defina o tipo de catálogo como **pooled-random** ou **pooled-static**, conforme os exemplos a seguir:

   - **Pooled-random:**



   - **Pooled-static:** se você selecionar pooled-static, configure áreas de trabalho para descartar todas as alterações e limpar as áreas de trabalho virtuais quando o usuário fizer logoff, conforme mostra a captura de tela a seguir:



> **Nota:**
>
> A camada de personalização do usuário não oferece suporte a catálogos estáticos em pool configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se estiver usando o MCS, selecione **Master Image** e o instantâneo da imagem criada na seção anterior.
5. Configure as propriedades de catálogo restantes conforme necessário para o seu ambiente.

Etapa 4: Crie um grupo de entrega

Crie e configure um **grupo de entrega**, incluindo máquinas do catálogo de máquinas que você criou. Para obter detalhes, consulte Criar grupos de entrega.

Etapa 5: Crie políticas personalizadas do grupo de entrega

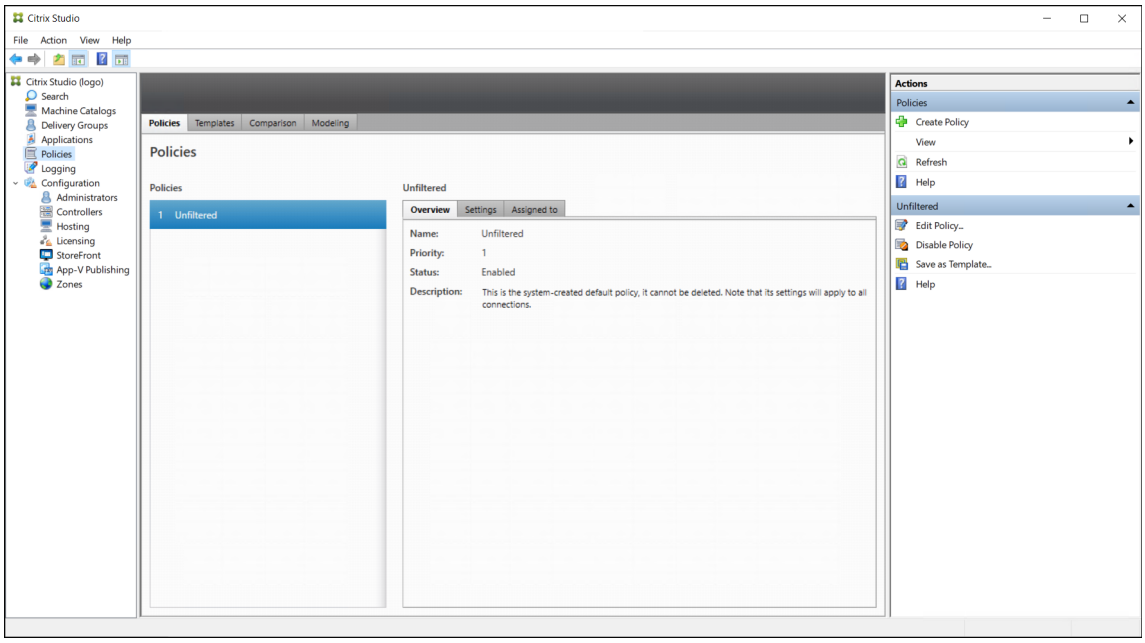
Para habilitar a montagem de camadas de usuário em Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Em que ponto da rede acessar as camadas do usuário.

- Quanto permitir que os discos da camada do usuário cresçam.

Para definir os parâmetros como políticas Citrix personalizadas no Web Studio e atribuí-las ao seu grupo de entrega.

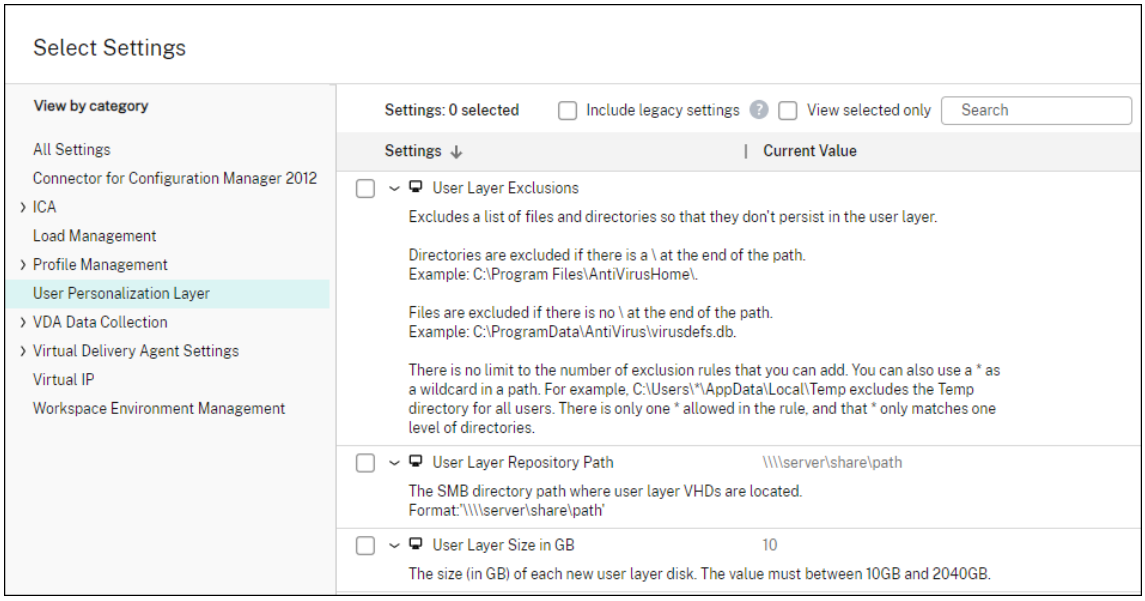
1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.



2. Selecione **Create Policy** na barra de ações. A janela Create Policy é exibida.
3. Digite 'user layer'no campo de pesquisa. As três políticas a seguir aparecem na lista de políticas disponíveis:

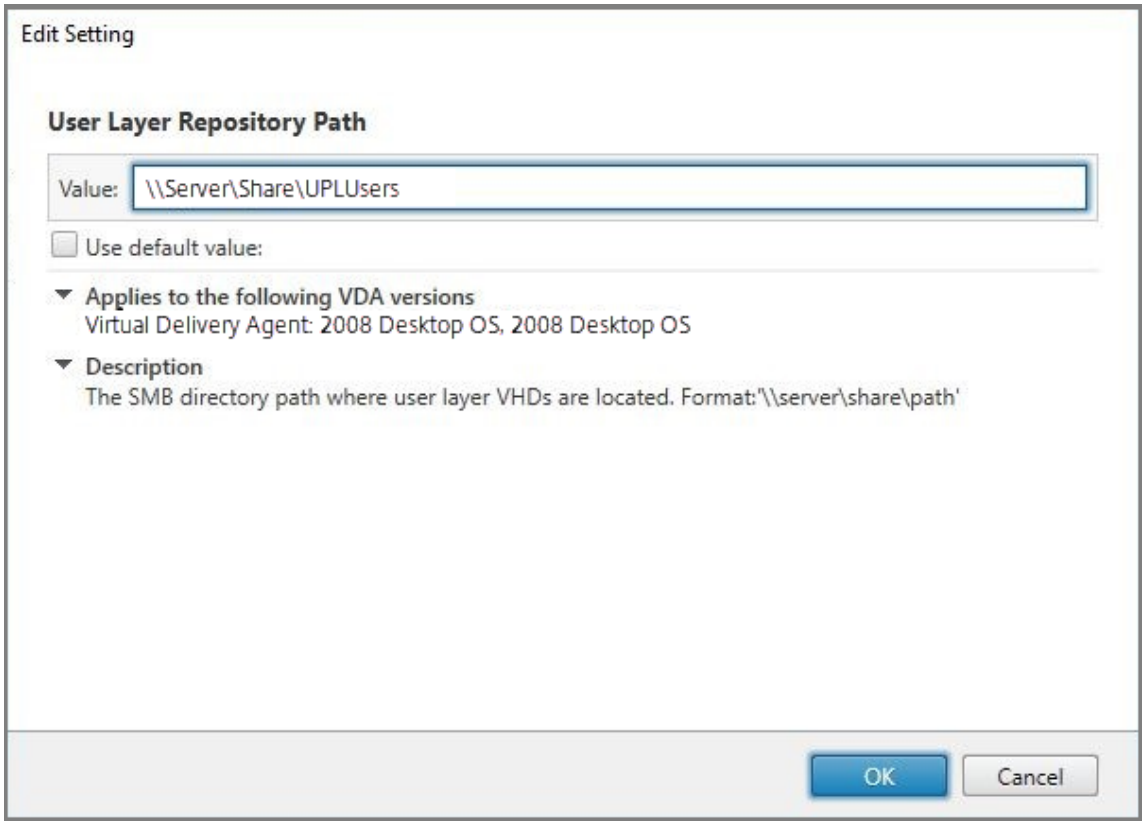
    - User Layer Exclusions
    - User Layer Repository Path
    - User Layer Size GB

    > **Nota:**
    >
    > Aumentar o tamanho afeta as novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas as novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.



4. Marque a caixa de seleção ao lado de **User Layer Repository Path** e clique em **Edit**. É exibida a janela Edit Setting.
5. Insira um caminho no campo **Value** e clique em **Save**:

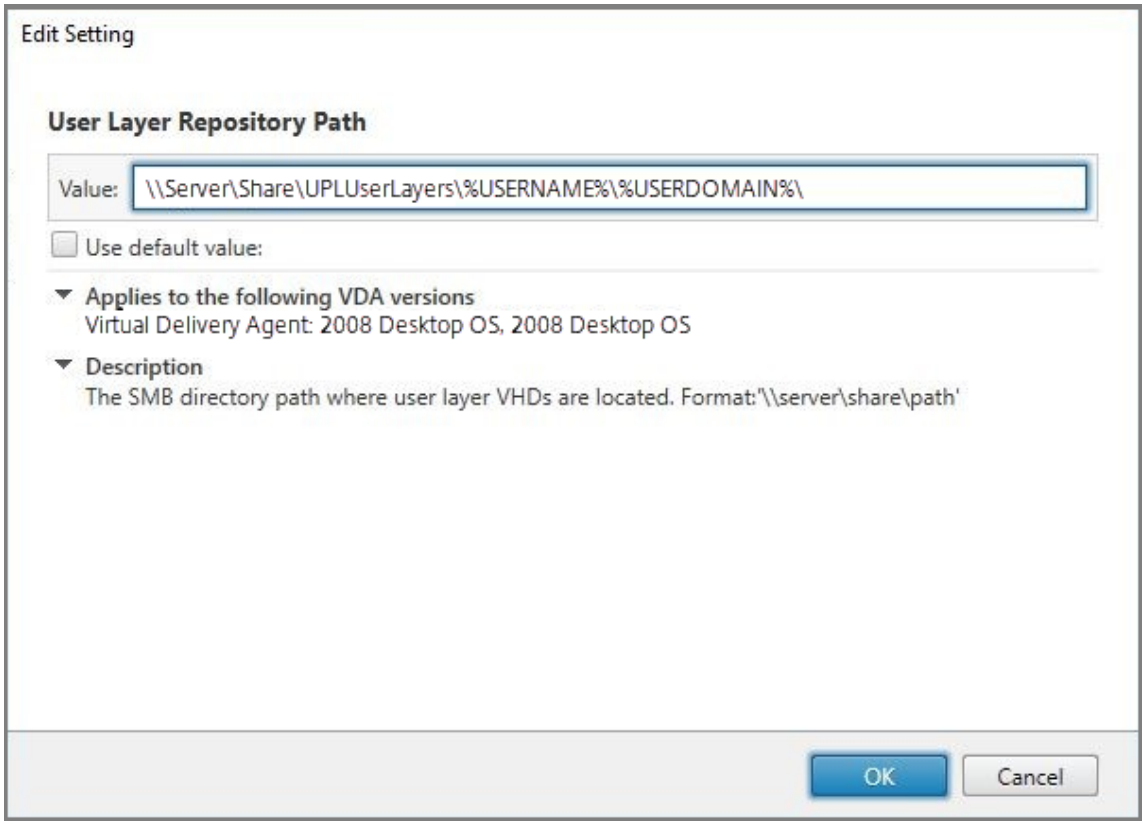
   - **Formato do caminho:** `\\server-name-or-address\share-name\folder`
   - **Exemplo de caminho:** `\\Server\Share\UPLUsers`
   - **Exemplo de caminhos resultantes:** para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



Você pode personalizar o caminho usando as variáveis %USERNAME% e %USERDOMAIN%, variáveis de ambiente da máquina e atributos do Active Directory (AD). Quando expandidas, essas variáveis resultam em caminhos explícitos.

Exemplo de variáveis de ambiente:

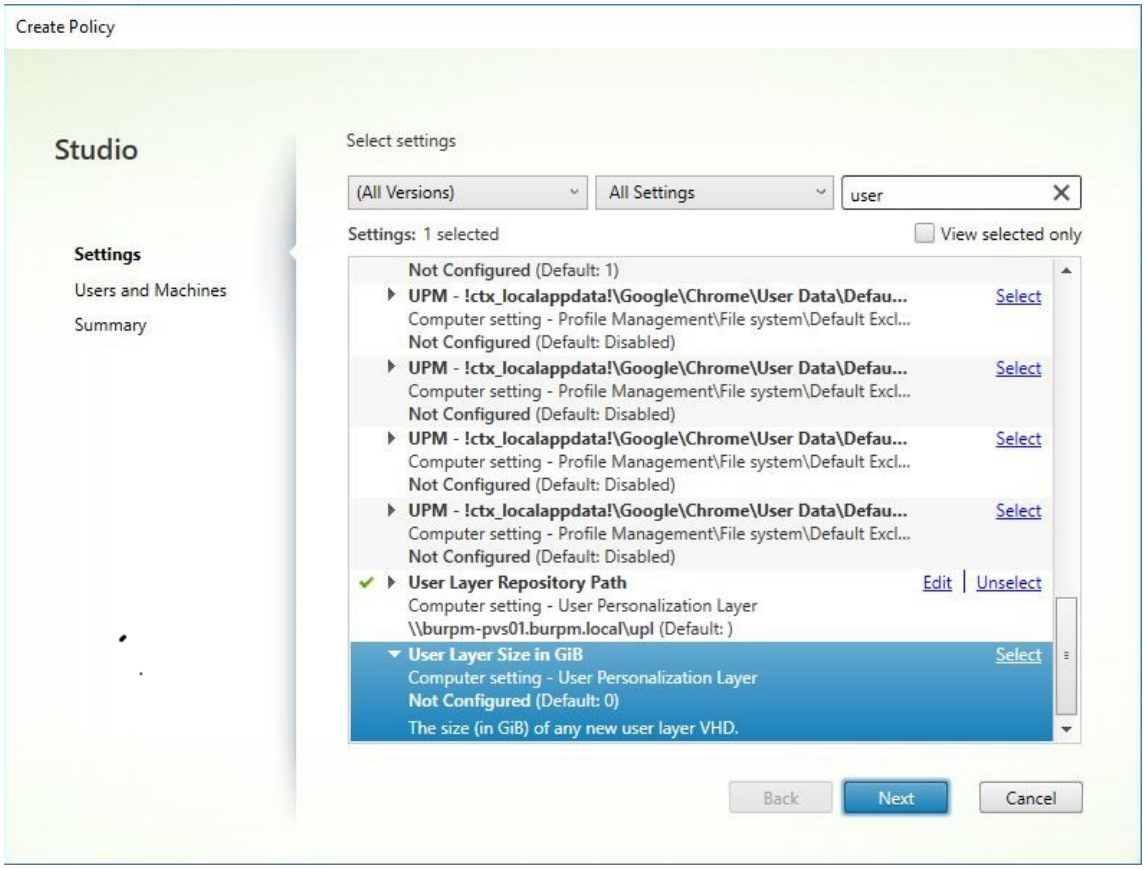
- **Formato do caminho:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Exemplo de caminho:** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Exemplo de caminhos resultantes:** para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



Exemplo de atributos personalizados do AD:

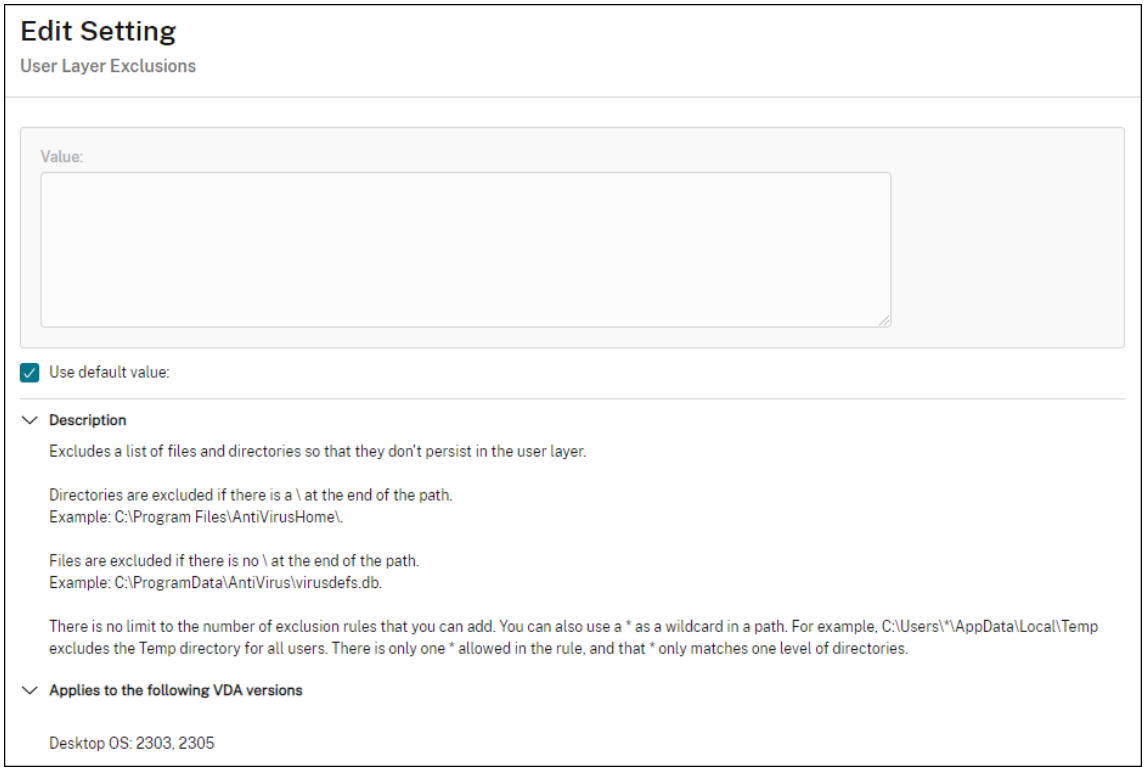
- Formato do caminho: `\\Server-name-or-address\share-name\AD-attribute`
- Exemplo de caminho: `\\Server\share\\#sAMAccountName#`
- Exemplo de caminhos resultantes: `\\Server\share\JohnSmith` (se #sAMAccount-Name # for resolvido para JohnSmith para o usuário atual)

6. Opcional: marque a caixa de seleção ao lado de **User Layer Size in GB** e clique em **Edit**:

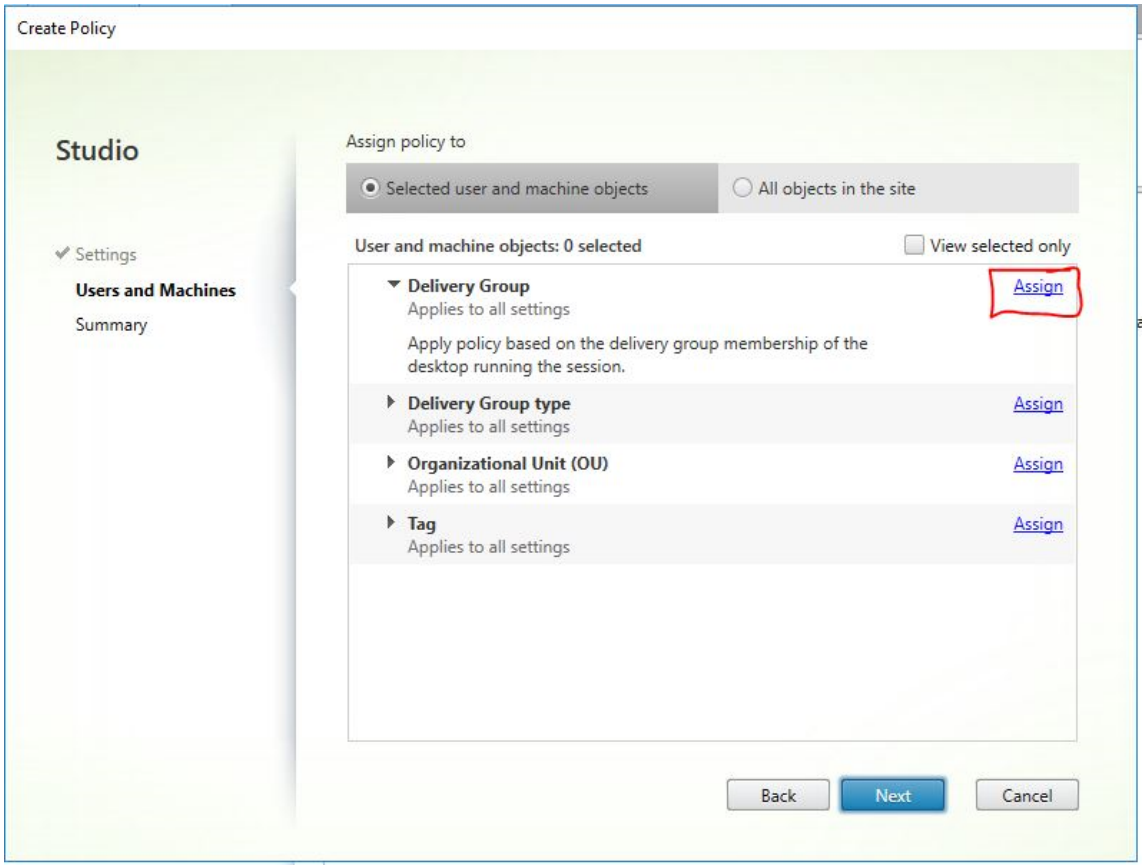


A janela Edit Settings é exibida.

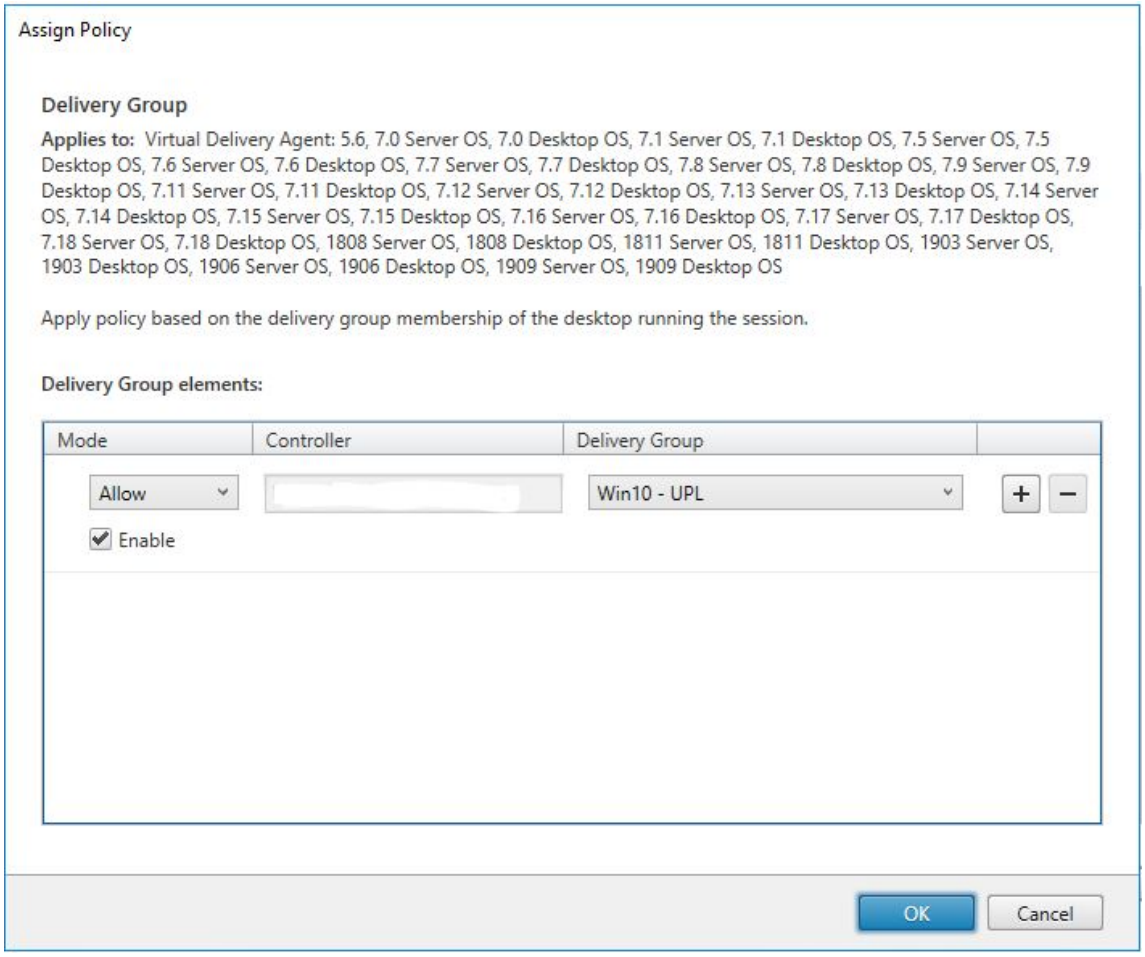
7. Opcional: altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode crescer. Clique em **Salvar**.
8. Opcional: marque a caixa de seleção ao lado de **User Layer Exclusions** e clique em **Edit**.



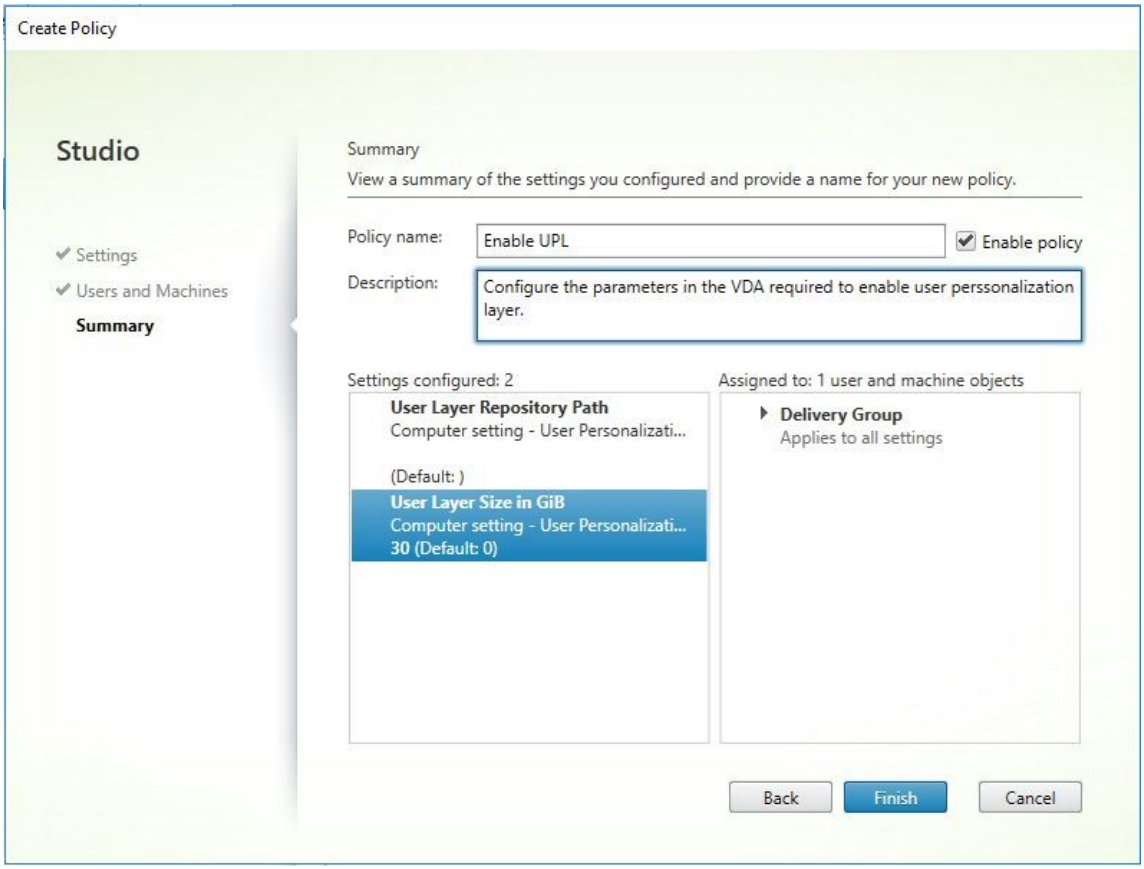
9. Opcional: especifique os arquivos e pastas a serem excluídos e clique em **Save**. Para obter mais informações, consulte a documentação do Citrix App Layering.
10. Clique em **Next** para configurar usuários e máquinas aos quais você deseja atribuir. Clique no link **Assign de Delivery Group**, em destaque nesta imagem:



11. No menu **Delivery Group**, selecione o grupo de entrega criado na seção anterior. Clique em **OK**.



12. Digite um nome para a política. Clique na caixa de seleção para ativar a política e clique em **Finish**.



Configurar parâmetros de segurança na pasta da camada de usuário

Como administrador de domínio, você pode especificar mais de um local de armazenamento para suas camadas de usuário. Crie uma subpasta `\Users` para cada local de armazenamento (incluindo o local padrão). Proteja cada local usando as seguintes configurações.

Nome do parâmetro	Valor	Aplica-se a
Creator Owner	Modify	Somente subpastas e arquivos
Owner Rights	Modify	Somente subpastas e arquivos
Users or group	Create Folder/Append Data; Traverse Folder/Execute File; List Folder/Read Data; Read Attributes	Somente pasta selecionada
System	Full Control	Pasta, subpastas e arquivos selecionados
Domain Admins, e Admin do grupo selecionado	Full Control	Pasta, subpastas e arquivos selecionados

Mensagens de camada de usuário

Quando um usuário não consegue acessar sua camada de usuário, ele recebe uma destas mensagens de notificação.

- **Camada de usuário em uso**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Camada do usuário indisponível**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **Sistema não redefinido após a saída do usuário**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

Arquivos de log para usar ao solucionar problemas

O arquivo de log ulayersvc.log contém a saída do software da camada de personalização do usuário onde as alterações são registradas.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

Limitações

Tenha em mente as seguintes limitações ao instalar e usar o recurso de camada de personalização do usuário.

- *Não* tente implantar o software de camada de personalização do usuário em uma camada dentro do App Layering. Implante camadas de personalização do usuário no Citrix Virtual Apps and Desktops ou ative camadas de usuário em um modelo de imagem no App Layering, não ambos. Qualquer um dos processos produz as camadas de usuário de que você precisa.
- *Não* configure o recurso de camada de personalização do usuário com catálogos de máquinas persistentes.
- *Não* use hosts de sessão.

- *Não* atualize o catálogo da máquinas com uma imagem executando uma nova instalação de sistema operacional (inclusive a mesma versão do Windows 10). A prática recomendada é aplicar atualizações ao sistema operacional dentro da mesma imagem mestre usada ao criar o catálogo de máquinas.
- *Não* use drivers de tempo de inicialização nem outros tipos de personalização de inicialização antecipada.
- *Não* migre dados PvD para o recurso de camada de personalização do usuário.
- *Não* migre camadas de usuário existentes do produto App Layering completo para o recurso de camada de personalização do usuário.
- *Não* altere o caminho SMB da camada de usuário para acessar camadas de usuário criadas usando uma imagem de sistema operacional mestre diferente.
- Quando um usuário faz logout de uma sessão e, em seguida, faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Centro de Software da Microsoft lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Não disponível** na segunda máquina.

  Para descobrir o verdadeiro status do aplicativo, instrua o usuário a selecionar o aplicativo no Centro de Software e clicar em **Instalar**. Em seguida, o SCCM atualiza o status para o valor verdadeiro.
- Ocasionalmente, o Centro de Software é interrompido imediatamente após iniciar em um VDA que tem o recurso de camada de personalização do usuário habilitado. Para evitar esse problema, siga as recomendações da Microsoft para Implementar o SCCM em um ambiente XenDesktop VDI. Além disso, certifique-se de que o serviço `ccmexec` está em execução antes de iniciar o Centro de Software.
- Nas Políticas de Grupo (Configurações do Computador), as configurações da camada do usuário substituem as configurações aplicadas à imagem mestre. Portanto, as alterações feitas às configurações do computador usando um GPO nem sempre estão apresentadas ao usuário no próximo login da sessão.

  Para contornar esse problema, crie um script de logon de usuário que emita o comando:

  ```
  gpupdate /force
  ```

  Por exemplo, um cliente define o seguinte comando para executar em cada login de usuário:

  ```
  gpudate /Target:Computer /force
  ```

  Para obter melhores resultados, aplique alterações às configurações do computador diretamente na camada do usuário, após o usuário ter feito login.
- Uma conta de usuário de domínio não deve ser o último usuário a ter feito login em uma imagem mestre. Caso contrário, as máquinas provisionadas a partir dessa imagem apresentarão

problemas.

- Os certificados personalizados não persistem quando o UPL está habilitado em um ambiente Azure AD puro, devido a um problema subjacente no Windows em execução no Azure. Se a Microsoft corrigir esse problema em um aprimoramento futuro, atualizaremos este artigo.

Remover componentes

June 28, 2023

Para remover componentes, a Citrix recomenda o uso do recurso Windows para remover ou alterar programas. Como alternativa, você pode remover componentes usando a linha de comando ou um script na mídia de instalação.

Quando você remove componentes, os pré-requisitos não são removidos e as configurações de firewall não são alteradas. Por exemplo, quando você remove 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. Não é possível 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 controlador.

Feche o Studio e o Director antes de removê-lo.

Remover componentes usando o recurso Windows para remover ou alterar programas

Usando o recurso Windows para remover ou alterar programas:

- Para remover um Controller, Studio, Director, License Server ou StoreFront, clique com o botão direito do mouse em **Citrix Virtual Apps *versão*** ou **Citrix Virtual Apps and Desktops *versão*** e selecione **Desinstalar**. O instalador é iniciado. Selecione os componentes a serem removidos.

  Como alternativa, você pode remover o StoreFront clicando com o botão direito do mouse 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 é iniciado e você pode selecionar os componentes a serem removidos. Por padrão, a máquina é reinicializada automaticamente após a remoção.
- Para remover o Servidor de Impressão Universal, clique com o botão direito em **Citrix Universal Print Server** e selecione **Desinstalar**.

Remover componentes principais usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopServerSetup.exe`.

- Para remover um ou mais componentes, especifique as opções `/remove` e `/components`.
- Para remover todos os componentes, especifique a opção `/removeall`.

Para obter detalhes de comando e parâmetro, consulte Instalar usando a linha de comando.

Por exemplo, o comando a seguir remove o Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

Remover VDAs usando a linha de comando

No diretório `\x64\XenDesktop Setup`, execute o comando `XenDesktopVdaSetup.exe`.

- Para remover um ou mais componentes, use as opções `/remove` e `/components`. Por exemplo, para remover o VDA e o aplicativo Citrix Workspace, use `/remove /components vda,plugin`.
- A opção `/removeall` remove apenas o VDA. Ela não remove o aplicativo Citrix Workspace.

Para obter detalhes de comando e parâmetro, consulte Instalar usando a linha de comando.

Por padrão, a máquina é reinicializada automaticamente após a remoção.

Para remover VDAs usando um script no Active Directory, consulte Instalar ou remover VDAs usando scripts.

Atualizar e migrar

June 28, 2023

Introdução

A atualização altera sua implantação da versão atual, Current Release (CR), do Citrix Virtual Apps and Desktops 7 sem precisar configurar novas máquinas ou sites. O processo é conhecido como uma atualização no local.

A atualização lhe dá acesso aos recursos e tecnologias mais recentes aos quais você tem direito de uso. As atualizações também podem conter correções, esclarecimentos e aprimoramentos de versões anteriores.

Visão geral da atualização

1. Leia o artigo Atualizar uma implantação antes de iniciar a atualização. Esta é a principal fonte de informações para aprender como fazer a preparação e implantação de uma atualização.
2. Certifique-se de que suas datas atuais do Customer Success Services estejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo Licenças de renovação de Customer Success Services.
3. Siga as instruções de preparação.
4. Execute os instaladores para atualizar os componentes principais.
5. Atualize os bancos de dados do sistema e o site.
6. Atualize os VDAs nas imagens (ou diretamente nas máquinas).
7. Atualize os 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 e XenDesktop 7.15 LTSR CU5 a CU8
- Virtual Apps and Desktops 1912 com ou sem CUs, até CU5, inclusive
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

O Citrix Upgrade Guide lista as versões do Citrix Virtual Apps and Desktops (e XenApp e XenDesktop) que você pode atualizar.

Perguntas frequentes

Esta seção responde a algumas perguntas frequentes sobre como atualizar o Citrix Virtual Apps and Desktops.

- **Qual é a ordem correta para atualizar meu ambiente Virtual Apps and Desktops?**

  Para obter uma ilustração e descrição da sequência de atualização recomendada, consulte Sequência de atualização e Procedimento de atualização.

- **Meu site tem vários Delivery Controllers (em diferentes zonas). 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 prática recomendada é atualizar todos os Delivery Controllers durante a mesma janela de manutenção, pois vários serviços em cada Controller se comunicam entre si. Manter versões diferentes pode causar problemas. Durante uma janela de manutenção, recomendamos que você atualize metade dos Controllers, atualize o site e, em seguida, atualize os Controllers restantes. (Para obter detalhes, consulte o Procedimento de atualização.)

- **Posso ir diretamente para a versão mais recente ou preciso fazer atualizações incrementais?**

  Você pode quase sempre atualizar para a versão mais recente e pular versões intermediárias, a menos que explicitamente indicado na seção de **Novidades** da versão para a qual você está atualizando. Consulte o Guia de atualização.

- **O cliente pode atualizar de um ambiente LTSR (Long Term Service Release) para uma versão CR (Current Release)?**

  Sim. Os clientes não são obrigados a permanecer em uma versão LTSR por um período prolongado. Os clientes podem mover um ambiente LTSR para uma versão CR com base em 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, pode ser que nem todos os recursos da versão mais recente estejam disponíveis. Para obter mais informações, consulte Considerações sobre ambientes mistos.

- **Com que frequência uma versão CR deve ser atualizada?**

  As versões Current Release (CR) chegam ao Fim da Manutenção (EOM) 6 meses após a data de lançamento da versão. A Citrix recomenda que os clientes adotem a versão atual CR mais recente. As versões Current Release (CR) chegam ao Fim da Vida Útil (EOL) 18 meses após a data de lançamento da versão. Para obter mais informações, consulte o Ciclo de vida da versão atual.

- **O que é recomendado: atualizar para LTSR ou CR?**

  As versões atuais (CRs) oferecem os recursos e funcionalidades mais recentes e inovadores de virtualização de aplicativos, áreas de trabalho e servidores. Isso permite que você continue

usando a tecnologia de ponta e à frente da concorrência.

As versões de serviço de longo prazo (LTSRs) são ideais para os ambientes de produção das grandes empresas, que preferem manter a mesma versão base por um período prolongado.

Para obter detalhes, consulte Opções de manutenção.

- **Preciso atualizar minhas licenças?**

  Certifique-se de que a data da licença atual não tenha expirado e seja válida para a versão para a qual você está atualizando. Consulte CTX111618. Para obter informações sobre renovação, consulte Licenças de renovação de Customer Success Services.

- **Quanto tempo demora uma atualização?**

  O tempo necessário para atualizar uma implantação varia, dependendo da infraestrutura e da rede. Portanto, não podemos precisar o tempo exato.

- **Quais são as melhores práticas?**

  Certifique-se de entender e seguir as instruções de preparação.

- **Quais sistemas operacionais são suportados?**

  A seção de requisitos do sistema da versão para a qual você está atualizando lista os sistemas operacionais compatíveis.

  Se a sua implantação atual usa sistemas operacionais que não são mais compatíveis, consulte Sistemas operacionais anteriores.

- **Quais versões do VMware vSphere (vCenter + ESXi) são suportadas?**

  CTX131239 lista os hosts e versões compatíveis, além de links para problemas conhecidos.

- **Quando minha versão atinge o fim da vida útil (EOL)?**

  Verifique em Product Matrix.

- **Quais são os problemas conhecidos com a versão mais recente?**

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix License Server
  - Aplicativo Citrix Workspace para Windows

Mais informações

As atualizações de implantação de Long Term Service Release (LTSR) usam atualizações cumulativas (CU). A Atualização Cumulativa (CU) atualiza os componentes da linha de base da LTSR, e cada atualização cumulativa inclui seu próprio metainstalador.

Todas as CUs têm uma documentação própria. Por exemplo, para a versão 7.15 LTSR, verifique o link na página **Novidades** daquela LTSR para saber qual a última CU. As páginas CU incluem informações sobre as versões suportadas, instruções e um link para o pacote de download da CU.

Migrar

Migrar para a nuvem

Você pode usar a ferramenta Automated Configuration do 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 mais antigo e a subsequente importação dos dados para o novo site.

Não há ferramentas ou scripts compatíveis para migrar versões do XenApp e XenDesktop ou para migrar versões anteriores do Citrix Virtual Apps and Desktops. A *atualização* é suportada pelas versões do Citrix Virtual Apps and Desktops listadas no Citrix Upgrade Guide e descritas nesta documentação do produto.

Para obter o conteúdo de migração do XenApp 6.x anterior, consulte o seguinte. Nem scripts, nem artigos são mantidos ou têm suporte.

- Scripts de migração de código aberto para versões XenApp 6.x estão disponíveis em https://github.com/citrix/xa65migrationtool. A Citrix não oferece suporte nem mantém esses scripts de migração.
- Alterações em 7.x
- Atualizar uma estação de trabalho XenApp 6.5 com um novo VDA
- Migrar XenApp 6.x

Atualizar uma implantação

January 3, 2024

Introdução

Você pode atualizar determinadas implantações para versões mais recentes sem precisar primeiro configurar novas máquinas, computadores ou sites. Isso é chamado de atualização no local ou atualização in-loco. Para saber quais versões do Citrix Virtual Apps and Desktops você pode atualizar, consulte o Citrix Upgrade Guide.

Antes de atualizar para qualquer uma das versões do Citrix Virtual Apps and Desktops, certifique-se de que as datas atuais do Customer Success Services estejam válidas e não tenham expirado. Para obter mais informações, consulte o artigo Licenças de renovação de Customer Success Services.

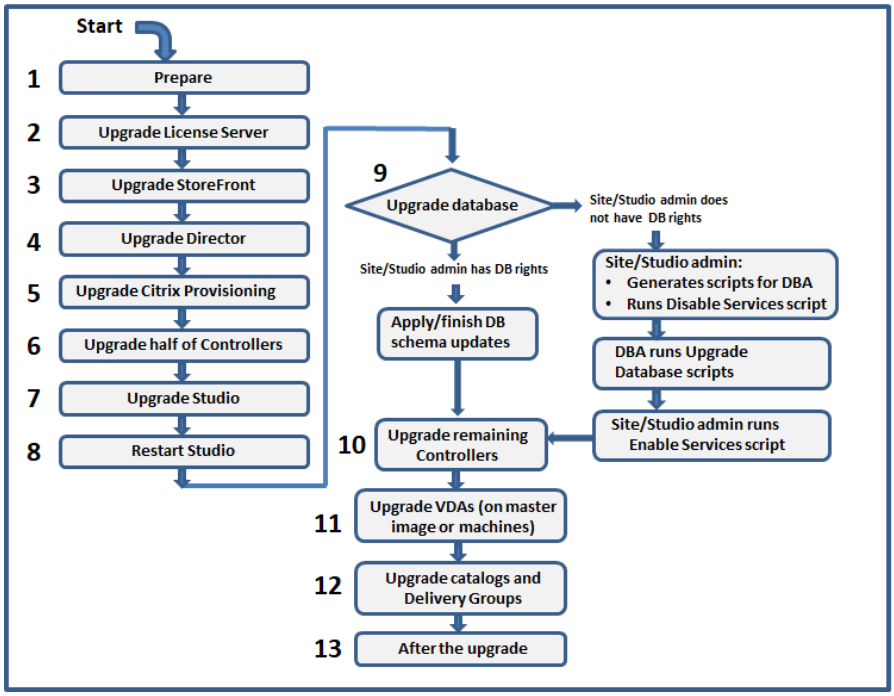
Para iniciar uma atualização, execute o instalador da nova versão para atualizar os componentes principais instalados anteriormente, VDAs e alguns outros componentes. Em seguida, atualize os bancos de dados e o site.

Você pode atualizar qualquer componente que possa ser instalado com o instalador de produto completo (e os instaladores de VDA autônomos), se houver uma versão mais recente fornecida. Para outros componentes que não são instalados com o instalador de produto completo (como Citrix Provisioning e Profile Management), consulte a documentação do componente para obter orientação. Para atualizações de host, consulte a documentação apropriada.

Leia todas as informações contidas neste artigo antes de iniciar uma atualização.

Sequência de atualização

O diagrama a seguir mostra as etapas da sequência de atualização. O procedimento de atualização contém detalhes de cada etapa no diagrama.



> **Nota:**
>
> Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer tarefa relacionada a provisionamento e grupo de entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

Licenças Hybrid Rights

As licenças Hybrid Rights são licenças de assinatura baseadas em prazo que são fornecidas além da assinatura do serviço em nuvem quando um cliente faz a transição ou troca de uma licença perpétua para uma assinatura de serviço em nuvem. Você também pode comprar um complemento Hybrid Rights com suas assinaturas DaaS.

Se você tiver uma licença Hybrid Rights com um atributo SaaS, ao fazer o upgrade para o Citrix Virtual Apps and Desktops LTSR 2203 e versões posteriores, você se torna elegível para acessar recursos não disponíveis com o Citrix Virtual Apps and Desktops LTSR 1912. Esses recursos incluem provisionamento e hospedagem de cargas de trabalho em nuvens públicas, como Microsoft Azure, AWS EC2 e Google Cloud. Antes de implantar o novo arquivo de licença, atualize o seu License Server para a versão mais recente.

Se você tiver acesso a uma licença Hybrid Rights sem atributo SaaS, siga estas etapas para obter acesso à nova licença Hybrid Rights com o atributo SaaS:

> **Nota:**
>
> - Você recebe um e-mail com um novo código de licença. Para obter mais informações, consulte Usar código de acesso de licença.
> - Suas licenças existentes são rescindidas. As licenças rescindidas devem ser excluídas dos License Servers seguidas pela instalação de novas licenças. Para obter mais informações, consulte Excluir arquivos de licença.

1. Acesse o portal de gerenciamento de licenças do citrix.com e baixe o novo arquivo de licença Hybrid Rights com os direitos de provisionamento de nuvem ativados (atributo SaaS). Para obter mais informações, consulte Baixar licenças. A imagem a seguir mostra o arquivo de licença Hybrid Rights com o atributo SaaS na seção Increments.

2. Instale o arquivo de licença Hybrid Rights no 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 broker para definir a edição e o modelo e, em seguida, inicie a atualização in-loco. Para obter mais informações sobre os comandos do Broker, consulte a seção Broker PowerShell SDK.

Para obter mais informações sobre o suporte à nuvem pública com versões atuais e Long Term Service Releases do Citrix Virtual Apps and Desktops, consulte CTX270373.

Procedimento de atualização

A maioria dos componentes principais do produto pode ser atualizada executando o instalador do produto no computador que contém o componente.

Se um computador contiver mais de um componente (por exemplo, Studio e License Server), todos os componentes do computador são atualizados, se a mídia do produto contiver versões mais recentes do software.

Para usar os instaladores:

- Para executar a interface gráfica do instalador do produto completo, faça logon no computador 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, execute o comando apropriado. Consulte Instalar usando a linha de comando.

Etapa 1: Preparar

Antes de iniciar uma atualização, prepare-se adequadamente. Leia, entenda e conclua todas as tarefas necessárias:

- Remover PVD, AppDisks e hosts não suportados
- VDAs que possuem componentes PvD ou AppDisks
- Limitações
- Considerações sobre ambientes mistos
- Sistemas operacionais anteriores
- Preparação
- Testes preliminares do site
- Verificação da versão do SQL Server

Etapa 2: Atualizar o servidor de licenças

Se a instalação tiver uma nova versão do software Citrix License Server, atualize esse componente antes de quaisquer outros componentes.

Se você ainda não determinou se o License Server é compatível com a nova versão, é essencial que você execute o instalador no Servidor de Licenças antes de atualizar quaisquer outros componentes principais.

Etapa 3: Atualizar o StoreFront

Se a mídia de instalação contiver uma nova versão do software StoreFront, execute o instalador no computador que contém o servidor StoreFront.

- Na interface gráfica, escolha **Citrix StoreFront** na seção **Extend deployment**.
- Na linha de comando, execute `CitrixStoreFront-x64.exe`, que está disponível na pasta `x64` da mídia de instalação do Citrix Virtual Apps and Desktops.

Etapa 4: Atualizar o Director

Se a mídia de instalação contiver uma nova versão do software Director, execute o instalador no computador 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 do Citrix Provisioning

e o software de 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 ocorrer de o site apresentar 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 da atualização do banco de dados. Os Controllers atualizados não podem processar solicitações até que o site inteiro seja atualizado.

Se o seu site tiver apenas um Controller, ele estará inoperante durante a atualização.

Os testes preliminares do site são executados no primeiro Controller, antes que a atualização seja realmente iniciada. Para obter detalhes, consulte Testes preliminares do site.

Etapa 7: Atualizar o Studio

Se você ainda não atualizou o Studio (porque estava no mesmo computador que outro componente), execute o instalador no computador que contém o Studio.

> **Nota:**
>
> Depois de atualizar o Web Studio, nem sempre as informações da versão são atualizadas imediatamente. Você pode ser solicitado a atualizar o Web Studio mesmo que ele já esteja atualizado. Para resolver o problema, acesse o servidor Web Studio, abra Internet Information Services (IIS) Manager, navegue até Start Page > Sites > Default Web Site e selecione **Restart** no painel Manage Website.

Etapa 8: Reiniciar o Studio

Reinicie o Studio atualizado. O processo de atualização é retomado automaticamente.

Etapa 9: Atualizar o banco de dados e o site

> **Nota:**
>
> Para evitar falhas, você deve atualizar todos os Delivery Controllers e o banco de dados antes de executar qualquer tarefa relacionada a provisionamento e grupo de entrega, como criar um novo catálogo de máquinas, excluir um catálogo de máquinas, atualizar uma máquina em um grupo de entrega e assim por diante.

Em Preparação, veja quais são as permissões necessárias para atualizar o esquema de bancos de dados do SQL Server.

- Se você tiver permissão suficiente para atualizar o esquema de banco de dados do SQL Server, poderá iniciar a 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 use scripts e prosseguir com a ajuda do administrador do seu banco de dados (alguém que tenha as permissões necessárias). Para a atualização manual, o usuário do Studio gera os scripts e depois executa os scripts que habilitam e desabilitam 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 de várias zonas e quiser atualizar o banco de dados e o site automaticamente, a Citrix recomenda que a atualização dbschema seja realizada na mesma zona que hospeda os bancos de dados do SQL Server do site. Caso contrário, atualizar o banco de dados e o site automaticamente poderá falhar.

A Citrix recomenda que você faça backup do banco de dados antes de fazer a atualização. Consulte CTX135207. Durante uma atualização de banco de dados, os serviços do produto são desativados. Durante esse tempo, os Controllers não podem intermediar novas conexões para o site, portanto planeje com atenção.

Atualizar o banco de dados e o site automaticamente

1. Inicie o Studio recém-atualizado.
2. Indique que você deseja iniciar a atualização do site automaticamente e confirme que está pronto.

A atualização do banco de dados e do site prossegue.

Atualizar o banco de dados e o site manualmente

1. Inicie o Studio recém-atualizado.
2. Indique que você deseja atualizar o site manualmente. O assistente verifica a compatibilidade do License Server e solicita a confirmação.
3. Confirme que você fez backup do banco de dados.

   O assistente gera e exibe os scripts e uma lista de verificação das etapas de atualização. Se o esquema de um banco de dados não tiver sido alterado desde a versão do produto que está sendo atualizada, o script não é gerado. Por exemplo, se o esquema do banco de dados de log não for alterado, o script `UpgradeLoggingDatabase.sql` não é gerado.

4. Execute os seguintes scripts na ordem mostrada.

    - `DisableServices.ps1`: o usuário do Studio executa este script do 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 de monitoramento.
    - `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 mudar (por exemplo, depois de aplicar um hotfix).
    - `EnableServices.ps1`: o usuário do Studio executa este script do PowerShell em um Controller para habilitar os serviços do produto.

    Depois que a atualização do banco de dados for concluída e os serviços de produtos habilitados, o Studio testa automaticamente o ambiente e a configuração e, em seguida, gera um relatório HTML. Se forem identificados problemas, você poderá restaurar o backup do banco de dados. Depois de resolver os problemas, você pode atualizar o banco de dados novamente.

5. Depois de concluir as tarefas da lista de verificação, clique em **Finish upgrade**.

Etapa 10: Atualizar os Delivery Controllers restantes

No Studio recém-atualizado, selecione **Citrix Studio** *nome-do-site* no painel de navegação. Na guia **Common Tasks**, selecione **Upgrade remaining Delivery Controllers**.

> **Nota:**
>
> Para disponibilizar a opção **Upgrade dos Controladores de Entrega restantes**, crie pelo menos um catálogo de máquinas e um grupo de entrega para o site.

Depois de concluir a atualização e confirmar a conclusão, feche e abra o Studio novamente. O Studio pode solicitar uma atualização adicional do site para registrar os serviços do Controller no site ou para criar um ID de zona se ainda não existir.

Etapa 11: Atualizar VDAs

> **Importante:**
>
> Se você estiver atualizando um VDA para a versão 1912 ou posterior, consulte Atualizar VDAs para 1912 ou posterior.

Execute o instalador do produto em computadores contendo VDAs.

Se você usou Machine Creation Services e uma imagem mestre para criar máquinas, acesse o seu host e atualize o VDA na imagem mestre. Você pode usar qualquer um dos instaladores de VDA disponíveis.

- Para obter orientação sobre interface gráfica, consulte Instalar VDAs.
- Para obter orientação sobre 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 orientações sobre a atualização.

Etapa 12: Atualizar catálogos de máquinas e Grupos de Entrega

- Atualizar catálogos que usam máquinas com VDAs atualizados.
- Fazer upgrade de catálogos que usam máquinas com VDAs atualizados.
- Fazer upgrade de Grupos de Entrega que usam máquinas com VDAs atualizados.

Etapa 13: Após a atualização

Depois de concluir uma atualização, você pode testar o site recém-atualizado. No Studio, selecione **Citrix Studio nome-do-site** no painel de navegação. Na guia **Common Tasks**, selecione **Test Site**. Esses testes são executados automaticamente depois de atualizar o 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 SQL Server Browser Service não for iniciado. Para evitar isso:

- Habilite o SQL Server Browser Service (se necessário) e inicie-o.
- Reinicie o serviço SQL Server (SQLEXPRESS).

Atualize outros componentes na sua implantação. Para obter orientações, 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 Dbschema

Quando você atualiza sua implantação, vários esquemas de bancos de dados podem ser atualizados. A tabela a seguir lista quais esquemas de bancos de dados são atualizados no processo:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

Definição de termos:

- Site: Site Datastore. A atualização do Dbschema é feita no Site Datastore.
- Monitor: Monitor Datastore. A atualização do Dbschema é feita no Monitor Datastore.
- Config: tabela Configuration. Versão do Desktop Studio, informações do Licensing ou ambos são atualizados na tabela Configuration.
- Logging: Logging Datastore. A atualização do Dbschema é feita no Logging Datastore.

Atualizar VDAs para 2203 ou posterior

Se o componente Personal vDisk (PvD) já tiver sido 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 instalar o novo VDA.

Essa instrução se aplica mesmo que você nunca tenha usado o PvD.

Veja como o componente PvD pode ter sido instalado em versões anteriores:

- Na interface gráfica do instalador do VDA, o PvD era uma opção na página **Additional Components**. O 7.15 LTSR e versões 7.x anteriores habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou ativou explicitamente a opção em alguma versão), o PvD foi instalado.
- Na linha de comando, a opção `/baseimage` instalou o PvD. Se você especificou essa opção ou usou um script que continha essa opção, o PvD foi instalado.

Se você não sabe se o seu VDA tem o PvD instalado, execute o instalador do novo VDA (2203 ou posterior) na máquina ou na imagem.

- Se o PvD estiver instalado, uma mensagem será exibida indicando que há um componente incompatível.

  - Na interface gráfica, clique em **Cancel** na página que contém a mensagem e confirme que deseja fechar o instalador.
  - Na CLI, o comando simplesmente falha com a mensagem exibida.
- Se o PvD não estiver instalado, a atualização continuará.

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 em desktops com Windows 7 no XenApp e no XenDesktop 7.15 LTSR?*
>
> A Citrix excluiu o Personal vDisk (PvD) do XenApp e do XenDesktop 7.6 LTSR, 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 do XenDesktop 7.15 LTSR. No entanto, para ajudar os clientes com implantações PvD existentes no Windows 7 a migrar para a tecnologia Citrix App Layering, a Citrix decidiu fornecer suporte por tempo limitado para implantações PvD para desktops com Windows 7 por meio do XenApp e XenDesktop 7.15 LTSR Cumulative Updates (CUs) até 14 de janeiro de 2020. O componente PvD será removido das CUs LTSR e não terá mais suporte após 14 de janeiro de 2020. Além disso, o uso do PvD para Windows 7 além de 14 de janeiro de 2020 deixará os sites LTSR fora de conformidade. Também, o PvD para Windows 10 continua a ser excluído do 7.15 LTSR. Portanto, os clientes não devem usá-lo com seus sites LTSR 7.15.

Remover PvD, AppDisks e hosts não suportados

As tecnologias e tipos de host a seguir não são compatíveis com as implantações da versão Current Release 7 do Citrix Virtual Apps and Desktops:

- **Personal vDisks (PvD)** para armazenar dados junto às VMs dos usuários nos catálogos. O recurso da camada de personalização do usuário agora lida com a persistência do usuário.
- **AppDisks** para gerenciar aplicativos usados em Grupos de Entrega.
- **Tipos de host:** Azure Classic, CloudPlatform (o produto Citrix original).

  - Para ver os tipos de host compatíveis nesta versão, consulte Requisitos do sistema.
  - Para obter informações sobre formas alternativas de continuar usando ARM e AWS, consulte CTX270373.

Se a sua implantação atual usa PvDs ou AppDisks, ou se tiver conexões com tipos de host não suportados (por exemplo, Microsoft Azure Classic), você poderá atualizar para a versão 2006 (ou versões posteriores suportadas) somente após remover itens que usam essas tecnologias. Se a sua implantação atual usa conexões de host de nuvem pública (por exemplo, AWS), certifique-se de ter uma Licença Hybrid Rights antes de atualizar. Quando o instalador detecta uma ou mais das tecnologias não suportadas ou conexões de host sem a Licença Hybrid Rights, a atualização é pausada ou interrompida, e uma mensagem explicativa é exibida. 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 VDA anterior. Antes que possa atualizar seus VDAs para a versão 2006 (ou uma versão mais recente suportada), você deve remover esse software, mesmo que nunca o tenha usado. Ao usar a interface gráfica, a remoção pode ser feita para você, ou você pode incluir opções de remoção ao usar a CLI. Para obter detalhes, consulte Atualizar 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 o PvD. Isso afeta catálogos e Grupos de Entrega.

Para remover PvD de grupos e catálogos:

1. No Studio, se um grupo de entrega contiver máquinas de um catálogo que usa PVD, remova essas máquinas do grupo.
2. No Studio, exclua todos os catálogos que contêm máquinas que usam PvD.

Atualizações de VDA: a atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA sim. Para obter detalhes, consulte VDAs que possuem componentes PvD ou AppDisks.

Se você planeja usar App Layering em vez de PvD, consulte Migrar de PvD para App Layering para obter informações sobre a movimentação de dados.

Remover AppDisks

Uma atualização de implantação não pode prosseguir até que você remova o AppDisks de todos os Grupos de Entrega que o utiliza, e depois remova os próprios AppDisks.

1. Selecione **Delivery Groups** no painel de navegação do Studio.
2. Selecione um grupo e clique em **Manage AppDisks** no painel Action.
3. Clique na ação que remove o AppDisk do grupo.
4. Repita as etapas 2 e 3 para cada Grupo de Entrega que usa AppDisks.
5. Selecione **AppDisks** no painel de navegação do Studio.
6. Selecione um AppDisk e clique na ação que exclui o AppDisk.
7. Repita as etapas 5 e 6 para cada AppDisk.

Atualizações de VDA: a atualização da implantação não detecta se os VDAs têm os componentes AppDisk ou PvD instalados. No entanto, os instaladores de VDA sim. Para obter detalhes, consulte VDAs que possuem componentes PvD ou AppDisks.

Remover itens de host não suportados

Uma atualização de implantação para a versão 2006 (ou versão suportada posterior) não pode prosseguir se o site tiver conexões com tipos de host não suportados, como Citrix CloudPlatform ou Microsoft Azure Classic. Conclua as seguintes tarefas antes de tentar uma atualização.

No Studio:

- Exclua todas as conexões com hosts não suportados.
- Se um grupo de entrega contiver máquinas de um catálogo criado com uma imagem mestre de um host não suportado, remova essas máquinas do grupo.
- Exclua todos os catálogos que foram criados usando uma imagem mestre de um host não suportado.

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 os componentes sejam removidos.

> **Nota:**
>
> Quando atualizou para a versão 1912, você teve que desinstalar o VDA atual e, em seguida, instalar o novo VDA. Nesta versão, você será perguntado se deseja que o Citrix remova o componente e continue a atualização.

Os componentes AppDisk e PvD podem ter sido instalados em versões anteriores do VDA, mesmo que você nunca tenha usado essas tecnologias:

- Interface gráfica: nos instaladores de VDA, a página **Additional Components** continha a opção **Citrix AppDisk / Personal vDisk**. O 7.15 LTSR e versões 7.x anteriores habilitavam essa opção por padrão. Portanto, se você aceitou os padrões (ou habilitou a opção explicitamente em qualquer versão em que foi oferecida), o componente foi instalado.
- Interface de linha de comando CLI: especificar a opção `/baseimage` instalou o componente.

O que fazer Se o instalador de VDA não detectar os componentes AppDisks ou PVD no VDA instalado atualmente, a atualização prosseguirá como de costume.

Se o instalador detectar os componentes AppDisks ou PvD no VDA atualmente instalado:

- Interface gráfica: a atualização pausa. Uma mensagem pergunta se você deseja que os componentes não suportados sejam removidos automaticamente. Se você clicar em **OK**, os componentes serão removidos automaticamente e a atualização prossegue.
- Interface de linha de comando CLI: para evitar a falha do comando, inclua as seguintes opções no comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

Limitações

As seguintes limitações se aplicam às atualizações:

- **Instalação de componente seletiva:** se você instalar ou atualizar um componente para uma nova versão, mas optar por não atualizar outros componentes (em máquinas diferentes) que exigem atualização, o Studio lembrará você. Por exemplo, digamos que uma atualização inclua novas versões do Controller e Studio. Você atualiza o Controller, mas não executa o instalador na máquina em que o Studio está instalado. O Studio não permitirá que você continue gerenciando o site até que 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:** não é possível atualizar a partir de uma versão Early Release, Technology Preview ou versão prévia.
- **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 precisa continuar executando sites da versão anterior e sites da versão atual, consulte Considerações sobre ambientes mistos.
- **Seleção de produto:** ao atualizar de uma versão anterior, você não escolhe nem especifica o produto (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) que foi definido durante a instalação.

Considerações sobre ambientes mistos

Quando você faz uma atualização, a Citrix recomenda que você atualize todos os componentes e VDAs para que possa acessar todos os recursos novos e melhorados em sua edição e versão.

Por exemplo, embora você possa usar VDAs atuais em implantações que contêm versões anteriores do Controller, os 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, quando cria um catálogo de máquina, você pode especificar a versão 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. Misturar versões de VDA em um catálogo de máquinas não é recomendado.

Se um catálogo for criado com a configuração de versão mínima de VDA padrão e uma ou mais máquinas tiverem um VDA anterior à versão padrão, essas máquinas não poderão se registrar no Controller e não funcionarão.

Para obter mais informações, consulte Versões do VDA e níveis funcionais.

Vários sites com diferentes versões

Quando seu ambiente contém sites com diferentes versões de produtos (por exemplo, um site XenDesktop 7.18 e um site Citrix Virtual Apps and Desktops 1909), a Citrix recomenda o uso do StoreFront para agregar aplicativos e áreas de trabalho de diferentes versões de produtos. Para obter detalhes, consulte a documentação do StoreFront.

Em um ambiente misto, continue usando as versões do Studio e Director para cada versão, mas certifique-se de que diferentes versões sejam 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 do sistema operacional (SO) suportada. Agora, você deseja usar uma versão

mais recente do componente, mas o sistema operacional não é mais suportado para a versão atual do componente.

Por exemplo, suponha que você instalou um VDA de servidor em uma máquina Windows Server 2008 R2. Agora você deseja atualizar esse VDA para a versão atual, mas o Windows Server 2008 R2 não é suportado na versão atual para a qual você está atualizando.

Se você tentar instalar ou atualizar um componente em um sistema operacional que não é mais permitido, uma mensagem de erro é exibida, como "Não é possível instalar neste sistema operacional" .

Essas considerações se aplicam à atualização das versões Current Release (CU) e Long Term Service Release (LTSR). (Não afeta a aplicação de Atualizações Cumulativas (CU) a uma versão LTSR.)

Siga os links para saber quais sistemas operacionais são suportados:

- Citrix Virtual Apps and Desktops (versão atual):
  - Delivery Controller, Studio, Director, VDAs, servidor de impressão universal
  - Serviço de autenticação federada
  - Para StoreFront, Self-Service Password Reset e Session Recording, consulte o artigo de requisitos do sistema para a versão atual.
- Para LTSRs, consulte as listas de componentes para sua versão LTSR e Atualização Cumulativa. (Selecione sua versão LTSR na página principal da 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. Ele indica a versão de componente válida mais recente suportada, para cada sistema operacional listado, e a versão do componente quando a instalação e a atualização se tornaram inválidas.

Os sistemas operacionais na tabela incluem service packs e atualizações.

Sistema operacional	Componente/recurso	Última versão válida	Instalar/atualizar 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

Sistema operacional	Componente/recurso	Última versão válida	Instalar/atualizar não é possível a partir da versão
Versões do Windows 10 anteriores a 1607	VDA	7.15 LTSR	7.16
Windows 10 versão x86	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Outros componentes do instalador	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	Outros componentes do instalador	7.17	7.18
Windows Server 2012 R2	Outros componentes do instalador *	1912 LTSR	2003
Windows Server 2012 R2	Server VDI	7.15 LTSR	7.16

Windows XP e Windows Vista não são válidos para componentes ou tecnologias 7.x.

* Aplica-se a Delivery Controller, Studio, Director e VDAs.

O que você pode fazer

Você tem opções. Você pode:

- Continuar com o sistema operacional atual
- Recriar a imagem ou atualizar a máquina
- Adicionar novas máquinas e depois remover máquinas antigas

Continuar com o sistema operacional atual Estes métodos são viáveis para VDAs. Se você quiser continuar usando máquinas com o sistema operacional anterior, você pode optar entre:

- Continuar usando a versão do componente instalada.
- Baixar a versão do componente válida mais recente e atualizar o componente para essa versão. (Pressupondo-se que a versão do componente válida mais recente ainda não esteja instalada.)

Por exemplo, você tem um 7.14 VDA 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 atualizar seu VDA para essa versão. Essas versões anteriores

do VDA funcionam em implantações contendo Delivery Controllers com versões mais recentes. Por exemplo, um VDA 7.15 LTSR pode se conectar a um Controller do Citrix Virtual Apps and Desktops 7 1808.

Recriar a imagem ou atualizar a máquina Estes métodos são viáveis para VDAs e outras máquinas que não possuem componentes principais (como Delivery Controllers) instalados. Escolha uma das seguintes opções:

- Depois de retirar a máquina de serviço (ativar o modo de manutenção e permitir que todas as sessões sejam fechadas), você pode recriar a imagem para uma versão do sistema operacional Windows suportada e, em seguida, instalar a versão mais recente do componente.
- Para atualizar o sistema operacional sem recriar a imagem, desinstale o software Citrix antes de atualizar o sistema operacional (isso inclui atualizações internas do seu sistema operacional. Por exemplo, Windows 10 versão 1903 para Windows 10 versão 1909). Caso contrário, o software Citrix ficará em um estado sem suporte. Em seguida, instale o novo componente.
- Para atualizar o sistema operacional em uma máquina VDA sem recriar a imagem, você deve primeiro instalar uma versão do VDA compatível com o sistema operacional para o qual você está atualizando ou atualizar o VDA após atualizar o sistema operacional. Caso contrário, o software Citrix ficará em um estado sem suporte.

Adicionar novas máquinas e depois remover máquinas antigas Este método é viável se você precisar atualizar o sistema operacional em máquinas que contenham um Delivery Controller ou outro componente principal.

A Citrix recomenda que todos os Controllers em um site tenham o mesmo sistema operacional. A sequência de atualização a seguir minimiza o intervalo quando Controllers diferentes têm sistemas operacionais diferentes.

1. Faça um instantâneo de todos os Delivery Controllers no site e, em seguida, faça backup do banco de dados do site.
2. Instale novos Delivery Controllers em servidores limpos com sistemas operacionais suportados. 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 de duas máquinas Windows Server 2008 R2. Siga as recomendações para remover Controllers em Delivery Controllers.

Preparação

Antes de iniciar uma atualização, revise as seguintes informações e realize as tarefas necessárias.

> **Nota:**
>
> Embora a atualização de VDAs ocorra mais adiante na sequência de atualização, seria uma boa ideia escolher um instalador e rever o procedimento antes de iniciar a atualização, para que você saiba o que esperar.

Escolher um instalador e a interface

Use o instalador de produto completo no ISO do produto para atualizar os componentes. Você pode atualizar os VDAs usando o instalador de produto completo ou um dos instaladores autônomos de VDA. Todos os instaladores oferecem interfaces gráficas e de linha de comando.

Para obter mais informações, consulte Instaladores.

Especificações da instalação: depois que concluir os trabalhos de preparação e assim que estiver pronto para iniciar o instalador, o artigo de instalação mostra o que você verá (se estiver usando a interface gráfica) ou o que digitar (se estiver usando a interface de linha de comando).

- Instalar/atualizar componentes principais usando a interface gráfica
- Instalar/atualizar componentes principais usando a linha de comando
- Instalar/atualizar VDAs usando a interface gráfica
- Instalar/atualizar VDAs usando a linha de comando

Se você instalou originalmente um VDA de sessão única com o instalador `VDAWorkstationCoreSetup.exe`, a Citrix recomenda usar o mesmo instalador para atualizá-lo. Se você usar o instalador de VDA de produto completo ou o instalador `VDAWorkstationSetup.exe` para atualizar o VDA, os componentes que foram originalmente excluídos poderão ser instalados, a menos que você os omita ou exclua expressamente da atualização.

Ao atualizar um VDA para a versão atual, ocorre uma reinicialização da máquina durante o processo de atualização. (Esse requisito começou com a versão 7.17.) Isso não pode ser evitado. A atualização é retomada automaticamente após a reinicialização (a menos que você especifique `/noresume` na linha de comando).

Ações com bancos de dados

Faça backup dos bancos de dados de site, monitoramento e log de configuração. Siga as instruções em CTX135207. Se algum problema for descoberto após a atualização, você pode restaurar o backup.

Para obter informações sobre como atualizar versões do SQL Server que não são mais suportadas, consulte Verificação da versão do SQL Server. (Isso se refere ao SQL Server usado para os bancos de dados de site, monitoramento e log de configuração.)

O Microsoft SQL Server Express LocalDB é instalado automaticamente, para uso com o cache de host local. Se você precisar substituir uma versão anterior, a nova versão deve ser SQL Server Express LocalDB 2019. Para obter detalhes sobre como substituir o SQL Server Express LocalDB pela nova versão depois de atualizar os componentes e o site, consulte Substituir SQL Server Express LocalDB.

Confirme que o Citrix Licensing está atualizado

Para obter uma visão abrangente sobre o gerenciamento do Citrix Licensing, consulte Ativar, atualizar e gerenciar licenças Citrix.

Você pode usar o instalador de produto completo para atualizar o servidor de licenças. Ou pode baixar e atualizar os componentes da licença separadamente. Consulte Upgrade.

Antes de atualizar, certifique-se de que a data em Customer Success Services / Software Maintenance / Subscription Advantage seja válida para a nova versão do produto. A data deve ser pelo menos 2021.11.15.

Confirme que o Citrix License Server é compatível

Confirme que o Citrix License Server é compatível com a nova versão. Existem duas maneiras de fazer isso:

- Antes de atualizar outros componentes Citrix, execute o instalador `XenDesktopServerSetup.exe` a partir do layout ISO na máquina que contém um Delivery Controller. Se houver algum problema de incompatibilidade, o instalador informa com as etapas recomendadas para resolver os problemas.
- No diretório `XenDesktop Setup` na mídia de instalação, execute o comando: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. A tela indica se o License Server é compatível. Se o servidor de licenças for incompatível, atualize o servidor de licenças.

Faça backup das modificações do StoreFront

Antes de iniciar uma atualização, se você tiver feito modificações nos arquivos em `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como *default.ica* e *usernamepassword.tfrm*, faça o backup dos arquivos para cada armazenamento. 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 os bloqueios de arquivos sejam eliminados e que não haja atualizações do Windows pendentes.

Antes de iniciar uma atualização, interrompa e desabilite os serviços de agente de monitoramento de terceiros.

Confirme que você tem as permissões adequadas

Além de ser usuário de um domínio, você deve ser um administrador local nas máquinas em que está atualizando os componentes do produto.

O banco de dados do site e o site podem ser atualizados automaticamente ou manualmente. Para a atualização automática de banco de dados, as permissões do usuário do Studio devem incluir a capacidade de atualizar o esquema de 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 gerará 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 as 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, os testes preliminares do site são executados antes que a atualização seja realmente iniciada. Estes testes verificam:

- O banco de dados do site pode ser acessado e o backup foi realizado
- As conexões com serviços essenciais da Citrix estão funcionando corretamente
- O endereço do Citrix License Server está disponível
- O banco de dados do log de configuração pode ser acessado
- Certifique-se de ter a Licença Hybrid Rights se quiser adicionar conexões de host de nuvem pública (por exemplo, AWS). Caso contrário, o teste preliminar do site será pausado ou interrompido e uma mensagem explicativa será exibida.

Após a execução dos testes, você pode exibir um relatório dos resultados. Em seguida, você pode corrigir os problemas que foram detectados e executar os testes novamente. Deixar de executar os testes preliminares do site e resolver os problemas pode afetar a forma como seu site funciona.

O relatório que contém os resultados do teste é um arquivo HTML (`PreliminarySiteTestResult.html`) no mesmo diretório que os logs de instalação. Esse arquivo é criado se não existir. Se o arquivo existir, seu conteúdo será substituído.

Execute os testes

- Quando você estiver usando a interface gráfica do instalador para atualizar, o assistente inclui uma página onde você pode iniciar os testes e exibir o relatório. Depois que os testes forem executados e você examinar o relatório e resolver os problemas encontrados, pode executar novamente os testes. Quando os testes forem concluídos com êxito, clique em Avançar para continuar com o assistente.
- Quando você usa a interface de linha de comando para atualizar, os testes são executados automaticamente. Por padrão, se um teste falhar, a atualização não é executada. Depois de examinar o relatório e resolver os problemas, execute novamente o comando.

A Citrix recomenda sempre executar os testes preliminares do site e, em seguida, resolver os problemas antes de continuar a atualização do Controller e do site. O benefício potencial compensa o tempo dedicado a executar os testes. No entanto, você pode ignorar esta ação recomendada.

- Ao atualizar com a interface gráfica, você pode optar por ignorar os testes e continuar com a atualização.
- Ao atualizar com a linha de comando, você não pode ignorar os testes. Por padrão, um teste de site com falha faz com que o instalador falhe, sem executar a atualização. Na maioria dos casos, se você incluir a opção `/ignore_site_test_failure`, todas as falhas de teste são ignoradas e a atualização prossegue. (Consulte Verificação da versão do SQL Server para ver as exceções.)

Quando atualizar vários Controllers

Quando você inicia a atualização em um Controller e depois inicia a atualização de outro Controller no mesmo local (antes que a primeira atualização termine):

- Se os testes preliminares do site tiverem sido concluídos no primeiro Controller, a página de testes preliminares do site não aparece no assistente do outro Controller.
- Se os testes no primeiro Controller estiverem em andamento quando você iniciar a atualização no outro Controller, a página de testes do site aparece no assistente do outro Controller. Contudo, se os testes no primeiro Controller terminarem, somente os resultados do teste do primeiro Controller são mantidos.

Falhas de teste não relacionadas à integridade do site

- Se os testes preliminares do site falharem devido à falta de memória, disponibilize mais memória e, em seguida, execute novamente os testes.
- Se você tiver permissão para atualizar, mas não executar os testes do site, os testes preliminares do site falharão. Para resolver isso, execute novamente o instalador com uma conta de usuário que tenha permissão para executar os testes.

Verificação da versão do SQL Server

Uma implantação bem-sucedida do Citrix Virtual Apps and Desktops requer uma versão compatível do Microsoft SQL Server para bancos de dados de site, monitoramento e log de configuração. A atualização de uma implantação da Citrix com uma versão do SQL Server que não é mais suportada pode resultar em problemas de funcionalidade, e o site ficará sem suporte.

Para saber quais versões do SQL Server são compatíveis com a versão da Citrix para a qual você está atualizando, consulte o artigo Requisitos do sistema referente à versão.

Ao atualizar um Controller, o instalador da Citrix verifica a versão do SQL Server atualmente instalada que é usada para os bancos de dados de site, monitoramento e log de configuração.

- Se a verificação determinar que a versão do SQL Server atualmente instalada não é suportada na versão do Citrix para a qual você está atualizando:
  - Interface gráfica: a atualização para com uma mensagem. Clique em **I understand** e, em seguida, clique em **Cancel** para fechar o instalador da Citrix. (Você não pode continuar com a atualização.)
  - Interface de linha de comando: o comando falha (mesmo se você incluiu a opção `/ignore_db_check_failure` com o comando).

  Atualize a versão do SQL Server e inicie a atualização do Citrix novamente.
- Se a verificação não puder determinar qual versão do SQL Server está instalada no momento, verifique se a versão atualmente instalada é suportada na versão para a qual você está atualizando (Requisitos do sistema).
  - Interface gráfica: a atualização para com uma mensagem.
    - Se a versão do SQL Server atualmente instalada for suportada, clique em **I understand** para fechar a mensagem e, em seguida, clique em **Next** para continuar com a atualização do Citrix.
    - Se a versão do SQL Server atualmente instalada não for suportada, clique em **I understand** para fechar a mensagem e clique em **Cancel** para encerrar a atualização do

Citrix. Atualize seu SQL Server para uma versão compatível e inicie a atualização do Citrix novamente.

- Interface de linha de comando: o comando falha com uma mensagem. Depois de fechar a mensagem:
  - Se a versão do SQL Server atualmente instalada for suportada, execute o comando novamente com a opção /`ignore_db_check_failure`.
  - Se a versão do SQL Server atualmente instalada não for suportada, atualize o SQL Server para uma versão suportada. Execute o comando novamente para iniciar a atualização do Citrix.

Atualizar o SQL Server

Se você abrir novos servidores SQL Server e migrar o banco de dados do site, as cadeias de conexão deverão ser atualizadas.

Se, atualmente, o site usa SQL Server Express para o banco de dados do site (que a Citrix instalou automaticamente durante a criação do site):

1. Instale a versão mais recente do SQL Server Express.
2. Desanexe o banco de dados.
3. Anexe o banco de dados ao novo SQL Server Express.
4. Migre as cadeias de conexão.

Para obter mais informações, consulte Configurar cadeias de conexão e a documentação do produto Microsoft SQL Server.

Substituir SQL Server Express LocalDB

O Microsoft SQL Server Express LocalDB é um recurso do SQL Server Express que o cache de host local usa de modo autônomo. O cache de host local não requer nenhum componente do SQL Server Express que não seja o SQL Server Express LocalDB.

Se você instalou uma versão do Delivery Controller anterior à 1912 e, em seguida, atualizou sua implantação para a versão 1912 ou posterior, o Citrix não atualiza automaticamente a versão do SQL Server Express LocalDB. Por que não? Porque você pode ter componentes não Citrix que dependem do SQL Server Express LocalDB. Se você tiver componentes não Citrix que estejam usando o SQL Server Express LocalDB, certifique-se de que a atualização do SQL Server Express LocalDB não interrompa esses componentes. Para atualizar (substituir) a versão do SQL Server Express LocalDB, siga as orientações nesta seção.

- **Ao atualizar Delivery Controllers para o Citrix Virtual Apps and Desktops versão 1912 ou 2003:** a atualização do SQL Server Express LocalDB é opcional. O cache de host local funciona corretamente, sem perda de funcionalidade, independentemente de você atualizar o SQL Server Express LocalDB. Adicionamos a opção de passar para uma versão mais recente do SQL Server Express LocalDB no caso de haver preocupações sobre o fim do suporte da Microsoft para SQL Server Express LocalDB 2014.
- **Ao atualizar Delivery Controllers para versões do Citrix Virtual Apps and Desktops mais recentes do que 2003:** a versão suportada é SQL Server Express LocalDB 2019. Se você instalou originalmente um Delivery Controller anterior à versão 1912 e não substituiu o SQL Server Express LocalDB pela versão mais recente desde então, você deve substituir o software do banco de dados agora. Caso contrário, o cache de host local não funcionará.

O que você precisa:

- A mídia de instalação do Citrix Virtual Apps and Desktops (para a versão para a qual você atualizou). A mídia contém uma cópia do Microsoft SQL Server Express LocalDB 2019.
- Uma ferramenta do Windows Sysinternals que você pode baixar da Microsoft.

Procedimento:

1. Conclua a atualização dos componentes, bancos de dados e site do Citrix Virtual Apps and Desktops. (Essas atualizações de bancos de dados afetam os bancos de dados de site, monitoramento e log de configuração. Elas não afetam o banco de dados de cache de host local que usa o SQL Server Express LocalDB.)
2. No Delivery Controller, faça o download de `PsExec` da Microsoft. Consulte o documento da Microsoft PsExec v2.2.
3. Pare o Citrix High Availability Service.
4. No prompt de comando, execute `PsExec` e alterne para a conta de serviço de rede, Network Service.

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE"cmd
   ```

   Opcionalmente, você pode usar `whoami` para confirmar se o prompt de comando está sendo executado como a conta de serviço de rede.

   ```
   whoami
   ```

   ```
   nt authority\networkservice
   ```

5. Vá para a pasta que contém SqlLocalDB.

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

6. Pare e exclua `CitrixHA` (LocalDB).


```
SqlLocalDB stop CitrixHA

SqlLocalDB delete CitrixHA
```

7. Remova os arquivos relacionados em `C:\Windows\ServiceProfiles\NetworkService`.

```
HADatabaseName.*
HADatabaseName_log.*
HAImportDatabaseName.*
HAImportDatabaseName_log.*
<!--NeedCopy-->
```

   Dica: sua implantação talvez não tenha `HAImportDatabaseName.*` nem `HAImportDatabaseName_.*`

8. Desinstale o SQL Server Express LocalDB 2014 do servidor, usando o recurso do Windows para remover programas.
9. Instale o SQL Server Express LocalDB 2019. Na pasta `Support > SQLLocalDB` na mídia de instalação do Citrix Virtual Apps and Desktops, clique duas vezes em `sqllocaldb.msi`. A reinicialização pode ser necessária para concluir a instalação. (O novo SQLLocalDB reside em `C:\Program Files\Microsoft SQL Server\150\Tools\Binn`.)
10. Inicie o Citrix High Availability Service.
11. Assegure-se de que o banco de dados do cache de host local seja criado em cada Delivery Controller. Isso confirma que o serviço de alta disponibilidade (agente secundário) pode assumir o controle, se necessário.
    - No servidor do Controller, vá para `C:\Windows\ServiceProfiles\NetworkService`.
    - Confirme que `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.

Segurança

June 28, 2023

O Citrix Virtual Apps and Desktops oferece uma solução elaborada pensando na segurança que permite adaptar o seu ambiente às suas necessidades de segurança.

Uma preocupação de segurança que o pessoal de TI enfrenta com os trabalhadores móveis são dados perdidos ou roubados. Ao hospedar aplicativos e áreas de trabalho, o Citrix Virtual Apps and Desktops separa com segurança os dados confidenciais e a propriedade intelectual dos dispositivos de ponto

final, mantendo todos os dados em um datacenter. Quando as políticas são ativadas para permitir a transferência de dados, todos os dados são criptografados.

Os datacenters do Citrix Virtual Apps and Desktops também facilitam a resposta a incidentes com um serviço centralizado de monitoramento e gerenciamento. O Director permite que o pessoal de TI monitore e analise os dados que estão sendo acessados em toda a rede, e o Studio permite que o pessoal da TI corrija e aplique patches à maioria das vulnerabilidades no datacenter, em vez de corrigir os problemas localmente em cada dispositivo de usuário final.

O Citrix Virtual Apps and Desktops também simplifica auditorias e conformidades regulamentares, pois os investigadores podem usar uma trilha de auditoria centralizada para determinar quem acessou quais aplicativos e dados. O Director reúne 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 dar 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 um controle granular sobre os usuários, aplicando políticas em diferentes níveis da rede: do nível local ao nível de 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 as preocupações de segurança com trabalhadores de contingência terceirizados. Os administradores também podem usar o recurso de Bloqueio de Área de Trabalho para que os usuários finais só possam usar a área de trabalho virtual, evitando qualquer acesso ao sistema operacional local do dispositivo do usuário final.

Os administradores podem aumentar a segurança no Citrix Virtual Apps ou no Citrix Virtual Desktops configurando o Site para usar o protocolo TLS (Transport Layer Security) do Controller ou entre usuários finais e Virtual Delivery Agents (VDAs). O protocolo também pode ser ativado em um Site para fornecer autenticação de servidor, criptografia de fluxo de dados e verificações de integridade de mensagens para uma conexão TCP/IP.

O Citrix Virtual Apps and Desktops também oferece suporte à autenticação multifator para Windows ou um aplicativo específico. A autenticação multifator também pode ser usada para gerenciar todos os recursos entregues pelo Citrix Virtual Apps and Desktops. Esses métodos incluem:

- Tokens
- Cartões inteligentes
- RADIUS
- Kerberos
- Biometria

O Citrix Virtual Desktops pode ser integrado a muitas soluções de segurança de terceiros: do gerenciamento de identidade até software antivírus. Uma lista de produtos suportados pode ser encontrada em http://www.citrix.com/ready.

As versões selecionadas do Citrix Virtual Apps and Desktops são certificadas para o padrão Common Criteria. Para obter uma lista desses padrões, vá para https://www.commoncriteriaportal.org/cc/.

Autenticação FIDO2

June 28, 2023

Autorização local e autenticação virtual usando FIDO2

O suporte para FIDO2 permite que os usuários aproveitem os componentes FIDO2 do ponto de extremidade local em uma máquina virtual. Agora, os usuários podem autenticar na sessão virtual usando chaves de segurança FIDO2 ou biometria integrada em dispositivos com TPM 2.0 e Windows Hello.

Para obter mais informações sobre o FIDO2, consulte FIDO2: WebAuthn & CTAP.

Para obter informações sobre como usar o recurso, consulte Redirecionamento FIDO2.

Requisitos

Requisitos da Citrix

- Citrix Virtual Apps and Desktops 2009 ou posterior
- Aplicativo Citrix Workspace 2009.1 para Windows ou posterior

Requisitos da Microsoft

- Windows 10 versão 1809 (cliente) ou posterior
- Windows 2019 (SO do servidor)
- Windows Hello (opcional)

Requisitos da FIDO2

- Windows Hello
  - TPM 2.0
  - Biometria integrada
    - Reconhecimento facial

        - Scanner de impressão digital
    - WebAuthn
- Chave de segurança habilitada para FIDO2

Suporte UWP para autenticação usando FIDO2

Com o lançamento do Citrix Virtual Apps and Desktops 2112, a Citrix oferece suporte ao FIDO2 em aplicativos que usam um aplicativo Microsoft UWP para fornecer autenticação.

Aplicativos como o Microsoft Teams, Microsoft Outlook para Office 365 e OneDrive usam um aplicativo UWP para autenticação como um link para o Azure Active Directory. A Citrix agora oferece suporte ao uso do FIDO2 para autenticar esses aplicativos.

Requisitos de UWP

- Citrix Virtual Apps and Desktops 2112 ou posterior
- Aplicativo Citrix Workspace 2009.1 para Windows ou posterior

Para obter mais informações sobre os requisitos da Microsoft e da FIDO2, consulte Requisitos.

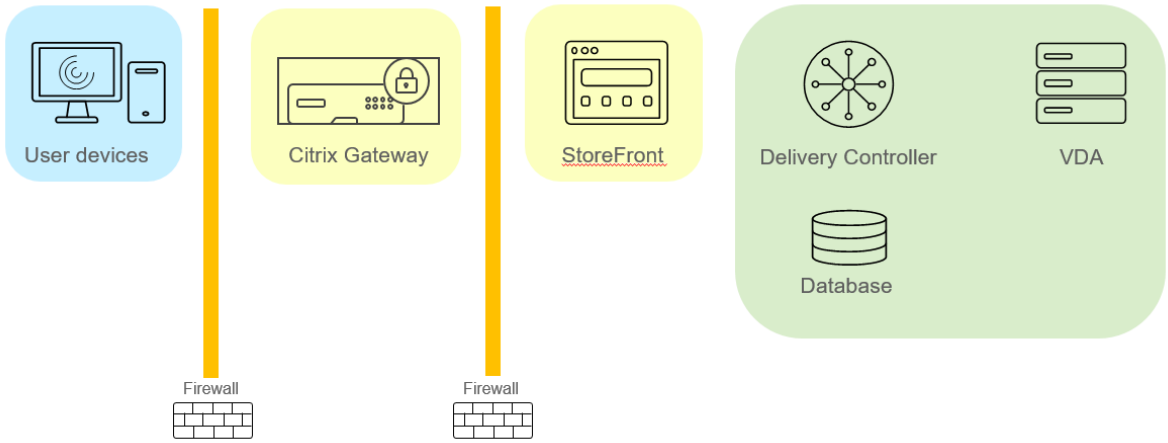
Integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway

June 28, 2023

Os servidores StoreFront são implantados e configurados para gerenciar o acesso a dados e recursos publicados. Para o acesso remoto, é recomendável adicionar o Citrix Gateway na frente do StoreFront.

> **Nota:**
>
> Para obter etapas de configuração detalhadas sobre como integrar o Citrix Virtual Apps and Desktops com o Citrix Gateway, consulte a documentação do StoreFront.

O diagrama a seguir ilustra um exemplo de uma implantação 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 de usuário executam o aplicativo Citrix Workspace para criar uma conexão segura e acessar seus aplicativos, área de trabalho e arquivos.



Os usuários fazem logon e se autenticam 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. Os aplicativos e os dados estão em servidores apropriados (não ilustrados no diagrama). Servidores separados são usados para aplicativos e dados confidenciais de segurança.

Considerações de segurança e práticas recomendadas

June 28, 2023

> **Nota:**
>
> Sua organização talvez precise atender a padrões de segurança específicos para atender aos requisitos regulamentares. Este documento não cobre esse assunto, porque tais padrões de segurança mudam ao longo do tempo. Para obter informações atualizadas sobre padrões de segurança e produtos Citrix, consulte http://www.citrix.com/security/.

Práticas de segurança recomendadas

Mantenha todos os computadores em seu ambiente atualizados com os patches de segurança. Uma vantagem é que você pode usar thin clients como terminais, o que simplifica essa tarefa.

Proteja todos os computadores no seu ambiente com software antivírus.

Considere usar um software antimalware específico à plataforma.

Ao instalar o software, instale nos caminhos padrão fornecidos.

- Se você instalar o software em um local de arquivo diferente do caminho padrão fornecido, considere adicionar medidas de segurança adicionais, como permissões restritas, ao local do seu arquivo.

Todas as comunicações de rede devem ser devidamente 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 áreas de trabalho é protegida pelo Citrix SecureICA, que é configurado por padrão para criptografia de 128 bits. Você pode configurar o SecureICA quando estiver criando ou atualizando um grupo de entrega.

> **Nota:**
>
> O Citrix SecureICA faz parte do protocolo ICA/HDX, mas não é um protocolo de segurança de rede compatível com padrões, como Transport Layer Security (TLS). Você também pode proteger as comunicações de rede entre dispositivos de usuário e áreas de trabalho usando o TLS. Para configurar o TLS, consulte Transport Layer Security (TLS).

Aplique as práticas recomendadas do Windows para gerenciamento de contas. Não crie uma conta em um modelo ou imagem antes que sejam duplicados pelo Machine Creation Services ou Provisioning Services. Não agende tarefas usando contas de domínio privilegiado armazenadas. Não crie manualmente contas de computadores Active Directory compartilhados. Essas práticas ajudarão a evitar que um ataque ao computador obtenha senhas de contas persistentes locais e, em seguida, as utilize para fazer logon em imagens compartilhadas do MCS/PVS pertencentes a outras pessoas.

Firewalls

Proteja todos os computadores em seu ambiente com firewalls de perímetro, inclusive em limites de enclave conforme apropriado.

Todos os computadores do seu ambiente devem ser protegidos 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 abertos automaticamente se o Serviço do Firewall do Windows for detectado (mesmo que o firewall não esteja ativado). Você também pode optar por configurar essas portas de firewall manualmente. Se você usar um firewall diferente, deverá configurá-lo manualmente.

Se você estiver migrando um ambiente convencional para esta versão, talvez seja 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 você usa essa versão, o firewall de perímetro deve ser dispositivo de modo que a área de trabalho 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 do banco de dados e os

Controllers. Considere também aplicar proteção entre o dispositivo do usuário e a área de trabalho 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-los. A Citrix recomenda que você não use essas portas para nenhuma outra coisa, para evitar a possibilidade de deixar inadvertidamente as interfaces administrativas abertas ao ataque. As portas 1494 e 2598 são oficialmente registradas na IANA (Internet Assigned Number Authority, http://www.iana.org/).

Segurança de aplicativos

Para evitar que usuários não administradores executem ações maliciosas, recomendamos que você configure as 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 necessários. Os privilégios do Microsoft Windows continuam a ser aplicados às áreas de trabalho da maneira usual: configure privilégios por meio de Atribuição de Direitos de Usuário e filiações a grupos por meio da Política de Grupo. Uma vantagem desta versão é que é possível conceder a um usuário direitos administrativos a uma área de trabalho sem também conceder controle físico sobre o computador no qual a área de trabalho é armazenada.

Observe o seguinte ao planejar privilégios de área de trabalho:

- Por padrão, quando usuários não privilegiados se conectam a uma área de trabalho, eles veem o fuso horário do sistema que executa a área de trabalho em vez do fuso horário de seu próprio dispositivo de usuário. Para obter informações sobre como permitir que os usuários vejam a hora local de seus dispositivos ao usar áreas de trabalho, consulte o artigo Gerenciar grupos de entrega.
- Um usuário que é administrador em uma área de trabalho tem controle total sobre essa área de trabalho. Se uma área de trabalho for uma área de trabalho em pool em vez de uma área de trabalho dedicada, o usuário deve ser confiável em relação a todos os outros usuários da área de trabalho, incluindo usuários futuros. Todos os usuários da área de trabalho precisam estar cientes do risco potencial permanente à segurança de seus dados que essa situação representa. Essa consideração não se aplica a áreas de trabalho dedicadas, que têm apenas um único usuário, usuário esse que não deve ser um administrador em nenhuma outra área de trabalho.

- Um usuário que é um administrador em uma área de trabalho geralmente pode instalar software nessa área de trabalho, incluindo softwares potencialmente maliciosos. O usuário também pode monitorar ou controlar o tráfego em qualquer rede conectada à área de trabalho, se quiser.

Gerenciar direitos de logon

Os direitos de logon são necessários para contas de usuário e contas de computador. Os direitos de logon do Microsoft Windows continuam a ser aplicados às áreas de trabalho da maneira usual: configure direitos de logon por meio de Atribuição de Direitos de Usuário e filiações a grupos por meio da Política de Grupo.

Os direitos de logon do Windows são: efetuar logon localmente, efetuar logon através dos Serviços de Área de Trabalho Remota, efetuar logon na rede (acessar o computador a partir da rede), efetuar logon como um trabalho em lote e efetuar logon como serviço.

Para contas de computador, conceda aos computadores apenas os direitos de logon necessários. O direito de logon "Acesso a este computador pela rede"é necessário:

- Em VDAs, para as contas de computador dos Delivery Controllers
- Em Delivery Controllers, para as contas de computador dos VDAs. Consulte Detecção do Controller baseada em unidades organizacionais do Active Directory.
- Em 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 necessários.

De acordo com a Microsoft, por padrão, o grupo Usuários de Área de Trabalho Remota recebe o direito de logon "Permitir logon pelos Serviços de Área de Trabalho Remota"(exceto em controladores de domínio).

A política de segurança da sua organização pode indicar explicitamente que esse grupo deve ser removido desse direito de logon. Considere a seguinte abordagem:

- O Virtual Delivery Agent (VDA) para SO multissessão usa os Serviços de Área de Trabalho Remota da Microsoft. Você pode configurar o grupo Usuários de Área de Trabalho Remota como um grupo restrito e controlar a afiliação do grupo por meio das 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 de Área de Trabalho Remota não é necessário. Sendo assim, para esses componentes, o grupo Usuários de Área de Trabalho Remota não requer o direito de logon "Permitir logon pelos Serviços de Área de Trabalho Remota"; você pode removê-lo. Adicionalmente:

  - Se você administrar os computadores por meio dos Serviços de Área de Trabalho Remota, certifique-se de que todos os administradores já sejam membros do grupo Administradores.
  - Se você não administrar os computadores por meio dos Serviços de Área de Trabalho Remota, considere desabilitar os Serviços de Área de Trabalho Remota nesses computadores.

Embora seja possível adicionar usuários e grupos ao direito de logon "Negar logon pelos Serviços de Área de Trabalho Remota", o uso de direitos de logon de negação não é geralmente 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 a coleta tiver sido aprovada pelo administrador do site. Em seguida, envia as informações à Citrix, para ajudar a melhorar o produto.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): oferece suporte ao gerenciamento e ao provisionamento de AppDisks, integração com AppDNA e gerenciamento de App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): seleciona as áreas de trabalho ou aplicativos virtuais 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 ao site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): repositório de 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 os 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 a funcionalidade usada pelo console para enumerar recursos em um pool de hipervisores.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): planeja a criação de VMs de área de trabalho.
- 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): oferece suporte ao gerenciamento do StoreFront. (Não faz parte do componente StoreFront em si.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): oferece suporte a operações de gerenciamento privilegiadas do StoreFront. (Não faz parte do componente StoreFront em si.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): propaga dados de configuração do banco de dados do site principal para o cache de host local.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): seleciona as áreas de trabalho ou aplicativos virtuais disponíveis para os usuários quando o banco de dados do site principal não está disponível.

A instalação do Delivery Controller também cria os seguintes serviços do Windows. Eles também são criados quando instalados com outros componentes Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): oferece suporte à 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 e recomendações da análise 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. Isso não é usado atualmente. Se tiver sido ativado, desative-o.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

A instalação do Delivery Controller também cria estes seguintes serviços do Windows. Eles não são usados atualmente, mas devem estar ativados. Não os desative.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Exceto para o Citrix Storefront Privileged Administration Service, esses serviços recebem o direito de logon Fazer logon como um serviço e os privilégios Ajustar cotas de memória para um processo, Gerar auditoria de segurança e Substituir um token no nível de processo. Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Delivery Controller e são desativados automaticamente.

Configurar configurações de serviço

Exceto para o Citrix Storefront Privileged Administration Service e o Citrix Telemetry Service, os serviços do Delivery Controller Windows listados acima na seção Configurar direitos de usuário são

configurados para fazer logon como a identidade NETWORK SERVICE. Não altere essas configurações de serviço.

O Citrix Config Synchronizer Service precisa que a conta NETWORK SERVICE pertença ao grupo Local Administrator no Delivery Controller. Isso permite que o cache de host local funcione corretamente.

O Citrix Storefront Privileged Administration Service é configurado para fazer logon no sistema local (NT AUTHORITY\SYSTEM). Isso é necessário para operações do Delivery Controller StoreFront que normalmente não estão disponíveis para serviços (incluindo a criação de sites do Microsoft IIS). Não altere suas configurações de serviço.

O Citrix Telemetry Service é configurado para fazer logon como sua própria identidade de serviço específica.

Você pode desativar o Citrix Telemetry Service. À parte desse serviço, e dos serviços que já estão desativados, não desative nenhum outro dos serviços Delivery Controller Windows.

Configurar configurações de registro

Não é mais preciso permitir a criação de pastas e nomes de arquivo 8.3 no sistema de arquivos VDA. A chave do registro **NtfsDisable8dot3NameCreation** pode ser configurada para desativar a criação de pastas e nomes de arquivo 8.3. Você também pode configurar isso usando o comando **fsutil.exe behavior set disable8dot3**.

Implicações de segurança no cenário de implantação

Seu ambiente de usuário pode conter dispositivos de usuário que não são gerenciados pela sua organização e estão completamente sob o controle do usuário, ou dispositivos de usuário que são gerenciados e administrados pela sua organização. As considerações de segurança para esses dois ambientes são geralmente diferentes.

Dispositivos de usuário gerenciados

Os 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 uma única área de trabalho é executada no modo somente tela inteira. Siga as práticas de segurança geral recomendadas descritas acima para todos os dispositivos de usuário gerenciados. Essa versão tem a vantagem de que um mínimo de softwares é necessário no dispositivo do usuário.

Um dispositivo de usuário gerenciado pode ser configurado para ser usado no modo somente tela inteira ou no modo de janela:

- Modo somente tela inteira: os usuários fazem logon com a tela usual de logon no Windows. As mesmas credenciais de usuário são usadas para fazer logon automaticamente nesta versão.
- Os usuários veem suas áreas de trabalho em uma janela: os usuários primeiro fazem logon no dispositivo do usuário e, em seguida, fazem logon nesta versão por meio de um site fornecido com a versão.

Dispositivos de usuário não gerenciados

Os dispositivos de usuário que não são gerenciados e administrados por uma organização confiável não podem ser considerados como sob controle administrativo. Por exemplo, você pode permitir que os usuários obtenham e configurem seus próprios dispositivos, mas os usuários podem não seguir as práticas recomendadas de segurança geral descritas acima. Esta versão tem a vantagem de que é possível entregar áreas de trabalho de forma segura para dispositivos de usuário não gerenciados. Esses dispositivos ainda devem ter proteção antivírus básica para a defesa contra registradores de pressionamento de teclas 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 o controle físico deles. No entanto, você ainda deve considerar as implicações dos usuários armazenando dados em áreas de trabalho. Não é uma boa prática para os usuários armazenar dados em áreas de trabalho; os dados devem ser mantidos em servidores de arquivos, servidores de bancos de dados ou outros repositórios onde possam ser adequadamente protegidos.

Seu ambiente de área de trabalho pode consistir em vários tipos de área de trabalho, como áreas de trabalho em poll e dedicadas. Os usuários nunca devem armazenar dados em áreas de trabalho compartilhadas entre usuários, como áreas de trabalho em poll. Se os usuários armazenarem dados em áreas de trabalho dedicadas, os dados devem ser removidos se a área de trabalho for disponibilizada posteriormente a outros usuários.

Ambientes de versões mistas

Os ambientes de versões mistas são inevitáveis durante algumas atualizações. Siga as práticas recomendadas e minimize o tempo de coexistência entre os componentes Citrix de diferentes versões. Em ambientes de versões mistas, a política de segurança, por exemplo, pode não ser aplicada uniformemente.

> **Nota:**
>
> Isso é típico de outros produtos de software; o uso de uma versão anterior do Active Directory apenas reforça parcialmente a Política de Grupo com versões posteriores do Windows.

O cenário a seguir descreve um problema de segurança que pode ocorrer em um ambiente Citrix específico de versões mistas. Quando o Citrix Receiver 1.7 é usado para se conectar a uma área de trabalho virtual executando o VDA no XenApp e XenDesktop 7.6 Feature Pack 2, a configuração de política **Permitir transferência de arquivos entre área de trabalho e cliente** é ativada no Site, mas não pode ser desativada por um Delivery Controller executando o XenApp e XenDesktop 7.1. Ele não reconhece a configuração de política, que foi lançada na versão posterior do produto. Essa configuração de política permite que os usuários façam upload e download de arquivos para sua área de trabalho virtual, que é o problema de segurança. Para solucionar isso, atualize o Delivery Controller (ou uma instância autônoma do Studio) para a versão 7.6 Feature Pack 2 e use a Política de Grupo para desativar a configuração de política. Alternativamente use uma política local em todas as áreas de trabalho virtuais afetadas.

Considerações de segurança do Remote PC Access

O Remote PC Access implementa os seguintes recursos de segurança:

- O uso do cartão inteligente é suportado.
- Quando uma sessão remota se conecta, o monitor do PC do escritório aparece em branco.
- O Remote PC Access redireciona todas as entradas de teclado e mouse para a sessão remota, exceto CTRL+ALT+DEL e cartões inteligentes habilitados por USB e dispositivos biométricos.
- O SmoothRoaming é suportado apenas para um único usuário.
- Quando um usuário tem uma sessão remota conectada a um PC de escritório, somente esse usuário pode retomar o acesso local do PC do escritório. Para retomar o acesso local, o usuário pressiona Ctrl-Alt-Del no PC local e, em seguida, faz logon com as mesmas credenciais usadas pela sessão remota. O usuário também pode retomar o acesso local inserindo um cartão inteligente ou usando a biometria, se o seu sistema tiver a integração apropriada do provedor de credenciais de terceiros. Esse comportamento padrão pode ser substituído ativando a Troca Rápida de Usuário por meio de Objetos de Política de Grupo (GPOs) ou editando o registro.

> **Nota:**
>
> A Citrix recomenda que você não atribua privilégios de administrador de VDA a usuários de sessão geral.

Atribuições automáticas

Por padrão, o Remote PC Access suporta a atribuição automática de vários usuários a um VDA. No XenDesktop 5.6 Feature Pack 1, os administradores podem substituir esse comportamento usando o script PowerShell RemotePCAccess.ps1. Essa 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:**
>
> Editar o registro incorretamente pode causar sérios problemas e exigir que você reinstale seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Para restringir atribuições automáticas a um único usuário:

Em cada Controller no site, defina a seguinte entrada do 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 posteriormente 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 do escritório físico.

Confiança em XML

A configuração de confiança em XML se aplica a implantações que usam:

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

Habilitar a configuração de confiança em XML permite que os usuários autentiquem com êxito e iniciem aplicativos. O Delivery Controller confia nas credenciais enviadas do StoreFront. Ative essa con-

figuração somente quando você tiver protegido as comunicações entre os Delivery Controllers e o StoreFront (usando firewalls, IPSec ou outras recomendações de segurança).

Essa configuração é desativada por padrão.

Use o Citrix Virtual Apps and Desktops PowerShell SDK para verificar, ativar ou desativar a configuração de confiança em XML.

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

Cartões inteligentes

June 28, 2023

Os cartões inteligentes e tecnologias equivalentes são suportados nas diretrizes descritas neste artigo. Para usar cartões inteligentes com o 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 devem ser usados com cartões inteligentes.
- Familiarize-se com a tecnologia de cartão inteligente e o hardware e software do fornecedor de cartões inteligentes selecionado.
- Saiba como implantar certificados digitais em um ambiente distribuído.

> **Nota:**
>
> O registro de cartões inteligentes não é suportado com o cartão inteligente rápido. O registro de cartões inteligentes pode funcionar quando o cartão inteligente rápido está desativado, mas depende do tipo de cartão inteligente e middleware. Entre em contato com o fornecedor de cartão inteligente e middleware para obter informações sobre sua integração com o Citrix Virtual Apps and Desktops e suporte para registro de cartões inteligentes em sessões virtuais.

Tipos de cartões inteligentes

Os cartões inteligentes empresariais e ao consumidor têm as mesmas dimensões, conectores elétricos e se encaixam nos mesmos leitores de cartões inteligentes.

Os cartões inteligentes para uso empresarial contêm certificados digitais. Esses cartões inteligentes suportam logon do Windows e também podem ser usados com aplicativos para assinatura digital e criptografia de documentos e e-mail. O Citrix Virtual Apps and Desktops oferece suporte a esses usos.

Os 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 com chip e PIN). Eles não suportam o logon do Windows ou aplicativos típicos do Windows. Aplicativos especializados do Windows e uma infraestrutura de software adequada (incluindo, por exemplo, uma conexão com uma rede de cartão de pagamento) são necessários para uso com esses cartões inteligentes. Entre em contato com o seu representante da Citrix para obter informações sobre o suporte a esses aplicativos especializados no Citrix Virtual Apps ou no Citrix Virtual Desktops.

Para cartões inteligentes empresariais, existem equivalentes compatíveis que podem ser usados de forma semelhante.

- Um token USB equivalente a cartão inteligente se conecta diretamente a uma porta USB. Esses tokens USB são geralmente do tamanho de uma unidade flash USB, mas podem ser tão pequenos quanto um cartão SIM usado em um celular. Eles aparecem como a combinação de um cartão inteligente com um leitor de cartão inteligente USB.
- Um cartão inteligente virtual usando um TPM (Trusted Platform Module) do Windows aparece como um cartão inteligente. Esses cartões inteligentes virtuais são compatíveis com 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 oferecem suporte a cartões inteligentes virtuais.
  - Para obter mais informações sobre cartões inteligentes virtuais, consulte Virtual Smart Card Overview.

  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 aos cartões inteligentes.

O suporte a cartões inteligentes Citrix Virtual Apps and Desktops é baseado nas especificações do padrão Microsoft Personal Computer/Smart Card (PC/SC). Um requisito mínimo é que os cartões inteligentes e os dispositivos de cartão inteligente devem ser suportados pelo sistema operacional Windows subjacente e devem ser aprovados pelos Windows Hardware Quality Labs (WHQL) da

Microsoft para serem usados em computadores que executam sistemas operacionais Windows qualificados. Consulte a documentação da Microsoft para obter informações adicionais sobre a conformidade PC/SC de hardware. Outros tipos de dispositivos de usuário podem estar em conformidade com o padrão PS/SC. Para obter mais informações, consulte o programa Citrix Ready.

Normalmente, um driver de dispositivo separado é necessário para o cartão inteligente ou equivalente de cada fornecedor. No entanto, se os cartões inteligentes estiverem em conformidade com um padrão, como o NIST Personal Identity Verification (PIV), pode ser possível usar um único driver de dispositivo para uma variedade de cartões inteligentes. O driver de dispositivo deve ser instalado no dispositivo do usuário e no Virtual Delivery Agent (VDA). O driver de dispositivo geralmente é fornecido como parte de um pacote de middleware de cartão inteligente disponível a partir de um parceiro Citrix; o pacote de middleware de cartão inteligente oferece recursos avançados. O driver do dispositivo também pode ser descrito como um provedor de serviços de criptografia (CSP), provedor de armazenamento de chaves (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 a Citrix, consulte http://www.citrix.com/ready.

Middleware	Cartões compatíveis
Gemalto Mini Driver 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 do dispositivo.

Remote PC Access

Os cartões inteligentes são suportados apenas para acesso remoto a PCs de escritório físico com Windows 10, Windows 8 ou Windows 7.

Os seguintes cartões inteligentes foram testados com o Remote PC Access:

Middleware	Cartões compatíveis
Gemalto .NET minidriver	Gemalto .NET v2+

Cartão inteligente rápido

O cartão inteligente rápido é uma melhoria ao redirecionamento de cartão inteligente baseado em PC/SC HDX existente. Melhora o desempenho quando os cartões inteligentes são usados em situações WAN de alta latência. Quando a latência é alta, a melhoria de desempenho pode ser significativa (por exemplo, 15 segundos para um logon rápido de cartão inteligente do Windows comparado a mais de 1 minuto com o redirecionamento de cartão inteligente baseado em PC/SC).

O cartão inteligente rápido é ativado por padrão em computadores host com Windows VDAs atualmente suportados. Para desabilitar o cartão inteligente rápido no lado do host —por exemplo, para fins de diagnóstico —defina a configuração do registro "Disable Cryptographic Redirection"com qualquer valor diferente de zero:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

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 ativado ou desativado à força (por exemplo, para fins de diagnóstico) com as seguintes configurações de registro:

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (como DWORD diferente de zero)

Ou

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (como DWORD diferente de zero)

O hive do 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 oferece suporte ao cartão inteligente rápido. Se você configurar cartões inteligentes rápidos no arquivo default.ica, os aplicativos Citrix Workspace que não são para Windows continuam a usar o redirecionamento PC/SC existente.
- Os únicos cenários de salto duplo que os cartões inteligentes rápidos suportam são ICA > ICA com cartão inteligente rápido ativado em ambos os saltos. Como o cartão inteligente rápido não suporta cenários de salto duplo ICA > RDP, esses cenários não funcionam.

- O cartão inteligente rápido não suporta Cryptography Next Generation. Sendo assim, o cartão inteligente rápido não aceita cartões inteligentes de criptografia de curva elíptica (ECC, Elliptic Curve Cryptography).
- O cartão inteligente rápido suporta apenas operações de contêiner de chave somente leitura.
- O cartão inteligente rápido não aceita a mudança do PIN do cartão inteligente.

A partir da versão 2203 do VDA e do aplicativo Citrix Workspace versão 2202 para Windows (ou posterior), o cartão inteligente rápido é compatível com o Cryptography Next Generation (CNG). Além disso, os cartões inteligentes de criptografia de curva elíptica (ECC, Elliptic Curve Cryptography) 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 a partir da mesma sessão de logon do usuário. Por exemplo, se **Session PIN Caching** estiver ativado e o usuário final tiver fornecido anteriormente o PIN do cartão inteligente para o 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). **Session PIN Caching** melhora a experiência do usuário, reduzindo o número de vezes que o usuário precisa inserir o PIN do cartão inteligente. Além disso, se o cartão inteligente for usado para fazer logon no VDA, o PIN de logon do cartão inteligente do Windows pode, opcionalmente, ser salvo no **Session PIN Caching**. Isso pode melhorar ainda mais a experiência do usuário.

Session PIN Caching está desativado por padrão. Ele pode ser ativado e controlado com as seguintes configurações de registro no VDA:

Em HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` como um DWORD (diferente de zero para habilitar)
- `EnableLogonPinSessionCache` como um DWORD (diferente de zero para habilitar)
- `PinSessionCacheEntryStaleTimeout` como um DWORD (número de segundos antes de uma entrada ficar obsoleta; o padrão é 1 hora)

Tipos de leitores de cartão inteligente

Um leitor de cartão inteligente pode ser incorporado ao dispositivo do usuário ou conectado separadamente ao dispositivo do usuário (geralmente por USB ou Bluetooth). Os leitores de cartão de contato que estão em conformidade com a especificação USB CCID (Chip Card Interface Devices) são suportados. Eles contêm um slot para leitura do cartão inteligente, por inserção ou passagem. O padrão Deutsche Kreditwirtschaft (DK) define quatro classes de leitores de cartão de contato.

- Os leitores de cartão inteligente de classe 1 são os mais comuns e geralmente contêm um slot. Os leitores de cartão inteligente de classe 1 são compatíveis, geralmente com um driver de dispositivo padrão CCID fornecido com o sistema operacional.

- Os leitores de cartão inteligente de classe 2 também contêm um teclado seguro que não pode ser acessado pelo dispositivo do usuário. Os leitores de cartão inteligente de classe 2 podem ser incorporados ao teclado regular com um teclado seguro integrado. Para leitores de cartão inteligente de classe 2, entre em contato com um representante da Citrix; um driver de dispositivo específico para leitor pode ser necessário para habilitar o recurso de teclado seguro.
- Os leitores de cartão inteligente de classe 3 também contêm uma tela segura. Os leitores de cartão inteligente de classe 3 não são suportados.
- Os leitores de cartão inteligente de classe 4 também contêm um módulo de transação seguro. Os leitores de cartão inteligente de classe 4 não são suportados.

> **Nota:**
>
> A classe do leitor de cartão inteligente não está relacionada com a 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 compatíveis de cartão inteligente, consulte a documentação do aplicativo Citrix Workspace que você está usando. Na documentação do aplicativo Citrix Workspace, as versões compatíveis são listadas na seção sobre cartões inteligentes ou na seção de requisitos do sistema.

Experiência do usuário

O suporte a cartões inteligentes é integrado ao Citrix Virtual Apps and Desktops usando um canal virtual de cartão inteligente ICA/HDX específico que é ativado por padrão.

Importante: não use o redirecionamento USB genérico para leitores de cartão inteligente. Essa funcionalidade é desativada por padrão para leitores de cartão inteligente e, se ativada, não é compatível.

Vários cartões inteligentes e vários leitores podem ser utilizados no mesmo dispositivo de usuário, mas se a autenticação de passagem estiver em uso, apenas um cartão inteligente deve ser inserido quando o usuário iniciar uma área de trabalho ou aplicativo virtual. Quando um cartão inteligente é usado em um aplicativo (por exemplo, para funções de criptografia ou assinatura digital), pode haver outras solicitações para inserir um cartão inteligente ou inserir um PIN. Isso pode ocorrer se mais de um cartão inteligente tiver sido inserido ao mesmo tempo.

- Se os usuários forem solicitados a inserir um cartão inteligente quando o cartão inteligente já estiver no leitor, eles devem selecionar Cancelar.
- Se os usuários forem solicitados a inserir o PIN, eles devem inserir o PIN novamente.

Você pode redefinir os PINs usando um sistema de gerenciamento de cartões ou um utilitário do fornecedor.

> **Importante:**
>
> Em uma sessão do Citrix Virtual Apps ou do Citrix Virtual Desktops, o uso de um cartão inteligente com o aplicativo de Conexão de Área de Trabalho Remota da Microsoft não é suportado. Isso é descrito às vezes como um uso de "salto duplo".

Antes de implantar cartões inteligentes

- Obtenha um driver de dispositivo para o leitor de cartão inteligente e instale-o no dispositivo do usuário. Muitos leitores de cartão inteligente podem usar o driver de dispositivo CCID fornecido pela Microsoft.
- Obtenha um driver de dispositivo e um software de provedor de serviços de criptografia (CSP) do fornecedor do seu cartão inteligente e instale-os em dispositivos de usuários e áreas de trabalho virtuais. O driver e o software CSP devem ser compatíveis com o Citrix Virtual Apps and Desktops; verifique a documentação do fornecedor para saber sobre a compatibilidade. Para áreas de trabalho virtuais que usam cartões inteligentes que suportam e usam o modelo minidriver, o download dos minidrivers de cartão inteligente ocorre automaticamente, mas você também pode obtê-los em http://catalog.update.microsoft.com ou com o seu fornecedor. Além disso, se o middleware PKCS#11 for necessário, peça-o para o 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 da Citrix.
- Adicione o URL do Citrix Receiver para Web à lista de sites confiáveis para usuários que usam cartões inteligentes no Internet Explorer com Windows 10. No Windows 10, o Internet Explorer não é executado no modo protegido por padrão para sites confiáveis.
- Certifique-se de que sua infraestrutura de chave pública (PKI) esteja configurada adequadamente. Isso inclui garantir que o mapeamento do certificado à conta esteja configurado corretamente para o ambiente do Active Directory e que a validação do certificado do usuário possa ser executada com êxito.
- Certifique-se de que a sua implantação atenda aos requisitos de sistema dos outros componentes Citrix usados com cartões inteligentes, incluindo o aplicativo Citrix Workspace e o StoreFront.
- Garanta o acesso aos seguintes servidores no seu site:
  - Controlador de domínio do Active Directory da 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 Remote PC Access): Microsoft Exchange Server

Habilitar o uso de cartão inteligente

Etapa 1. Emita cartões inteligentes para os usuários de acordo com a sua política de emissão de cartão.

Etapa 2. (Opcional) Configure os cartões inteligentes para habilitar os usuários para o Remote PC Access.

Etapa 3. Instale e configure o Delivery Controller e o StoreFront (se ainda não estiverem instalados) para controlar remotamente o cartão inteligente.

Etapa 4. Habilite o StoreFront para uso do cartão inteligente. Para obter detalhes, consulte Configurar autenticação por cartão inteligente na documentação do StoreFront.

Etapa 5. Habilite o Citrix Gateway/Access Gateway para o uso de cartão inteligente. Para obter detalhes, consulte Configurar autenticação e autorização e Configurar acesso a cartão inteligente com Web Interface na documentação do NetScaler.

Etapa 6. Habilite VDAs para uso de cartão inteligente.

- Assegure-se de que o VDA tenha os aplicativos e as atualizações necessários.
- Instale o middleware.
- Configure o controle remoto do cartão inteligente, permitindo a comunicação de dados de cartões inteligentes entre o aplicativo Citrix Workspace em um dispositivo de usuário e uma sessão de área de trabalho virtual.

Etapa 7. Habilite dispositivos de usuário (incluindo computadores associados ao domínio ou não associados ao domínio) para uso de cartões inteligentes. Consulte Configurar autenticação de cartão inteligente na documentação do StoreFront para obter detalhes.

- Importe o certificado raiz da autoridade de certificação e o certificado de 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, importando o icaclient.adm usando o Console de Gerenciamento de Política de Grupo e habilite a autenticação de cartão inteligente.

Etapa 8. Teste a implantação. Certifique-se de que a implantação esteja configurada corretamente, iniciando uma área de trabalho virtual com o cartão inteligente de um usuário de teste. Teste todos os mecanismos de acesso possíveis (por exemplo, acessar a área de trabalho por meio do Internet Explorer e do aplicativo Citrix Workspace).

Rastrear a contagem de inserções no leitor de cartão inteligente

Com o controle 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 uma matriz de estruturas de dados SCARD_READERSTATE —uma por cada leitor que você monitora. A palavra superior (16 bits) do campo dwEventState de cada SCARD_READERSTATE contém a contagem de leitores. Para obter mais informações, consulte os artigos da Microsoft SCardGetStatusChangeA function e SCARD_READERSTATEA structure.

A configuração do relatório de inserções **Reader Insert Count Reporting** está desativada por padrão. Para ativar 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 se desconecta, a contagem é reiniciada do zero.

O **Reader Insert Count Reporting** é compatível com middleware de cartão inteligente de terceiros.

Implantações de cartões inteligentes

June 28, 2023

Os seguintes tipos de implantações de cartão inteligente são suportados por esta versão de produto e por ambientes mistos que contêm esta versão. Outras configurações podem funcionar, mas não são suportadas.

Tipo	Conectividade ao StoreFront
Computadores associados ao domínio local	Diretamente conectado
Acesso remoto a partir de computadores associados ao domínio	Conectado através do Citrix Gateway
Computadores não associados ao domínio	Diretamente conectado
Acesso remoto a partir de computadores não associados ao domínio	Conectado através do Citrix Gateway
Thin clients e computadores não associados ao domínio que acessam o site do Desktop Appliance	Conectado através de sites de Desktop Appliance

Tipo	Conectividade ao StoreFront
Thin clients e computadores associados ao domínio que acessam o StoreFront através da URL de Serviços XenApp	Conectado através de URLs de 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 é associado ao domínio ou não é associado ao domínio.
- Como o dispositivo está conectado ao StoreFront.
- Qual software é usado para visualizar áreas de trabalho e aplicativos virtuais.

Além disso, aplicativos habilitados para cartões inteligentes, como o Microsoft Word e o Microsoft Excel, podem ser usados nessas implantações. Esses aplicativos permitem que os usuários assinem ou criptografem digitalmente documentos.

Autenticação bimodal

Sempre que possível em cada uma dessas implantações, o Receiver suporta a 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 deixou o cartão em casa ou o certificado de logon expirou).

Como os usuários de dispositivos não associados ao domínio fazem logon no Receiver para Windows diretamente, você pode habilitar que os usuários façam fallback para a autenticação explícita. Se você configurar a autenticação bimodal, os usuários são inicialmente solicitados a fazer logon usando seus cartões inteligentes e PINs, mas têm a opção de selecionar a autenticação explícita se tiverem algum problema com seus cartões inteligentes.

Se você implantar o Citrix Gateway, os usuários efetuam logon em seus dispositivos e são solicitados pelo Receiver para Windows para se autenticar no Citrix Gateway. Isso se aplica a dispositivos associados ao domínio e não associados ao domínio. Os usuários podem fazer logon no Citrix Gateway usando seus cartões inteligentes e PINs ou com credenciais explícitas. Isso permite que você ofereça aos usuários a autenticação bimodal para logons do Citrix Gateway. Configure a autenticação de passagem do Citrix Gateway para o StoreFront e delegue a validação de credenciais ao Citrix Gateway para usuários de cartões inteligentes, para que os usuários sejam autenticados silenciosamente no StoreFront.

Considerações sobre várias florestas do Active Directory

Em um ambiente Citrix, os cartões inteligentes são suportados em uma única floresta. Os logons de cartões inteligentes em várias florestas exigem a confiança bidirecional direta da floresta para todas as contas de usuário. Implantações multiflorestas mais complexas envolvendo cartões inteligentes (ou seja, quando as relações de confiança são apenas unidirecionais ou de tipos diferentes) não são suportadas.

Você pode usar cartões inteligentes em um ambiente Citrix que inclui áreas de trabalho remotas. Esse recurso pode ser instalado localmente (no dispositivo do usuário ao qual o cartão inteligente está conectado) ou remotamente (na área de trabalho remota à qual o dispositivo do usuário se conecta).

Política de remoção de cartões inteligentes

A política de remoção de cartões inteligentes definida no produto determina o que acontece se você remover o cartão inteligente do leitor durante uma sessão. A política de remoção de cartões inteligentes é configurada e tratada pelo sistema operacional Windows.

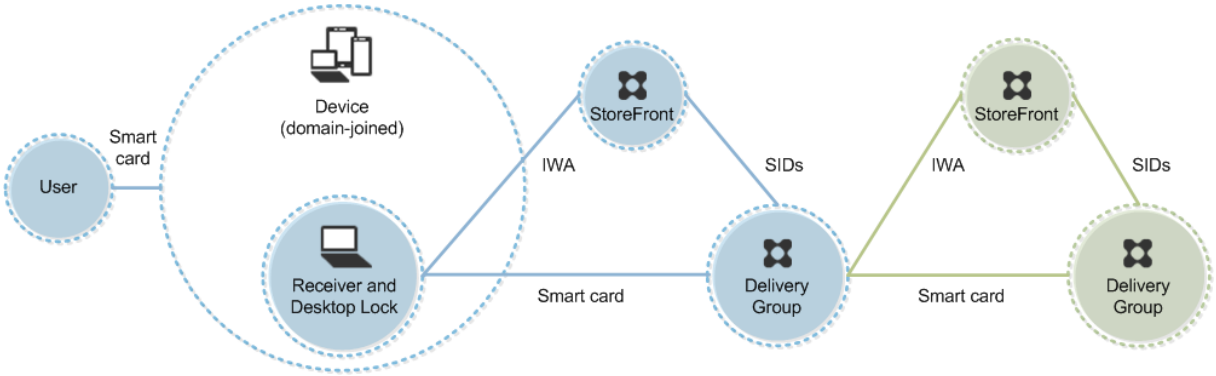
Configuração da política	Comportamento da área de trabalho
Nenhuma ação	No action.
Bloquear estação de trabalho	A sessão da área de trabalho é desconectada e a área de trabalho virtual é bloqueada.
Forçar logoff	O usuário é forçado a fazer logoff. Se a conexão da rede for perdida e essa configuração 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 certificados

Se a verificação de revogação de certificado estiver ativada e um usuário inserir um cartão inteligente com um certificado inválido em um leitor de cartões, o usuário não poderá autenticar ou acessar a área de trabalho ou 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 permanecem ativas.

Exemplo de implantação: computadores associados ao domínio

Essa implantação envolve dispositivos de usuário associados ao domínio que executam o Desktop Viewer e se conectam diretamente ao StoreFront.

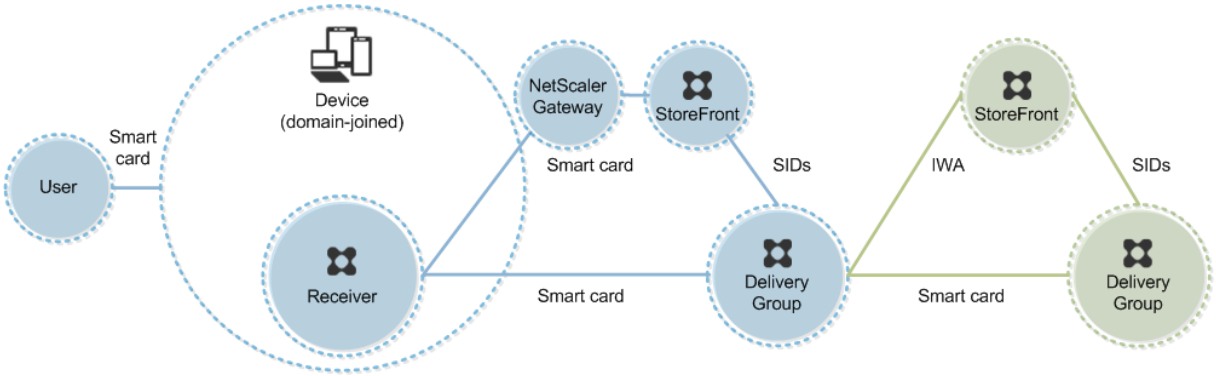


Um usuário faz logon em um dispositivo usando um cartão inteligente e um PIN. O Receiver autentica o usuário em um servidor Storefront usando a Autenticação Integrada do Windows (IWA). O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia uma área de trabalho ou aplicativo virtual, ele não é solicitado a digitar o PIN novamente porque o recurso de logon único está configurado no Receiver.

Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Exemplo de implantação: acesso remoto a partir de computadores associados ao domínio

Essa implantação envolve dispositivos de usuário associados ao domínio que executam o Desktop Viewer e se conectam ao StoreFront através do Citrix Gateway/Access Gateway.



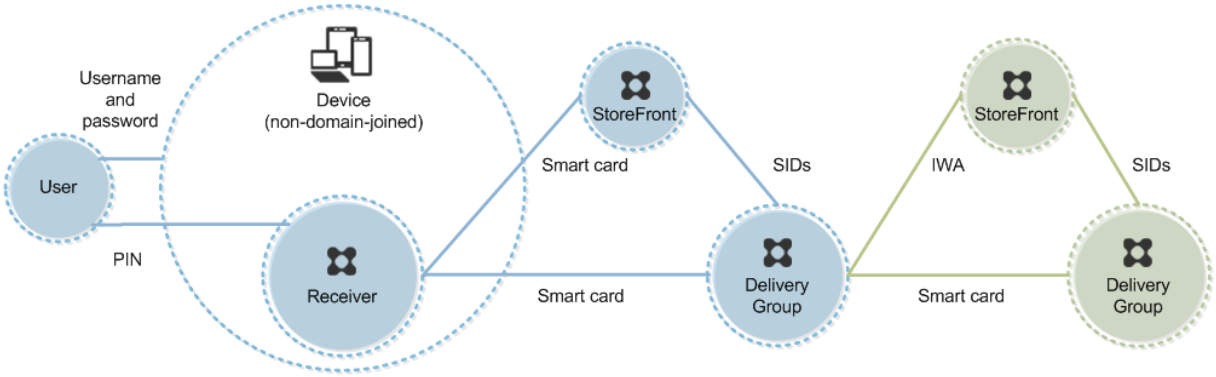
Um usuário faz logon em um dispositivo usando um cartão inteligente e um PIN e, em seguida, faz logon novamente no Citrix Gateway/Access Gateway. Este segundo logon pode ser com o cartão inteligente e PIN ou com um nome de usuário e senha, porque o Receiver permite a autenticação bimodal nesta implantação.

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 uma área de trabalho ou aplicativo virtual, ele não é solicitado a digitar o PIN novamente porque o recurso de logon único está configurado no Receiver.

Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Exemplo de implantação: computadores não associados ao domínio

Essa 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 uma senha, mas, como o dispositivo não está associado a um domínio, as credenciais para esse 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. Em seguida, o Receiver se autentica no Storefront.

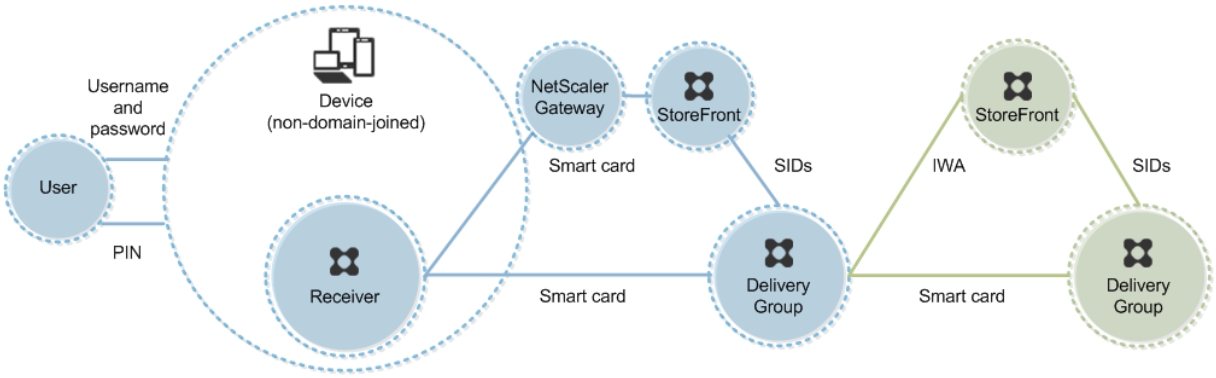
O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia uma área de trabalho ou aplicativo virtual, ele é solicitado a digitar um PIN novamente porque o recurso de logon único não está disponível nesta implantação.

Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no

segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Exemplo de implantação: acesso remoto a partir de computadores não associados ao domínio

Essa 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 uma senha, mas, como o dispositivo não está associado a um domínio, as credenciais para esse 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. Em seguida, o Receiver se autentica no Storefront.

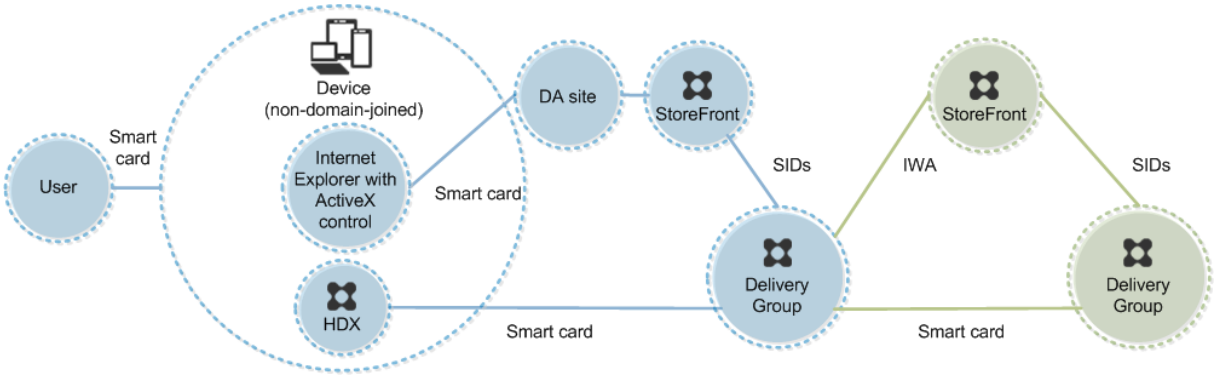
O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. Quando o usuário inicia uma área de trabalho ou aplicativo virtual, ele é solicitado a digitar um PIN novamente porque o recurso de logon único não está disponível nesta implantação.

Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Exemplo de implantação: thin clients e computadores não associados ao domínio acessando o site do Desktop Appliance

Essa implantação envolve dispositivos de usuário não associados ao domínio que podem executar o Desktop Lock e se conectar ao StoreFront através 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. Uma alternativa ao Desktop Viewer, ele é projetado principalmente para thin clients Windows e computadores Windows reatribuídos. 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 áreas de trabalho de computadores Windows Server e áreas de trabalho de computadores Windows Desktop A instalação do Desktop Lock é opcional.



Um usuário faz logon em um dispositivo com um cartão inteligente. Se o Desktop Lock estiver sendo executado no dispositivo, o dispositivo será configurado para iniciar um site do Desktop Appliance através do Internet Explorer em execução no Modo de Quiosque. Um controle ActiveX no site solicita ao usuário um PIN e o envia para o StoreFront. O StoreFront passa os identificadores de segurança do usuário (SIDs) para o Citrix Virtual Apps ou Citrix Virtual Desktops. A primeira área de trabalho disponível na lista alfabética de um grupo de área de trabalho atribuído é iniciada.

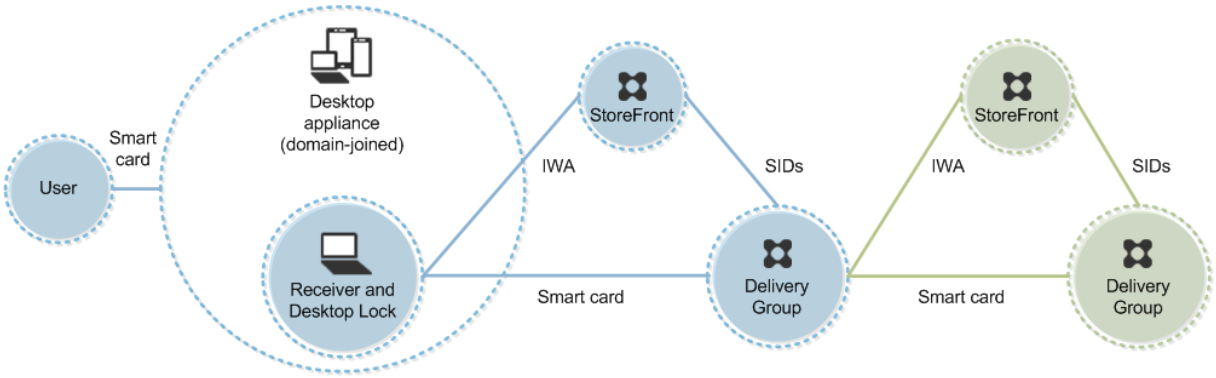
Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Exemplo de implantação: thin clients e computadores associados ao domínio que acessam o StoreFront através da URL de Serviços XenApp

Essa implantação envolve dispositivos de usuário associados ao domínio que executam o Desktop Lock e se conectam ao StoreFront através de URLs do XenApp Services.

O Desktop Lock é um componente separado que é lançado com o Citrix Virtual Apps, Citrix Virtual Desktops e VDI-in-a-Box. Uma alternativa ao Desktop Viewer, ele é projetado principalmente para thin clients Windows e computadores Windows reatribuídos. 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 áreas de trabalho de

computadores Windows Server e áreas de trabalho de computadores Windows Desktop A instalação do Desktop Lock é opcional.



Um usuário faz logon em um dispositivo usando um cartão inteligente e um PIN. Se o Desktop Lock estiver sendo executado 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 uma área de trabalho virtual, ele não é solicitado a digitar o PIN novamente porque o recurso de logon único está configurado no Receiver.

Essa implantação pode ser estendida para um salto duplo com a adição de um segundo servidor StoreFront e um servidor que hospeda aplicativos. Um Receiver da área de trabalho virtual se autentica no segundo servidor StoreFront. Qualquer método de autenticação pode ser usado para essa segunda conexão. A configuração mostrada para o primeiro salto pode ser reutilizada no segundo salto ou usada somente no segundo salto.

Autenticação de passagem e logon único com cartões inteligentes

June 28, 2023

Autenticação de passagem

A autenticação de passagem com cartões inteligentes para áreas de trabalho virtuais é suportada em dispositivos de usuário que executam Windows 10, Windows 8 e Windows 7 SP1 edições Enterprise e Professional.

A autenticação de passagem com cartões inteligentes para aplicativos hospedados é suportada em servidores que executam o Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 e Windows Server 2008 R2 SP1.

Para usar a autenticação de passagem com aplicativos hospedados em cartões inteligentes, certifique-se de ativar o uso do Kerberos quando configurar a Passagem com autenticação de cartão inteligente como o método de autenticação para o site.

Nota: a disponibilidade da autenticação de passagem com cartões inteligentes depende de muitos fatores que incluem, mas não se limitam a:

- Políticas de segurança da sua organização em relação à autenticação de passagem.
- Tipo e configuração de middleware.
- Tipos de leitores de cartão inteligente.
- Política de cache de PIN do middleware.

A passagem com autenticação de cartão inteligente 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 de passagem ao iniciar áreas de trabalho e aplicativos virtuais. Você pode usar esse recurso em implantações de cartão inteligente associadas ao domínio, diretas ao StoreFront e associadas ao domínio de NetScaler para StoreFront para reduzir o número de vezes que o usuário digita o PIN. Para usar o logon único nesses tipos de implantação, edite os seguintes parâmetros no arquivo default.ica, localizado no servidor StoreFront:

- Implantações de cartão inteligente diretas ao StoreFront associadas ao domínio —Defina DisableCtrlAltDel como Desativado
- Implantações de smart card conectado ao domínio NetScaler-to-StoreFront —Defina UseLocalUserAndPassword como Ativado

Para obter mais instruções sobre como definir esses parâmetros, consulte a documentação do StoreFront ou Citrix Gateway.

A disponibilidade da funcionalidade de logon único depende de muitos fatores, incluindo, entre outros:

- Políticas de segurança da sua organização em relação ao logon único.
- Tipo e configuração de 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 um computador com um leitor de cartão inteligente conectado, um bloco do Windows pode aparecer representando o modo de autenticação bem-sucedido anterior, como cartão inteligente ou senha. Como resultado,

> quando o logon único está ativado, o bloco de logon único pode aparecer. Para fazer logon, o usuário deve selecionar **Alternar Usuários** para selecionar outro bloco, pois o bloco de logon único não funcionará.

Transport Layer Security (TLS)

June 28, 2023

O Citrix Virtual Apps and Desktops oferece suporte ao protocolo TLS (Transport Layer Security) para conexões baseadas em TCP entre componentes. O Citrix Virtual Apps and Desktops também oferece suporte ao protocolo DTLS (Datagram Transport Layer Security) para conexões ICA/HDX baseadas em UDP usando transporte adaptativo.

TLS e DTLS são semelhantes e suportam os mesmos certificados digitais. Configurar um site Citrix Virtual Apps ou Citrix Virtual Desktops para usar o TLS também o configura para usar o DTLS. Use os seguintes procedimentos; as etapas são comuns ao TLS e ao 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.

- Ative as conexões TLS entre o aplicativo Citrix Workspace e os Virtual Delivery Agents (VDAs) realizando as seguintes tarefas:

  - Configure o TLS nos computadores onde os VDAs estão instalados. (Para sua comodidade, referências a computadores onde os VDAs estão instalados serão simplesmente mencionadas como "VDAs".) Para obter informações gerais, consulte Configurações de TLS em VDAs. É altamente recomendável usar o script do PowerShell fornecido pela Citrix para configurar o TLS/DTLS. Para obter detalhes, consulte Configurar o TLS em um VDA usando o script PowerShell. No entanto, se você quiser configurar o TLS/DTLS manualmente, consulte Configurar manualmente o TLS em um VDA.

  - Configure o TLS nos Grupos de Entrega que contêm os VDAs executando um conjunto de cmdlets do PowerShell no Studio. Para obter detalhes, consulte Configurar o TLS em grupos de entrega.

    Requisitos e considerações:

    * A ativação de conexões TLS entre usuários e VDAs é válida somente para os Sites XenApp 7.6 e XenDesktop 7.6, além das versões posteriores suportadas.

* Configure o TLS nos Grupos de Entrega e nos VDAs depois de instalar componentes, criar um Site, criar catálogos de máquinas e criar Grupos de Entrega.
* Para configurar o TLS nos Grupos de Entrega, 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 no computador onde o VDA está instalado.
* Em VDAs em pool que são provisionados por Machine Creation Services ou Provisioning Services, a imagem da máquina VDA é redefinida na reinicialização, fazendo com que as configurações anteriores de TLS sejam perdidas. Execute o script do PowerShell sempre que o VDA for reiniciado para redefinir as configurações de TLS.

> **Aviso:**
>
> Nas tarefas que incluem trabalhar no registro do Windows, tenha muito cuidado: editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Para obter informações sobre como ativar o TLS no banco de dados do Site, consulte CTX137556.

Instalar certificados de servidor TLS em Controllers

Para HTTPS, o XML Service suporta 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 aos Cloud Connectors para criptografar o tráfego STA e XML.

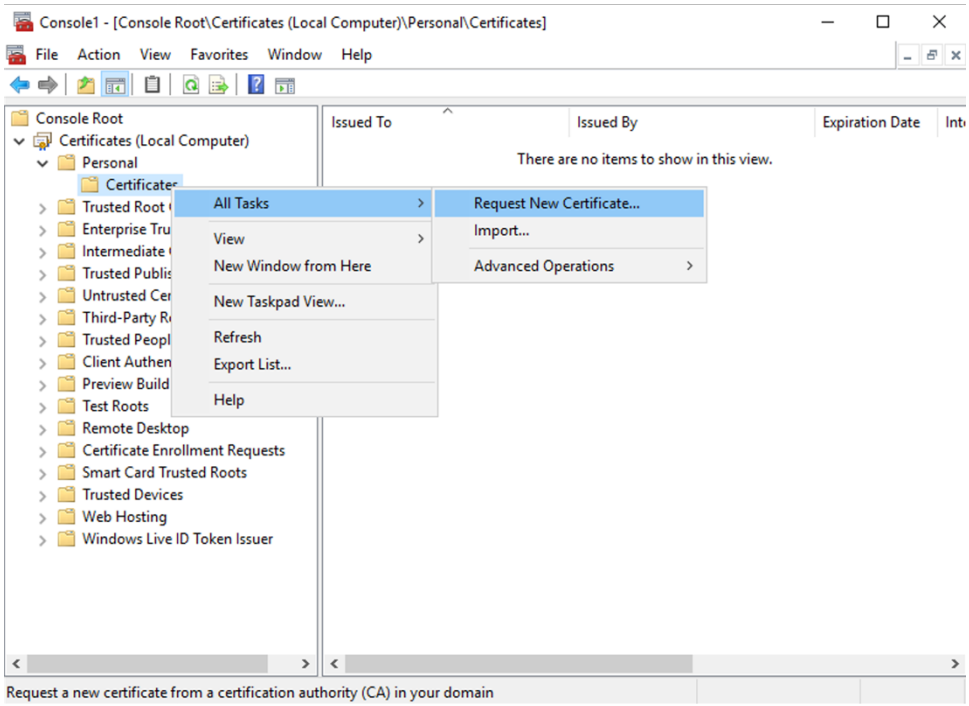
Embora existam vários tipos diferentes de autoridades de certificação e métodos de solicitação de certificado a partir delas, este artigo descreve a Autoridade de Certificação da Microsoft. A Autoridade de Certificação da Microsoft precisa ter um modelo de certificado publicado para fins de Autenticação de Servidor.

Se a Autoridade de Certificação da Microsoft estiver integrada a um domínio do Active Directory ou a uma floresta confiável à qual os Delivery Controllers estão associados, você pode adquirir um certificado no assistente de Registro de Certificado do snap-in do MMC dos Certificados.

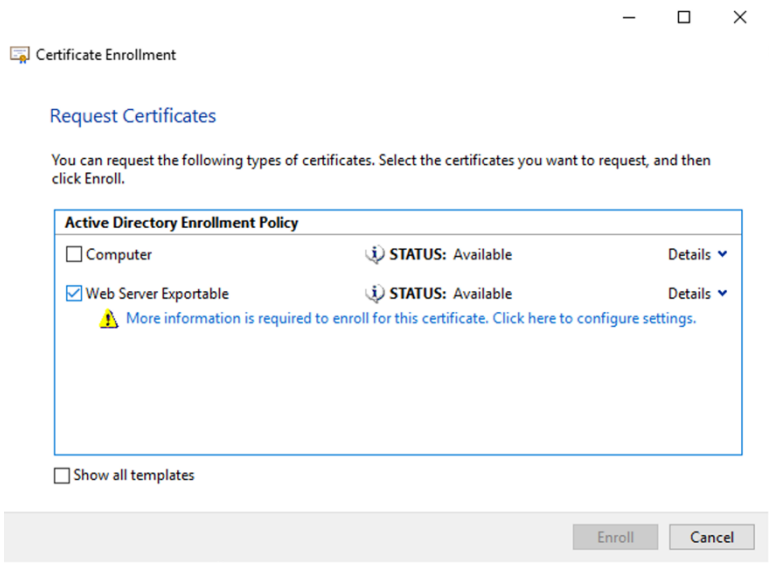
Solicitar e instalar um certificado

1. No Delivery Controller, abra o console MMC e adicione o snap-in Certificates. Quando solicitado, selecione Conta de computador.

2. Expanda **Pessoal > Certificates** e, em seguida, use o comando de menu de contexto **Todas as tarefas > Solicitar novo certificado**.



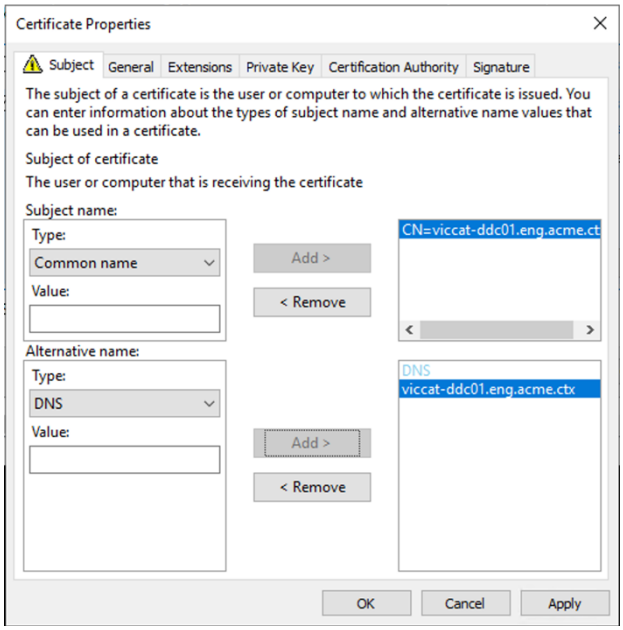
3. Clique em **Avançar** para começar e, depois, clique em **Avançar** para confirmar que você está adquirindo o certificado no registro do Active Directory.
4. Selecione o modelo para o certificado de autenticação do servidor. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Entidade, você pode clicar em **Inscrever** 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 da entidade: selecione o nome comum Common Name e adicione o FQDN do Delivery Controller.

Nome alternativo: selecione o DNS e adicione o FQDN do Delivery Controller.



Configurar a porta de ouvinte SSL/TLS

1. Abra uma janela de comando do PowerShell como administrador da máquina.
2. Execute os seguintes comandos para obter GUID do Aplicativo de Serviço de Broker:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $\_; $\_.GetValueNames() | ForEach-Object {
  $key.GetValue($\_)  }
  | Where-Object {
  $\_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

```



```
19 Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
       ForegroundColor Yellow
20 <!--NeedCopy-->
```

3. Execute os seguintes comandos na mesma janela do PowerShell para obter a impressão digital do certificado que você instalou anteriormente:

```
1 $HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
      .Hostname
2
3 $Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
      Object {
4  $_.Subject -match ("CN=" + $HostName) }
5  ).Thumbprint -join ';'
6
7 Write-Host -Object "Certificate Thumbprint for $($HostName): $(
      $Thumbprint)" -Foreground Yellow
8 <!--NeedCopy-->
```

4. Execute os seguintes comandos na mesma janela do PowerShell para configurar a porta SSL/TLS do Broker Service e usar o certificado para criptografia:

```
1 $IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
      | Select-Object -ExpandProperty IPV4Address
2
3 $IPPort = "$($IPV4_Address):443"
4
5 $SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
      appid={
6  $Formatted_Guid }
7  "
8
9 $SSLxml | netsh
10
11 . netsh http show sslcert
12 <!--NeedCopy-->
```

Quando configurada corretamente, a saída do último comando `.netsh http show sslcert` mostra que o ouvinte está usando o `IP:port` correto e que `Application ID` corresponde ao GUID do aplicativo Broker Service.

Se os servidores confiam no certificado instalado nos Delivery Controllers, agora você pode configurar as vinculações de StoreFront Delivery Controllers e Citrix Gateway STA para usar HTTPS em vez de HTTP.

> **Nota:**
>
> Se o Controller estiver instalado no Windows Server 2016 e o StoreFront estiver instalado no Windows Server 2012 R2, uma alteração de configuração será necessária no Controller para alterar a ordem dos pacotes de codificação TLS. Essa alteração de configuração não é necessária para

> o Controller e o StoreFront com outras combinações de versões do Windows Server.

A lista ordenada de pacotes de codificação deve incluir os pacotes de codificação `TLS_ECDHE_RSA_WITH_AES_` ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (ou ambos); esses pacotes de codificação devem preceder os pacotes de codificação `TLS_DHE_`.

1. Usando o Editor de Política de Grupo da Microsoft, navegue até **Configuração do Computador > Modelos Administrativos > Rede > Definições de configuração de SSL**.
2. Edite a política "Ordem do Pacote de Codificação de SSL". Por padrão, essa política é definida como "Não configurada". Defina essa política como Ativado.
3. Organize os pacotes na ordem correta; remova os pacotes de codificação que você não deseja usar.

Certifique-se de que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou `TLS_ECDHE_RSA_WITH_AES_12` precede qualquer pacote de codificação `TLS_DHE_`.

No Microsoft MSDN, consulte também Prioritizing Schannel Cipher Suites.

Alterar portas HTTP ou HTTPS

Por padrão, o XML Service no Controller escuta a porta 80 para o tráfego HTTP e a porta 443 para o tráfego HTTPS. Embora você possa usar portas não padrão, esteja ciente dos riscos de segurança de expor um Controller a redes não confiáveis. É preferível implantar um servidor StoreFront autônomo do que 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 o tráfego HTTP e `<https-port>` é o número da porta para o tráfego HTTPS.

> **Nota:**
>
> Depois de alterar uma porta, o Studio pode exibir uma mensagem sobre compatibilidade e atualização de licenças. Para resolver o problema, registre novamente as instâncias de serviço usando a seguinte sequência de cmdlet do PowerShell:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
    XML_HTTPS |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
<!--NeedCopy-->
```


Aplicar apenas tráfego HTTPS

Se você quiser que o XML Service ignore o tráfego HTTP, crie a seguinte configuração de registro em HKLM\Software\Citrix\DesktopServer\ no Controller e reinicie o Broker Service.

Para ignorar o tráfego HTTP, crie DWORD XmlServicesEnableNonSsl e defina como 0.

Há um valor DWORD de registro correspondente que você pode criar para ignorar o tráfego HTTPS: DWORD XmlServicesEnableSsl. Assegure-se de que não esteja definido como 0.

Configurações de TLS em VDAs

Um Grupo de Entrega não pode ter uma mistura de VDAs com TLS configurado e VDAs sem TLS configurado. Antes de configurar o TLS para um Grupo de Entrega, assegure-se de que já tenha configurado o TLS para todos os VDAs no Grupo de Entrega.

Quando você configura o TLS em VDAs, as permissões no certificado TLS instalado são alteradas, dando ao serviço ICA acesso de leitura à chave privada do certificado e informando o serviço ICA sobre:

- **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 nessa 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 seu uso do SSLv3 e reconfigure as implantações para remover o suporte para SSLv3 onde for apropriado. Consulte CTX200238.

  As versões do protocolo TLS suportadas seguem uma hierarquia (da mais baixa à mais alta): SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3. Especifique a versão mínima permitida; todas as conexões de protocolo que usam essa versão ou uma versão superior são permitidas.

  Por exemplo, se você especifica TLS 1.1 como a versão mínima, as conexões de protocolo TLS 1.1 e TLS 1.3 são permitidas. Se você especifica SSL 3.0 como a versão mínima, as conexões a todas as versões suportadas são permitidas. Se você especifica TLS 1.3 como a versão mínima, somente conexões TLS 1.3 são permitidas.

  DTLS 1.0 corresponde a TLS 1.1 e DTLS 1.3 corresponde a TLS 1.3.
- **Quais pacotes de codificação TLS permitir.**

Um pacote de codificação seleciona a criptografia que é usada para uma conexão. Clientes e VDAs podem suportar diferentes conjuntos de pacotes de codificação. Quando um cliente (aplicativo Citrix Workspace ou StoreFront) se conecta e envia uma lista de pacotes de codificação TLS suportados, o VDA faz a correspondência de um dos pacotes de codificação de cliente com um dos pacotes de codificação em sua própria lista de pacotes de codificação configurados e aceita a conexão. Se não houver um pacote de codificação correspondente, o VDA rejeita a conexão.

O VDA suporta três conjuntos de pacotes de codificação (também conhecidos como modos de conformidade): GOV (governo), COM (comercial) e ALL (todos). Os pacotes de codificação 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 pacotes de codificação em cada conjunto:

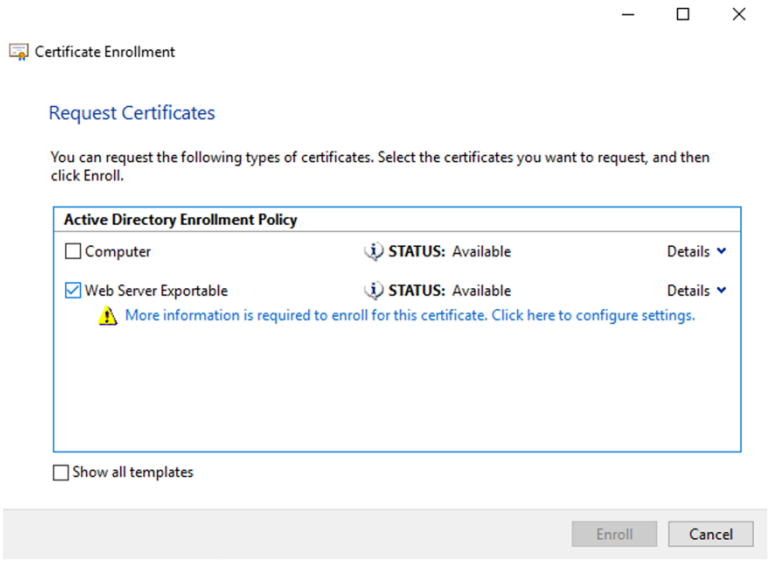
Pacote de codificação TLS/DTLS	**ALL**	**COM**	**GOV**	**ALL**	**COM**	**GOV**
Modo FIPS	Desativado	Desativado	Desativado	Ativado	Ativado	Ativado
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X		X	X	X	

* Não suportado no Windows Server 2012 R2.

> **Nota:**
>
> O VDA não oferece suporte a Pacotes de Codificação DHE (por exemplo, TLS_DHE_RSA_WITH_AES_256_GCM_SH 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, não podem ser usados pelo Receiver.
>
> Se você estiver usando um Citrix Gateway, consulte a documentação do Citrix ADC para obter informações sobre o suporte a pacotes de codificação para comunicação de back-end. Para obter informações sobre o suporte o pacote de codificação TLS, consulte Ciphers available on the Citrix ADC appliances. Para obter informações sobre o suporte ao pacote de codificação DTLS, consulte DTLS cipher support.

Solicitar e instalar um certificado

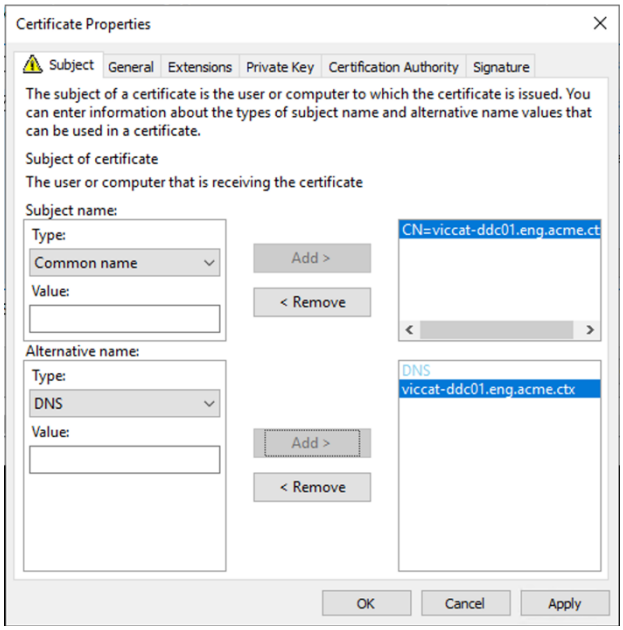
1. No VDA, abra o console MMC e adicione o snap-in Certificates. Quando solicitado, selecione Conta de computador.
2. Expanda **Pessoal > Certificates** e use o comando de menu de contexto **Todas as tarefas > Solicitar novo certificado**.
3. Clique em **Avançar** para começar e, depois, clique em **Avançar** para confirmar que você está adquirindo o certificado no registro do Active Directory.
4. Selecione o modelo para o certificado de autenticação do servidor. Tanto **Computer** quanto **Web Server Exportable**, padrão Windows, são aceitáveis. Se o modelo tiver sido configurado para fornecer automaticamente os valores para Subject, você pode clicar em **Enroll** sem fornecer mais detalhes.



5. Para fornecer mais detalhes para o modelo de certificado, clique em **Details** e configure o seguinte:

   Subject name —selecione o tipo **Common name** e adicione o FQDN do VDA

   Alternative name —selecione o tipo **DNS** e adicione o FQDN do VDA

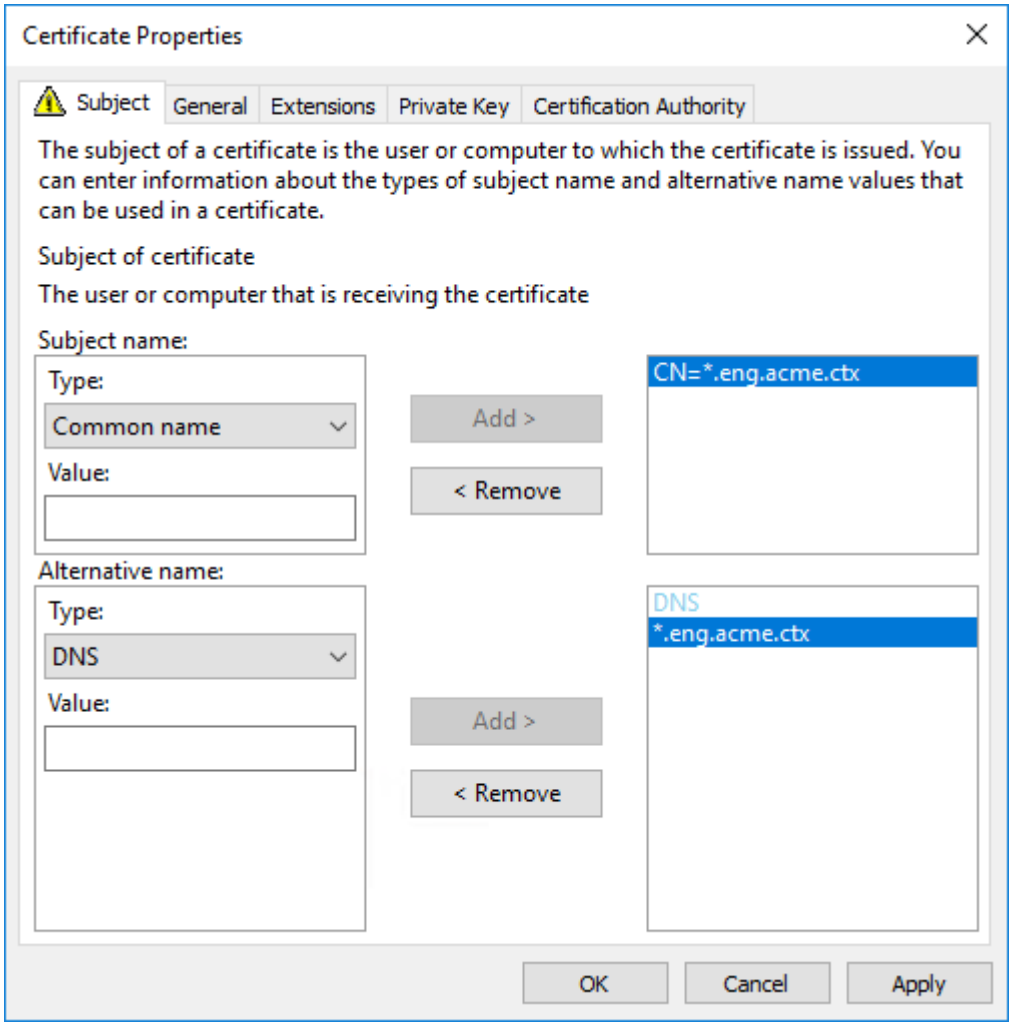


> **Nota:**
>
> Use o registro automático do certificado dos Serviços de Certificados do Active Directory para automatizar a emissão e implantação de certificados nos VDAs. Isso está descrito em https://support.citrix.com/article/CTX205473.

Você pode usar certificados curinga para permitir que um único certificado proteja vários VDAs:

Subject name —selecione o tipo **Common name** e insira *.domínio.primário dos VDAs

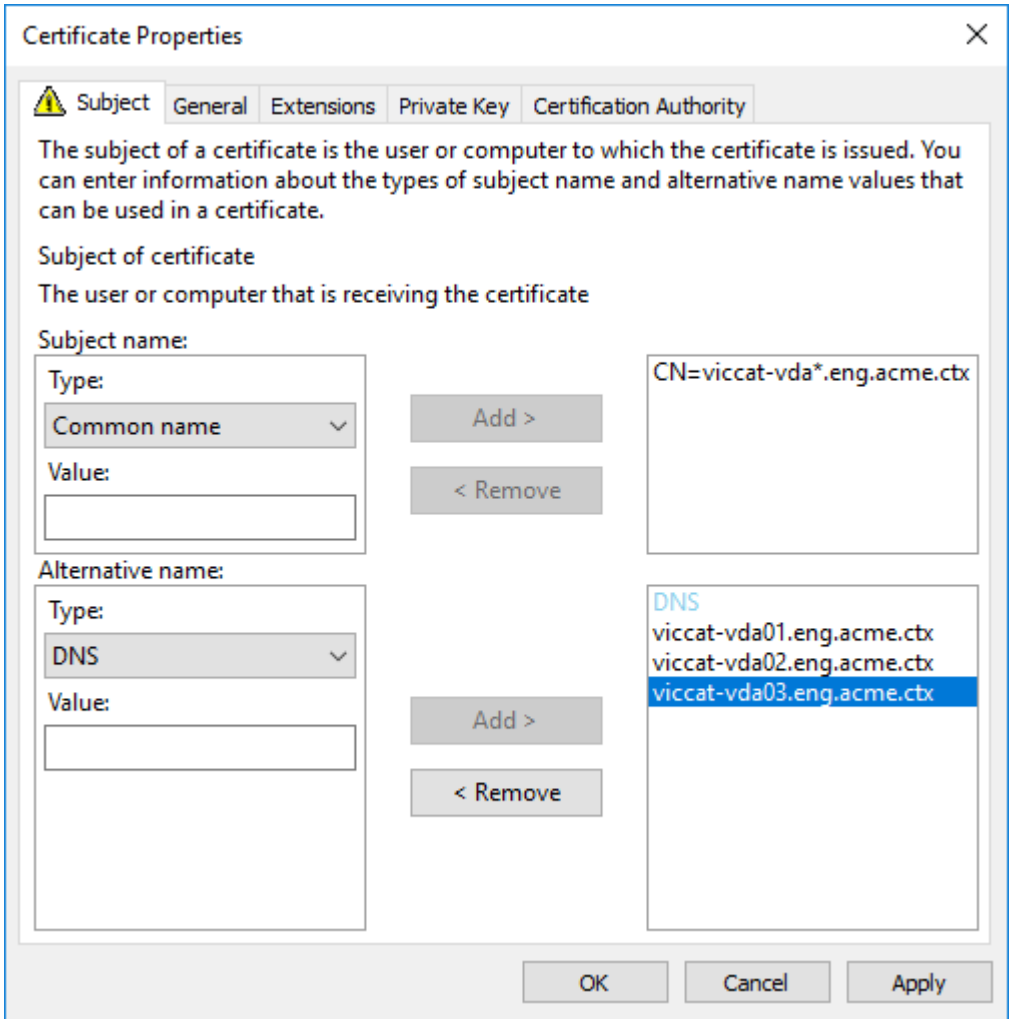
Alternative name —selecione o tipo **DNS** e adicione *.domínio.primário dos VDAs



Você pode usar certificados SAN para permitir que um único certificado proteja vários VDAs específicos:

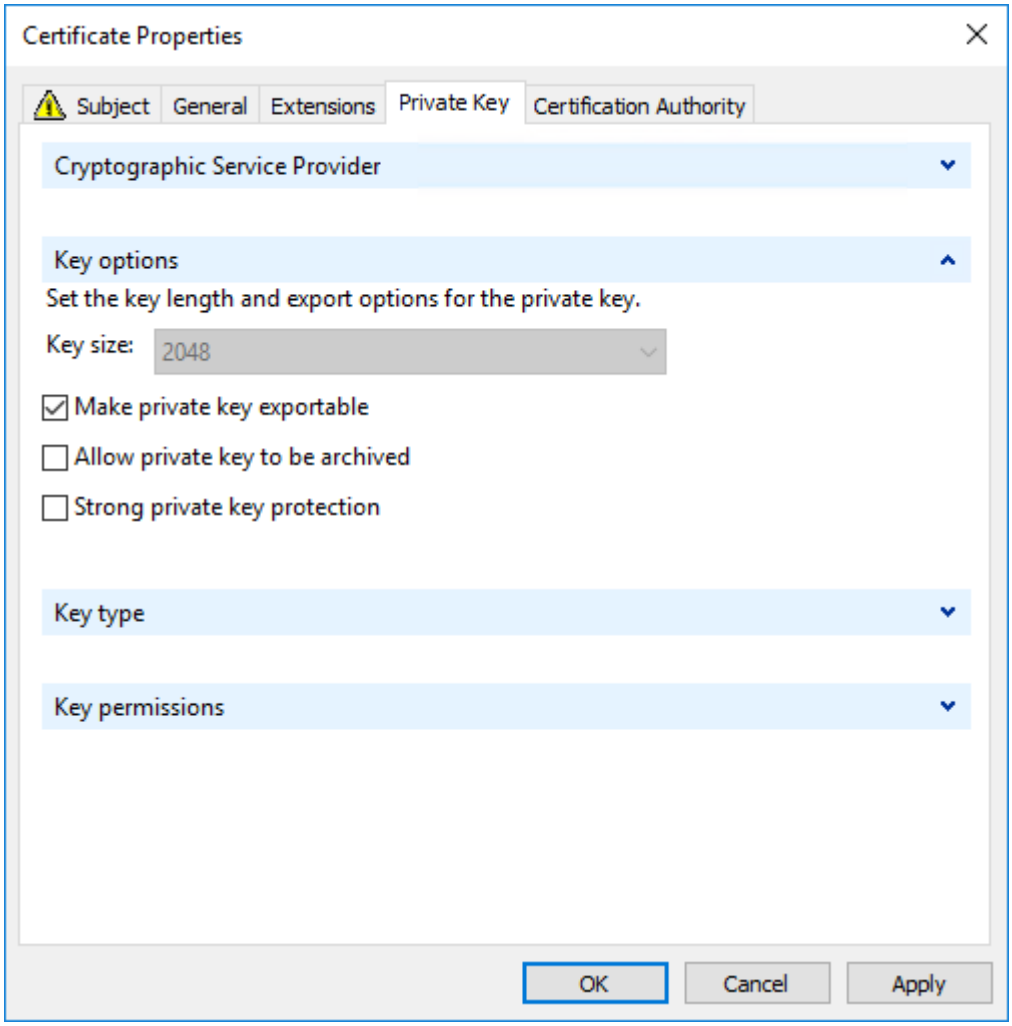
Subject name —selecione o tipo **Common name** e insira uma cadeia de caracteres para ajudar a identificar o ouso do certificado

Alternative name —selecione o tipo **DNS** e adicione uma entrada para o FQDN de cada VDA. Mantenha o número de Alternative Names a um mínimo para garantir a negociação ideal de TLS.



Nota:

Os certificados curinga e SAN exigem que **Tornar a chave privada exportável**, na guia Chave Privada, esteja selecionado:



Configurar o TLS em um VDA usando o script do PowerShell

Instale o certificado TLS na área de armazenamento de certificados: Computador local > Pessoal > Certificates. Se mais de um certificado residir nesse local, forneça a impressão digital do certificado para o script do PowerShell.

> **Nota:**
>
> Começando com XenApp e XenDesktop 7.16 LTSR, o script do PowerShell localiza o certificado correto com base no FQDN do VDA. Você não precisa fornecer a impressão digital quando somente um único certificado está presente para o VDA FQDN.

O script Enable-VdaSSL.ps1 ativa ou desativa o ouvinte TLS em um VDA. Esse script está disponível na pasta *Support* > *Tools* > *SslSupport* da mídia de instalação.

Quando você ativa o TLS, os pacotes de codificação DHE são desativados. Os pacotes de codificação ECDHE não são afetados.

Quando você habilita o TLS, o script desativa todas as regras de Firewall do Windows existentes da porta TCP especificada. Em seguida, adiciona uma nova regra que permite que o serviço ICA aceite conexões de entrada somente nas portas TLS TCP e UDP Também desativa as regras de Firewall do Windows para:

- Citrix ICA (padrão: 1494)
- Citrix CGP (padrão: 2598)
- Citrix WebSocket (padrão: 8008)

O resultado é que os usuários só podem se conectar usando TLS ou DTLS. Eles não podem usar ICA/HDX, ICA/HDX com confiabilidade de sessão ou HDX por WebSocket, sem TLS ou DTLS.

> **Nota:**
>
> O DTLS não é suportado com o ICA/HDX Audio por UDP Real-Time Transport ou com ICA/HDX Framehawk.

Consulte Portas de rede.

O script contém as seguintes descrições de sintaxe, além de exemplos extras; você pode usar uma ferramenta como o Notepad++ para revisar essas informações.

> **Importante:**
>
> Especifique o parâmetro Enable ou Disable e o parâmetro CertificateThumbPrint. Os outros parâmetros são opcionais.

Sintaxe `Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

Parâmetro	Descrição
Enable	Instala e habilita o ouvinte TLS no VDA. Esse parâmetro ou o parâmetro Disable é necessário.
Disable	Desabilita o ouvinte TLS no VDA. Esse parâmetro ou o parâmetro Enable é necessário. Se você especificar esse parâmetro, nenhum outro parâmetro será válido.

Parâmetro	Descrição
CertificateThumbPrint “”	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 esse parâmetro for omitido, um certificado incorreto será selecionado.
SSLPort	Porta TLS. Padrão: 443
SSLMinVersion “”	Versão mínima do protocolo TLS, entre aspas. Valores válidos: “TLS_1.0”(padrão), “TLS_1.1”e “TLS_1.3”.
SSLCipherSuite “”	Pacote de codificação 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 pacote de codificação GOV e o valor mínimo de protocolo TLS 1.2. A impressão digital (representada como “12345678987654321”neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.3"
-SSLCipherSuite "All"
```

O script a seguir desabilita o ouvinte TLS no VDA.

```
Enable-VdaSSL -Disable
```

Configurar manualmente o TLS em um VDA

Ao configurar o TLS em um VDA manualmente, você concede acesso de leitura genérico à chave privada do certificado TLS para o serviço apropriado em cada VDA: NT SERVICE\PorticaService, para VDA para SO Windows de sessão única, ou NT SERVICE\TermService para, VDA para SO Windows multissessão. No computador onde o VDA está instalado:

ETAPA 1. Inicie o Console de Gerenciamento Microsoft (MMC): Iniciar > Executar > mmc.exe.

ETAPA 2. Adicione o snap-in Certificates ao MMC:

1. Selecione Arquivo > Adicionar/remover snap-in.
2. Selecione Certificados e clique em Adicionar.
3. Quando a mensagem "Este snap-in sempre gerenciará certificados para:"for exibida, escolha "Conta de computador"e clique em Avançar.
4. Quando a mensagem "Selecione o computador a ser gerenciado pelo snap-in"for exibida, escolha "Computador local"e clique em Finalizar.

ETAPA 3. Em Certificates (Computador local) > Pessoal > Certificates, clique com o botão direito do mouse no certificado e selecione Todas as tarefas > Gerenciar chaves privadas.

ETAPA 4. O Editor de Listas de Controle de Acesso exibe "Permissões para chaves privadas de (FriendlyName)", onde (FriendlyName) é o nome do seu certificado TLS. Adicione um dos seguintes serviços e dê acesso de leitura a ele:

- Para VDA para SO de sessão única Windows, "PORTICASERVICE"
- Para VDA para SO multissessão Windows, "TERMSERVICE"

ETAPA 5. Clique duas vezes no certificado TLS instalado. Na caixa de diálogo do certificado, selecione a guia Detalhes e role para baixo. Clique em Impressão digital.

ETAPA 6. Execute regedit e vá para HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Edite a chave de impressão digital do SSL e copie o valor da impressão digital do certificado TLS para esse 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 mais tarde, altere o valor de DWORD para 0.)
3. Se você quiser alterar as configurações padrão (opcional), use o seguinte no mesmo caminho do registro:

   SSLPort DWORD —Número da porta SSL. Padrão: 443.

   SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.3. Padrão: 2 (TLS 1.0).

   SSLCipherSuite DWORD –1 = GOV, 2 = COM, 3 = ALL. Padrão: 3 (ALL).

ETAPA 7. Certifique-se de que as portas TLS TCP e UDP estejam abertas no Firewall do Windows se não forem o padrão 443. (Quando você cria a regra de entrada no Firewall do Windows, assegure que suas propriedades tenham as entradas "Permitir a conexão"e "Habilitada"selecionadas.)

ETAPA 8. Certifique-se de que nenhum outro aplicativo ou serviço (como o IIS) esteja usando a porta TLS TCP.

ETAPA 9. Para VDAs para SO multissessão Windows, reinicie o computador para que as alterações entrem em vigor. (Não é necessário reiniciar os computadores que contêm VDAs para SO de sessão única Windows.)

> **Importante:**
>
> Uma etapa extra é necessária quando o VDA está no Windows Server 2012 R2, Windows Server 2016, Windows 10 Anniversary Edition ou em uma versão mais recente suportada. Isso afeta as conexões do Citrix Receiver para Windows (versão 4.6 a 4.9), aplicativo Citrix Workspace para HTML5 e aplicativo Citrix Workspace para Chrome. Isso também inclui conexões usando o Citrix Gateway.
>
> Essa etapa também é necessária para todas as conexões usando 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, Windows 10 Anniversary Edition ou posterior), usando o Editor de Política de Grupo, vá para Configuração do Computador > Políticas > Modelos Administrativos > Rede > Definições de configuração de SSL > Ordem do Pacote de Codificação de SSL. Selecione na seguinte ordem:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Nota:**
>
> Os 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 essa configuração de Política de Grupo é configurada, o VDA seleciona um pacote de codificação somente se aparecer nas duas listas: lista de Política de Grupo e lista com o modo de conformidade selecionado (COM, GOV ou ALL). O pacote de codificação também deve aparecer na lista enviada pelo cliente (aplicativo Citrix Workspace ou StoreFront).

Essa configuração de política de grupo também afeta outros aplicativos e serviços TLS no VDA. Se seus aplicativos precisarem de pacotes de codificação específicos, será necessário adicioná-los à lista da Política de Grupo.

> **Importante:**
>
> Mesmo que as alterações na Política de Grupo sejam mostradas quando aplicadas, as alterações da Política de Grupo à configuração TLS só entram em vigor após a reinicialização do sistema op-

> eracional. Consequentemente, para áreas de trabalho em pool, aplique as alterações da Política de Grupo à configuração TLS para a imagem base.

Configurar TLS em Grupos de Entrega

Siga 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 de produtos Citrix.
3. Execute **Get-BrokerAccessPolicyRule -DesktopGroupName '*<nome-do-grupo-de-entrega>*' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Execute **Set-BrokerSite -DnsResolutionEnabled $true**.

Solução de problemas

Se ocorrer um erro de conexão, verifique o log de eventos do sistema no VDA.

Ao usar o aplicativo Citrix Workspace para Windows, se você receber um erro de conexão que indique um erro de TLS, desative o Desktop Viewer e tente conectar-se novamente. Embora a conexão ainda falhe, você poderá ver uma explicação do problema subjacente com o TLS. 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 bem com DTLS, incluindo aquelas que usam as versões mais recentes do aplicativo Citrix Workspace, Citrix Gateway e VDA. Algumas configurações que usam DTLS entre o aplicativo Citrix Workspace e o Citrix Gateway, e que usam DTLS entre o Citrix Gateway e o VDA, exigem ações adicionais.

Uma ação adicional é necessária se:

- a versão do Citrix Receiver suporta HDX Adaptive Transport e DTLS: Receiver para Windows (4.7, 4.8, 4.9), Receiver para Mac (12.5, 12.6, 12.7), Receiver para iOS (7.2, 7.3.x) ou Receiver para Linux (13.7)

e qualquer uma das seguintes condições ocorrer:

- a versão Citrix Gateway suporta DTLS para o VDA, mas a versão do VDA não suporta DTLS (versão 7.15 ou anterior),
- a versão do VDA suporta DTLS (versão 7.16 ou posterior), mas a versão do Citrix Gateway não suporta DTLS para o VDA.

Para evitar que as conexões do Citrix Receiver falhem, siga um destes procedimentos:

- atualize o Citrix Receiver para: Receiver para Windows versão 4.10 ou posterior, Receiver para Mac 12.8 ou posterior ou Receiver para iOS versão 7.5 ou posterior; ou
- atualize o Citrix Gateway para uma versão compatível com o DTLS para o VDA; ou
- atualize o VDA para a versão 7.16 ou posterior; ou
- desabilite o DTLS no VDA; ou
- desabilite o HDX Adaptive Transport.

> **Nota:**
>
> A atualização adequada para Receiver para Linux ainda não está disponível. O Receiver para Android (versão 3.12.3) não suporta HDX Adaptive Transport nem DTLS via Citrix Gateway, portanto, ele não é afetado.
>
> Para desabilitar o DTLS no VDA, altere a configuração do firewall do VDA para desabilitar a porta UDP 443. Consulte Portas de rede.

Comunicação entre o controlador e o VDA

A proteção no nível de mensagem do Windows Communication Framework (WCF) protege a comunicação entre o Controller e o VDA. Não é necessária proteção extra no nível de transporte usando TLS. A configuração 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.

Segundo a Microsoft, os protocolos de segurança utilizados pelo WCF estão em conformidade com os padrões da OASIS (Organization for the Advancement of Structured Information Standards), incluindo WS-SecurityPolicy 1.2. Além disso, a Microsoft afirma que o WCF suporta todos os conjuntos de algoritmos listados em Security Policy 1.2.

A comunicação entre o Controller e o VDA usa o conjunto de algoritmos basic256, cujos algoritmos são como indicado 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 Citrix HDX HTML5 Video Redirection Service em execução no VDA. Para isso, o serviço de redirecionamento de vídeo HTML5 gera dois certificados personalizados no armazenamento de certificados no VDA. Parar o serviço remove os certificados.

A política de redirecionamento de vídeo HTML5 é desativada por padrão.

O redirecionamento de conteúdo do navegador é habilitado por padrão.

Para obter mais informações sobre o redirecionamento de vídeo HTML5, consulte Configurações da política multimídia.

Protocolo TLS no servidor de impressão universal

June 28, 2023

O protocolo TLS (Transport Layer Security) é suportado para conexões baseadas em TCP entre o Virtual Delivery Agent (VDA) e o Servidor de impressão universal.

> **Aviso:**
>
> Nas tarefas que incluem trabalhar no registro do Windows, tenha muito cuidado: editar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

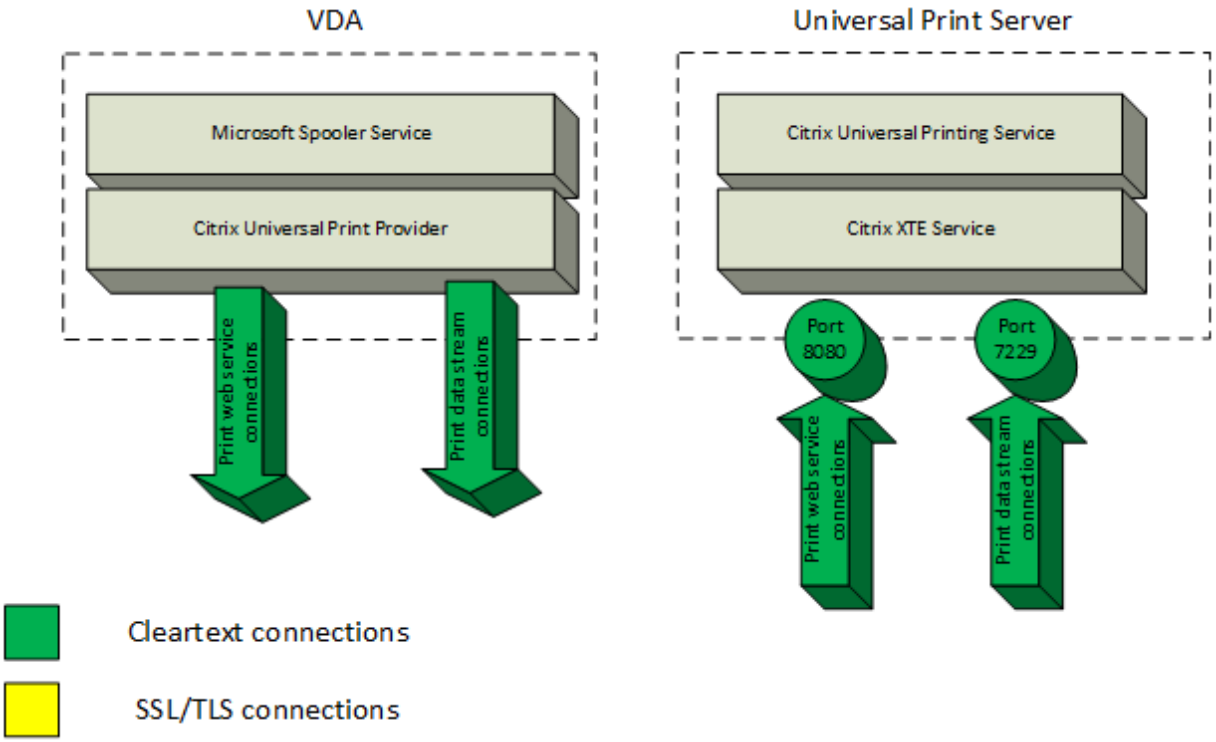
Tipos de conexões de impressão entre o VDA e o Servidor de impressão universal

Conexões de texto não criptografado

As seguintes conexões relacionadas à impressão são originadas no VDA e se conectam às portas no Servidor de impressão universal. Essas conexões são estabelecidas somente quando a configuração da política **SSL habilitado** é definida como **Desativado** (o padrão).

- Conexões de serviço Web de impressão de texto não criptografado (porta TCP 8080)
- Conexões de fluxo de dados de impressão (CGP) de texto não criptografado (porta TCP 7229)

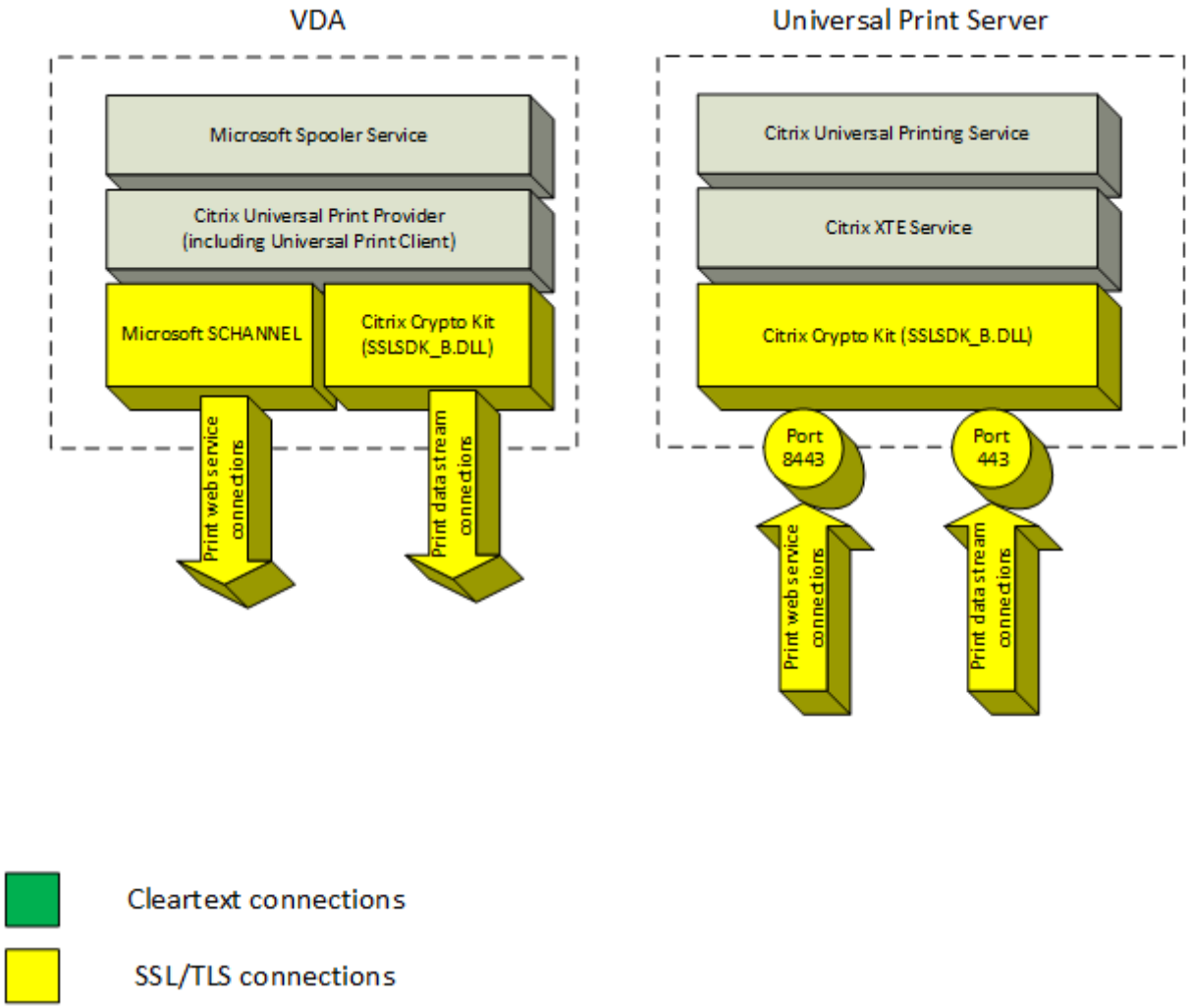
O artigo de suporte da Microsoft Visão geral do serviço e requisitos de porta de rede para Windows descreve as portas usadas pelo serviço de Spooler de Impressão do Microsoft Windows. As configurações SSL/TLS neste documento não se aplicam às conexões NETBIOS e RPC estabelecidas pelo serviço de Spooler de impressão do Windows. O VDA usa o Provedor de Impressão de Rede do Windows (win32spl.dll) como fallback se a configuração da política de **Ativação do Servidor de Impressão Universal** estiver definida como **Enabled with fallback to Windows'native remote printing**.



Conexões criptografadas

Essas conexões SSL/TLS relacionadas à impressão são originadas no VDA e se conectam às portas no Servidor de impressão universal. Essas conexões são estabelecidas somente quando a configuração de política **SSL habilitado** é definida como **Ativado**.

- Conexões de serviço Web de impressão criptografadas (porta TCP 8443)
- Conexões de fluxo de dados de impressão (CGP) criptografadas (porta TCP 443)



Configuração 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 nas conexões de serviço Web de impressão criptografadas (porta TCP 8443). O artigo de suporte da Microsoft Configurações do Registro do protocolo TLS descreve as configurações do registro para 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 > Definições de configuração de SSL > Ordem do Pacote de Codificação de SSL**. Selecione na seguinte ordem:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Nota:**
>
> Ao estabelecer esta configuração da política de grupo, o VDA seleciona um pacote de codificação de conexões de serviço Web de impressão criptografadas (porta padrão: 8443) somente se as conexões aparecerem nas duas listas do pacote de codificação SSL:
>
> - Lista ordenada de pacotes de codificação SSL da política de grupo
> - Lista correspondente à configuração da política do Pacote de codificação SSL selecionada (COM, GOV ou ALL)
>
> Essa configuração de política de grupo também afeta outros aplicativos e serviços TLS no VDA. Se seus aplicativos precisarem de pacotes de codificação específicos, será necessário adicioná-los à lista ordenada de pacotes de codificação da política de grupo.
>
> **Importante:**
>
> As alterações da política de grupo para a configuração TLS entram em vigor somente após a reinicialização do sistema operacional.
>
> Use uma política Citrix para definir as configurações SSL/TLS das conexões criptografadas de fluxo de dados de impressão (CGP) (porta TCP 443).

Configuração de servidor SSL/TLS

O Servidor de Impressão Universal funciona como o servidor SSL/TLS.

Use o script `Enable-UpsSsl.ps1` do PowerShell para definir as configurações SSL/TLS.

Instalar o certificado de servidor TLS no servidor de impressão universal

Para HTTPS, o servidor de impressão universal aceita recursos TLS usando certificados de servidor. Os certificados cliente não são usados. Use os Serviços de Certificados do Microsoft Active Directory ou outra autoridade de certificação para solicitar um certificado para o Servidor de Impressão Universal.

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 **pessoais** do computador local.

2. Configure o atributo de nome comum **Common Name** do DN (nome diferenciado) da entidade do certificado com o nome de domínio totalmente qualificado (FQDN) do Servidor de Impressão Universal. Especifique isso no modelo de certificado.
3. Defina o provedor de serviços de criptografia (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.

Configurar o SSL no servidor de impressão universal

O serviço XTE no servidor de impressão universal escuta as conexões de entrada. Ele funciona como um servidor SSL quando o SSL está habilitado. As conexões de entrada têm 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 desativado.

O script do PowerShell usado para configurar SSL está na mídia de instalação e tem este nome de arquivo: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

Configurar números de porta de escuta no servidor de impressão universal

Estas são portas padrão para o serviço XTE:

- Porta TCP de serviço Web de impressão de texto não criptografado (HTTP): 8080
- Porta TCP de fluxo de dados de impressão (CGP) de texto não criptografado: 7229
- Porta TCP de serviço Web de impressão criptografada (HTTPS): 8443
- Porta TCP de fluxo de dados de impressão criptografada (CGP): 443

Para alterar as portas usadas pelo serviço XTE no servidor de impressão universal, execute os seguintes comandos no PowerShell como administrador (consulte a seção a seguir para ler as observações sobre o uso do script do 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 servidor de impressão universal

Se você tiver vários servidores de impressão universal em uma configuração de balanceamento de carga, certifique-se de que as configurações TLS estejam configuradas de forma consistente em todos os servidores de impressão universal.

Quando você configura o TLS no servidor de impressão universal, as permissões no certificado TLS instalado são alteradas, dando ao serviço de impressão universal acesso de leitura à chave privada do certificado e informando o serviço universal de impressão sobre 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 para você quando você usa o script Enable-UpsSsl.ps1 do PowerShell.

- Quais versões do protocolo TLS permitir.

O servidor de impressão universal 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 pacotes de codificação TLS permitir.

Um pacote de codificação seleciona os algoritmos de criptografia que são usados para uma conexão. Os VDAs e o servidor de impressão universal podem suportar diferentes conjuntos de pacotes de codificação. Quando um VDA se conecta e envia uma lista de pacotes de codificação TLS suportados, o servidor de impressão universal faz a correspondência de um dos pacotes de codificação de cliente com um dos pacotes de codificação em sua própria lista de pacotes de codificação configurados e aceita a conexão. Se não houver um pacote de codificação correspondente, o servidor de impressão universal rejeita a conexão.

O servidor de impressão universal suporta os seguintes conjuntos de pacotes de codificação chamados GOV (governo), COM (comercial) e ALL (todos) para os modos OPEN, FIPS e os modos SP800-52 nativos do Crypto Kit. Os pacotes de codificação aceitáveis também dependem da configuração da política de **Modo SSL FIPS** e do modo FIPS do Windows. Consulte este artigo de suporte da Microsoft para obter informações sobre o modo FIPS do Windows.

Pacote de codificação (em ordem de prioridade decrescente)	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_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

Configurar o TLS em um servidor de impressão universal usando o script do PowerShell

Instale o certificado TLS na área de armazenamento de certificados: **Computador local > Pessoal > Certificates**. Se mais de um certificado residir nesse local, forneça a impressão digital do certificado para o script `Enable-UpsSsl.ps1` do PowerShell.

> **Nota:**
>
> O script do PowerShell encontra o certificado correto com base no FQDN do servidor de impressão universal. Você não precisa fornecer a impressão digital do certificado quando apenas um único certificado estiver presente para o FQDN do servidor de impressão universal.

O script `Enable-UpsSsl.ps1` ativa ou desativa as conexões TLS originadas no VDA para o servidor de impressão universal. Esse script está disponível na pasta **Support > Tools > SslSupport** da mídia de instalação.

Quando você habilita o TLS, o script desativa todas as regras de Firewall do Windows existentes das portas TCP do servidor de impressão universal. Em seguida, adiciona novas regras que permitem que o serviço XTE aceite conexões de entrada somente nas portas TLS TCP e UDP. Também desativa as regras de Firewall do Windows para:

- Conexões de serviço Web de impressão de texto não criptografado (padrão: 8080)
- Conexões de fluxo de dados de impressão (CGP) de texto não criptografado (padrão: 7229)

O efeito é que o VDA pode fazer essas conexões somente quando utiliza o TLS.

> **Nota:**
>
> Ativar o TLS não afeta as conexões RPC/SMB do Spooler de impressão do Windows originadas no VDA e que seguem para o servidor de impressão universal.
>
> **Importante:**
>
> Especifique **Enable** ou **Disable** como o primeiro parâmetro. O parâmetro CertificateThumbprint é opcional se apenas um certificado no armazenamento de certificados pessoais do computador local tiver o FQDN do servidor de impressão universal. Os outros parâmetros são opcionais.

Sintaxe

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

Parâmetro	Descrição
Enable	Habilita SSL/TLS no servidor XTE. Esse parâmetro ou o parâmetro Disable é necessário.
Disable	Desabilita SSL/TLS no servidor XTE. Esse parâmetro ou o parâmetro Enable é necessário.
CertificateThumbprint "<thumbprint>"	Impressão digital do certificado TLS no armazenamento de certificados pessoais do computador local, entre aspas. O script usa a impressão digital especificada para selecionar o certificado que você deseja usar.
HTTPPort <port>	Porta de serviço Web de impressão de texto não criptografado (HTTP/SOAP). Padrão: 8080
CGPPort <port>	Porta de fluxo de dados de impressão (CGP) de texto não criptografado. Padrão: 7229
HTTPSPort <port>	Porta de serviço Web de impressão criptografada (HTTPS/SOAP). Padrão: 8443
CGPSSLPort <port>	Porta de fluxo de dados de impressão criptografada (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.

Parâmetro	Descrição
SSLCipherSuite "<name>"	Nome do pacote de codificação TLS, entre aspas. Valores válidos: “GOV”, “COM”e “ALL”(padrão).
FIPSMode <Boolean>	Ativa ou desativa o modo FIPS 140 no servidor XTE. Valores válidos: $true para habilitar o modo FIPS 140, $false para desabilitar o modo FIPS 140.

Exemplos

O script a seguir habilita o TLS. A impressão digital (representada como “12345678987654321”neste exemplo) é usada para selecionar o certificado a ser usado.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

O script a seguir desabilita o TLS.

```
Enable-UpsSsl.ps1 –Disable
```

Configuração do modo FIPS

Habilitar o modo FIPS (Federal Information Processing Standards) dos EUA garante que apenas a criptografia compatível com FIPS 140 seja usada para conexões criptografadas do servidor de impressão universal.

Configure o modo FIPS no servidor antes de configurar o modo FIPS no cliente.

Consulte o site de documentação da Microsoft para habilitar/desabilitar o modo FIPS do Windows.

Habilitar o modo FIPS no cliente

No Delivery Controller, execute o Web Studio e defina a configuração da política **SSL FIPS Mode** da Citrix como **Enabled**. Habilite a política da Citrix.

Faça isso em cada VDA:

1. Habilite o modo FIPS do Windows.
2. Reinicie o VDA.

Habilitar o modo FIPS no servidor

Faça isso em cada servidor de impressão universal:

1. Habilite o modo FIPS do Windows.
2. Execute este comando do PowerShell como administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $true`.
4. Reinicie o servidor de impressão universal.

Desabilitar o modo FIPS no cliente

No Web Studio, defina a configuração da política **SSL FIPS Mode** da Citrix como **Disabled**. Habilite a política da Citrix. Você também pode excluir a configuração da política **SSL FIPS Mode** da Citrix.

Faça isso em cada VDA:

1. Desabilite o modo FIPS do Windows.
2. Reinicie o VDA.

Desabilitar o modo FIPS no servidor

Faça isso em cada servidor de impressão universal:

1. Desabilite o modo FIPS do Windows.
2. Execute este comando do PowerShell como administrador: `stop-service CitrixXTEServer, UpSvc`
3. Execute o script `Enable-UpsSsl.ps1` com os parâmetros `-Enable -FIPSMode $false`.
4. Reinicie o servidor de impressão universal.

Configurar a versão do protocolo SSL/TLS

A versão padrão do protocolo SSL/TLS é TLS 1.2. O TLS 1.2 é a única versão de protocolo SSL/TLS recomendada para uso em produção. Para a solução de problemas, pode ser necessário alterar temporariamente a versão do protocolo SSL/TLS para um ambiente que não seja de produção.

SSL 2.0 e SSL 3.0 não são suportados no servidor de impressão universal.

Definir a versão do protocolo SSL/TLS no servidor

Faça isso em cada servidor de impressão universal:

1. Execute este comando do 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 de testar.
3. Reinicie o servidor de impressão universal.

Definir a versão do protocolo SSL/TLS no cliente

Faça isso em cada VDA:

1. No Delivery Controller, defina a configuração da política de **SSL Protocol Version** como a versão desejada do protocolo e habilite a política.
2. O artigo de suporte da Microsoft Configurações do Registro do protocolo TLS descreve as configurações do registro para Microsoft SCHANNEL SSP. Habilite **TLS 1.0, TLS 1.1 ou TLS 1.2** do lado do cliente usando as configurações do registro.

   > **Importante:**
   >
   > Lembre-se de restaurar as configurações do registro para seus valores originais quando terminar o teste.

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 servidor de impressão universal.

A mensagem de erro **SSL handshake from client failed** aparece no arquivo de log se o handshake SSL/TLS falhar. Tais falhas podem ocorrer se as versões do protocolo SSL/TLS no VDA e no servidor de impressão universal não corresponderem.

Use o FQDN do Servidor de Impressão Universal nas seguintes configurações de política que contêm nomes de host do servidor de impressão universal:

- Session printers
- Printer assignments
- Universal Print Servers for load balancing

Assegure-se de que o clock do sistema (data, hora e fuso horário) esteja correto nos servidores de impressão universal e nos VDAs.

Segurança de canais virtuais

June 28, 2023

Por padrão, o recurso Virtual channel allow list está ativado. Como resultado, apenas os canais virtuais Citrix podem abrir nas sessões de aplicativos e áreas de trabalho virtuais. Se houver necessidade de usar canais virtuais personalizados, sejam eles internos ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

Adicionar canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa ter:

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`.

Quando tiver as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando as Configurações de política de lista de permissão de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, eles podem ser adicionados separados por vírgula.

Usando os exemplos anteriores, você adicionaria o seguinte à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Se houvesse vários processos, você adicionaria o seguinte à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

O uso de curingas (*) é suportado. Você pode usar caracteres curinga quando os nomes de diretórios ou executáveis forem alterados com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas para o seguinte:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application\*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`

- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application\*\run1.exe`
  - Não permitido: `C:\Program Files\*\run1.exe`
- As entradas devem conter a extensão do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2\*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2\*`
- Todos os caminhos devem ser locais. Caminhos de rede não são permitidos.

Considerações sobre o canal virtual Citrix

Todos os canais virtuais Citrix internos são confiáveis e podem ser abertos sem configurações extras. No entanto, existem dois recursos que exigem entradas explícitas na lista de permissões devido a dependências externas:

- Multimedia Redirection
- HDX RealTime Optimization Pack for Skype for Business

Multimedia Redirection

Esta informação é necessária para a entrada na lista de permissão:

- Nome do canal virtual: CTXMM
- Processo: caminho para o media player usado em sua máquina VDA. Por exemplo, C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- Entrada na lista de permissão: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

Esta informação é necessária para a entrada na lista de permissão:

- Nome do canal virtual: CTXRMEP
- Processo: caminho para o arquivo executável do Skype for Business na sua máquina VDA, que pode variar de acordo com a 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 na lista de permissão: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obtendo as informações diretamente do desenvolvedor ou fornecedor terceirizado que forneceu o canal virtual.

Como alternativa, essas informações podem ser obtidas aplicando os logs do recurso e seguindo estas etapas:

1. Quando os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou uma área de trabalho virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo no seguinte evento:
    - Em um VDA de sessão única, ID de evento 2002, origem Picadd.
    - Em um VDA multissessão, ID de evento 14, origem Rpm.
3. Faça logoff da sessão.
4. Adicione uma entrada na configuração da política de lista de permissão de canal virtual para o canal virtual identificado e o processo.
5. Inicie o aplicativo virtual ou a área de trabalho virtual para confirmar que o canal virtual personalizado é aberto com êxito.

Registro em log da lista de permissão do canal virtual

Os seguintes eventos são registrados no log de eventos da máquina VDA de sessão única:

Nome do log	System
Id	2001
Origem	Picadd
Nível	Informativo

	Descrição	O canal virtual personalizado <vcName> foi aberto pelo processo <processName>

	Nome do log	System
	Id	2002
	Origem	Picadd
	Nível	Aviso
	Descrição	O canal virtual personalizado <vcName> não pode ser aberto pelo processo <processName>

	Nome do log	System
	Id	2003
	Origem	Picadd
	Nível	Informativo
	Descrição	<username> abriu o canal virtual personalizado <vcName>

	Nome do log	System
	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 multissessão:

Nome do log	System
Id	13
Origem	Rpm
Nível	Informativo
Descrição	O canal virtual personalizado <vcName> foi aberto pelo processo <processName>

Nome do log	System
Id	14
Origem	Rpm
Nível	Aviso
Descrição	O canal virtual personalizado <vcName> não pode ser aberto pelo processo <processName>

Nome do log	System
Id	15
Origem	Rpm

	Nível	Informativo
	Descrição	<username> abriu o canal virtual personalizado <vcName>

	Nome do log	System
	Id	16
	Origem	Rpm
	Nível	Aviso
	Descrição	<username> tentou abrir o canal virtual personalizado <vcName>

Canais virtuais de terceiros conhecidos

A seguir, listamos as soluções de terceiros conhecidas que usam canais virtuais Citrix personalizados. Esta lista não inclui todas as soluções que usam um canal virtual Citrix personalizado.

- Cerner
- 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
- Zoom Meetings for VDI

Para obter detalhes sobre como adicionar os canais virtuais associados à lista de permissão, entre em contato com os fornecedores das soluções. Como alternativa, siga as etapas descritas na seção Obter nomes e processos de canais virtuais.

Transporte HDX

June 28, 2023

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

O HDX é projetado em torno de três princípios técnicos:

- Redirecionamento inteligente
- Compactação adaptativa
- Desduplicação de dados

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

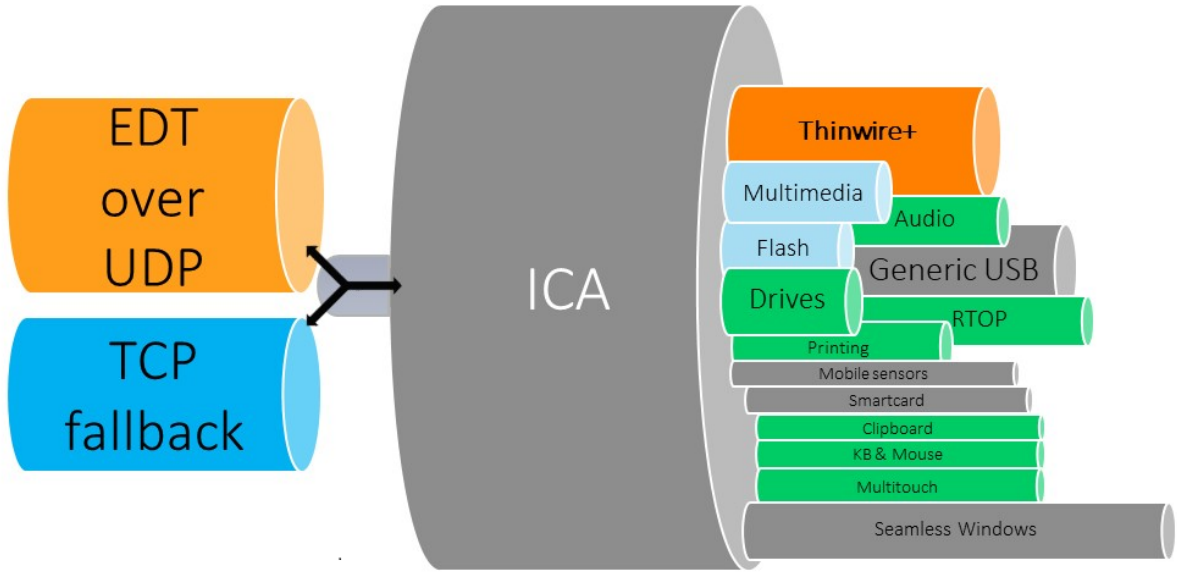
Na oferta HDX, você pode se conectar por meio de um protocolo de transporte exclusivo e proprietário, utilizar o máximo de unidades de transmissão ao estabelecer sessões e otimizar a conectividade com o Citrix SD-WAN.

Transporte adaptativo

June 28, 2023

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

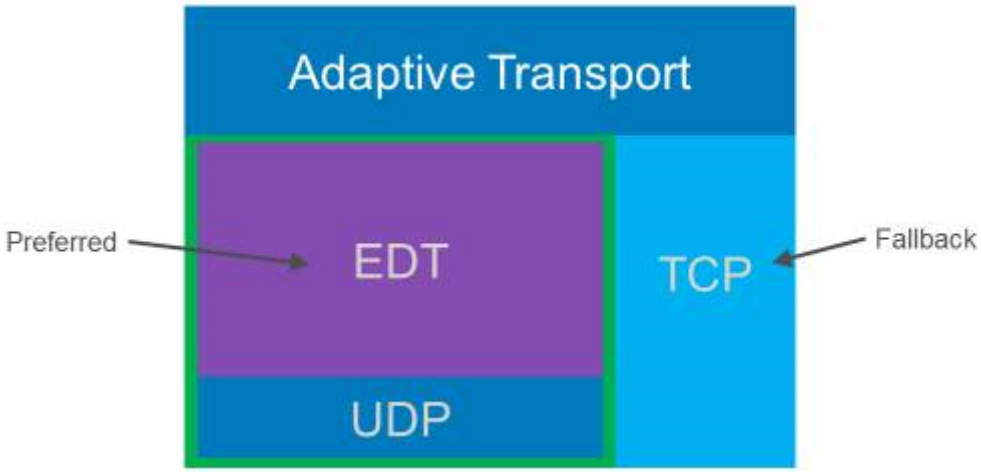
EDT é um protocolo de transporte proprietário da Citrix desenvolvido sobre o protocolo UDP (User Datagram Protocol). Ele oferece uma experiência de usuário superior em conexões mais difíceis de longo alcance, mantendo a escalabilidade do servidor. O EDT melhora a taxa de transferência de dados para todos os canais virtuais ICA em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.



Quando o transporte adaptativo é definido como **Preferred**, o EDT é usado como o protocolo de transporte primário e o TCP é usado para fallback. Por padrão, o transporte adaptativo é definido como **Preferred**. Você pode definir o transporte adaptativo para o **modo de diagnóstico** para fins de teste, o que permite apenas o EDT e desabilita o fallback para TCP.

Com o aplicativo Citrix Workspace para Windows, Mac e iOS, as conexões EDT e TCP são realizadas em paralelo durante a conexão inicial, a reconexão de confiabilidade da sessão e a reconexão automática de cliente. Isso reduz o tempo de conexão se o transporte UDP subjacente não estiver disponível e o TCP precisar ser usado em seu lugar. Se o transporte adaptativo estiver definido como **Preferred** e a conexão for estabelecida usando TCP, o transporte adaptativo continuará tentando alternar para EDT a cada cinco minutos.

Com o aplicativo Citrix Workspace para Linux e Android, as tentativas de conexões EDT são realizadas primeiro. Se a conexão não for bem-sucedida, o aplicativo Citrix Workspace tentará se conectar usando TCP depois que a solicitação EDT expirar.



Requisitos do sistema

A seguir estão os requisitos para usar o transporte adaptativo e EDT:

- Plano de controle
  - Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 1912 ou posterior
- Virtual Delivery Agent
  - Versão 1912 ou posterior (recomendado 2103 ou posterior)
  - A versão 2012 é o mínimo necessário 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 (recomendada 2105 ou posterior)
  - Linux: versão 1912 ou posterior (recomendada 2109 ou posterior)
  - Mac: Versão 1912 ou posterior (recomendada 2108 ou posterior)
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível na Google Play
- Citrix Gateway (ADC)
  - 13.0.52.24 ou posterior
  - 12.1.56.22 ou posterior
- Firewall (da perspectiva do VDA)

  - Entrada UDP 1494 —se a confiabilidade da sessão estiver desativada
  - Entrada UDP 2598 —se a confiabilidade da sessão estiver ativada
  - Entrada UDP 443 —se o VDA SSL estiver ativado para criptografia ICA (DTLS)
  - Saída UDP 443 —se estiver usando o Citrix Gateway Service. Para obter mais informações, consulte a documentação do Citrix Gateway Service.

Considerações

- Permita a confiabilidade da sessão para usar EDT MTU Discovery e usar o EDT com o Citrix Gateway e o Citrix Gateway Service.
- Certifique-se de que o EDT MTU esteja configurado adequadamente para evitar fragmentação. Caso contrário, o desempenho pode ser afetado ou as sessões podem não ser iniciadas em algumas situações. Para obter mais informações, consulte a seção Descoberta de MTU em EDT .
- Para obter detalhes sobre requisitos e considerações para usar o EDT com o Citrix Gateway Service, consulte HDX Adaptive Transport with EDT support for Citrix Gateway service.
- Para obter detalhes sobre a configuração do Citrix Gateway para oferecer suporte ao EDT, consulte Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight.
- Atualmente, o IPv6 não é suportado.

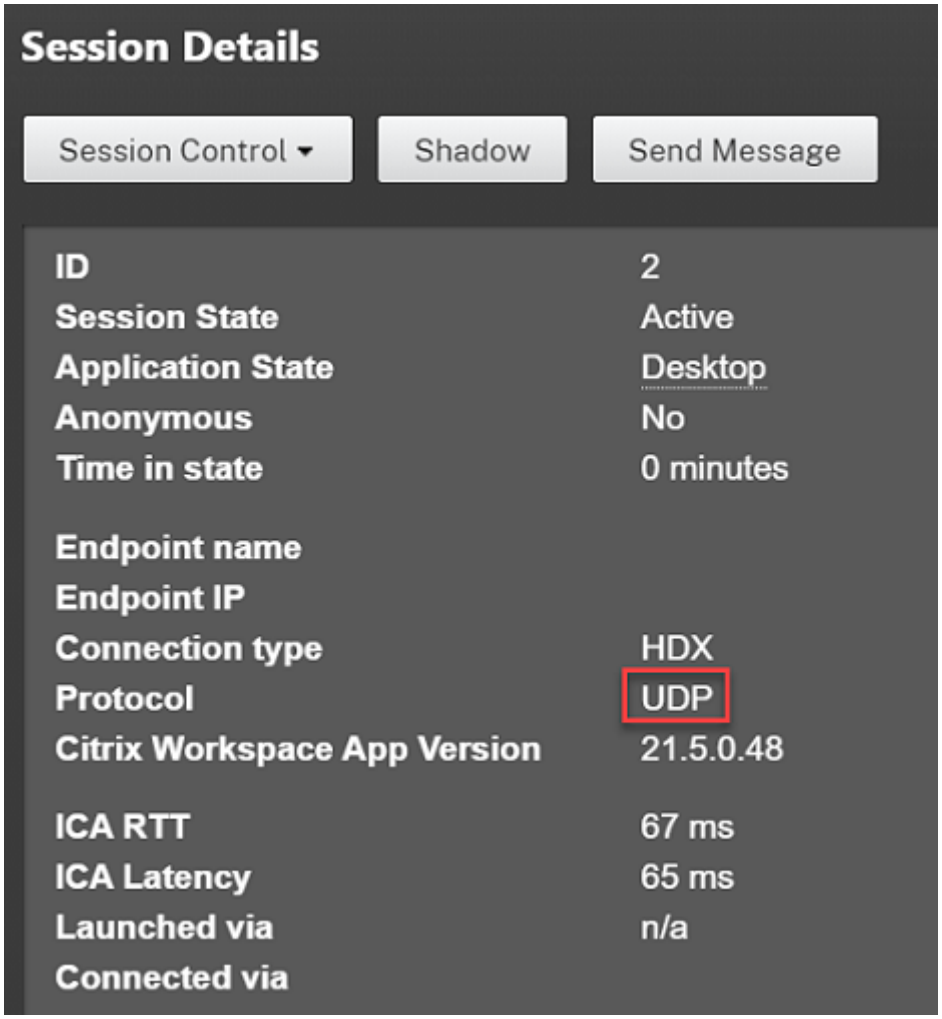
Configuração

O transporte adaptativo está habilitado por padrão. Você pode configurar as seguintes opções usando a configuração de **transporte adaptativo HDX** na política da Citrix.

- **Preferred**. Essa é a configuração padrão. O transporte adaptativo está ativado e usa o EDT como o protocolo de transporte preferido, com fallback para TCP.
- **Diagnostic mode**. O transporte adaptativo está ativado e força o uso do EDT. O fallback para TCP está desativado. Essa configuração é recomendada somente para testes e solução de problemas.
- **Off**. O transporte adaptativo está desativado e somente o TCP é usado para o transporte.

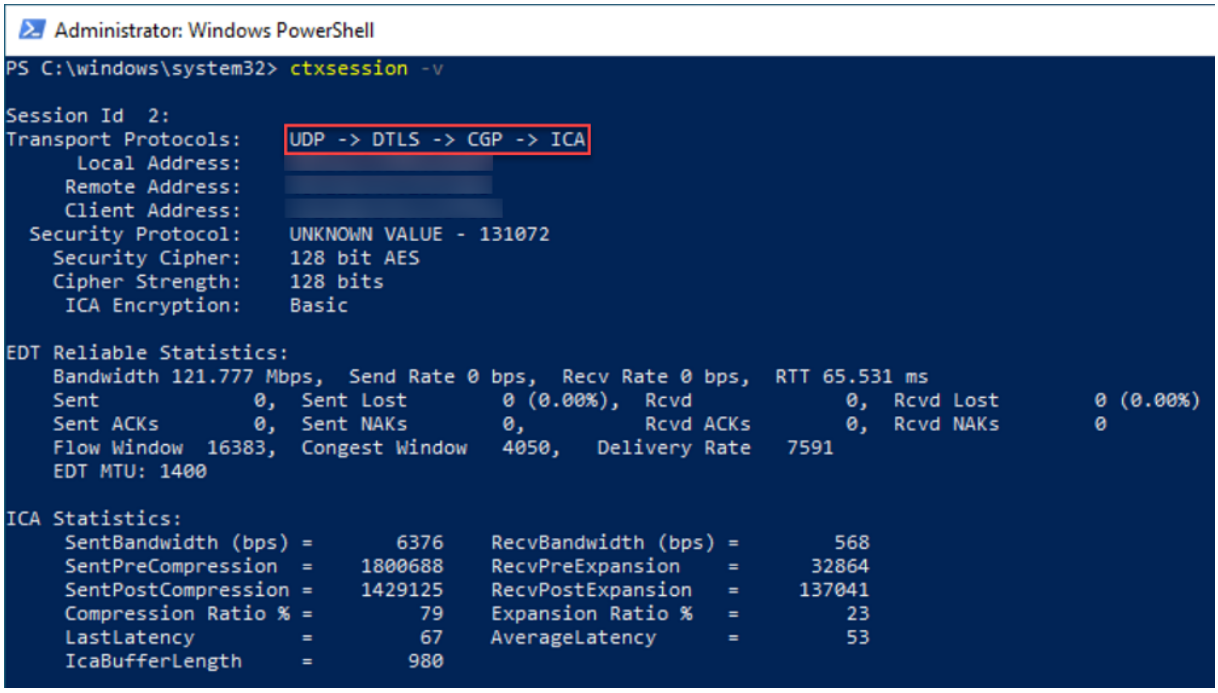
Para confirmar se o EDT está sendo usado como protocolo de transporte para a sessão, você pode usar o Director ou o utilitário de linha de comando CtxSession.exe no VDA.

No Director, procure a sessão e selecione **Details**. Se **Connection type** for **HDX** e **Protocol** for **UDP**, EDT está sendo usado como o protocolo de transporte para a sessão. Se **Connection type** for **RDP**, ICA não está em uso e **Protocol** exibe N/A. Para obter mais informações, consulte Monitorar sessões.



Para usar o utilitário CtxSession.exe, inicie um prompt de comando ou PowerShell dentro da sessão e execute `ctxsession.exe`. Para ver estatísticas detalhadas, execute `ctxsession.exe -v`. Se EDT estiver em uso, o protocolo de transporte mostra um dos seguintes:

- **UDP > ICA** (confiabilidade da sessão desativada)
- **UDP > CGP > ICA** (confiabilidade da sessão ativada)
- **UDP > DTLS > CGP > ICA** (ICA é criptografada por DTLS de ponta a ponta)



Descoberta de MTU em EDT

A descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso impede a fragmentação do pacote EDT que possa resultar em degradação de desempenho ou falha para estabelecer uma sessão.

Requisitos do sistema

- VDA com versão mínima 1912 (recomendado 2103 ou posterior)
- Aplicativo Citrix Workspace
  - Windows: versão 1912 ou posterior (recomendada 2105 ou posterior)
  - Mac: versão 2108 ou posterior
  - Linux: versão 2109 ou posterior
  - Android: versão 21.5 ou posterior
- Citrix ADC:
  - 13.1.17.42 ou posterior (recomendado)
  - 13.0.52.24 ou posterior
  - 12.1.56.22 ou posterior
- A confiabilidade da sessão deve estar ativada

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

> **Importante:**
>
> A descoberta de MTU não é suportada com o ICA multi-stream.

Para controlar a descoberta de MTU em EDT no VDA

A descoberta de MTU é ativada por padrão. Para desativar esse recurso, exclua o valor do registro e **EDT MTU Discovery** e reinicie o VDA. Para obter mais informações, consulte a configuração de EDT MTU Discovery na lista de recursos HDX gerenciados através do registro.

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

Loss tolerant mode

> **Importante:**
>
> - O recurso requer, no mínimo, o aplicativo Citrix Workspace 2002 para Windows.
> - O modo de tolerância a perdas não é suportado no Citrix Gateway ou no Citrix Gateway Service. Esse modo está disponível apenas com conexões diretas.

O modo de tolerância a perdas usa o protocolo de transporte EDT com perdas para melhorar a experiência dos usuários que se conectam através de redes com alta latência e perda de pacotes.

Inicialmente, as sessões são estabelecidas usando o EDT. Se os limites de latência e perda de pacotes forem alcançados ou ultrapassados, os canais virtuais aplicáveis passam do EDT para o EDT com perdas, deixando os outros canais virtuais no EDT. Se a latência e a perda de pacotes caírem abaixo dos limites, os canais virtuais aplicáveis voltam para o EDT.

Os limites padrão são:

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

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

Requisitos do sistema

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

Problemas conhecidos

Transporte adaptativo e EDT contêm os seguintes problemas:

- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha ao iniciar as sessões. Você pode ajustar o EDT MTU para evitar isso. Use a descoberta de MTU ou a solução alternativa descrita em CTX231821.
- Uma tela cinza ou preta pode aparecer ao iniciar uma sessão a partir de um cliente Windows se a descoberta de MTU estiver ativada. Para resolver esse problema, atualize para o aplicativo Workspace para Windows 2105, ou posterior, ou para o aplicativo Workspace para Windows 1912 CU4, ou posterior.
- O fallback para TCP pode falhar em clientes Linux e Android ao se conectar por meio do Citrix Gateway ou Citrix Gateway Service. Isso acontece quando há uma negociação EDT bem-sucedida entre o cliente e o Gateway, e a negociação EDT falha entre o Gateway e o VDA. Para resolver esse problema, atualize para o aplicativo Workspace para Linux 2104, ou posterior, e para o aplicativo Workspace para Android 21.5, ou posterior.
- Caminhos de rede assimétricos podem fazer com que a descoberta de MTU falhe nas conexões que não passam pelo Citrix Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para o VDA versão 2103 ou posterior. [CVADHELP-16654]
- Ao usar o Citrix Gateway, caminhos de rede assimétricos podem fazer com que a descoberta de MTU falhe. Isso se deve a um problema no Gateway que faz com que o bit DF (Don't Fragment) no cabeçalho dos pacotes EDT não seja propagado. Uma correção para esse problema está disponível a partir da versão de firmware 13.1 compilação 17.42. Para obter detalhes sobre como habilitar a correção, consulte a documentação do Citrix Gateway. [CGOP-18438]
- A descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não conseguem respeitar o bit DF quando o processamento de pacotes está ativado, impedindo que a descoberta de MTU detecte a fragmentação. Nessa situação, estas são as opções disponíveis:
  - Desativar o processamento de pacotes no modem do usuário.
  - Desativar a descoberta de MTU e usar uma MTU codificada conforme descrito em CTX231821.

- Desativar o transporte adaptativo para forçar as sessões a usarem o TCP. Se apenas um subconjunto de usuários for afetado, considere desativá-lo no lado do cliente para que outros usuários possam continuar a usar o EDT.

Solução de problemas

Para solucionar problemas de transporte adaptativo e EDT, sugerimos o seguinte:

1. Analise e valide minuciosamente os requisitos, considerações e problemas conhecidos.
2. Verifique se há políticas Citrix no Studio ou no objeto de política de grupo substituindo a configuração de **HDX Adaptive Transport** desejada.
3. Verifique se há configurações no cliente substituindo a configuração de HDX Adaptive Transport desejada. Pode ser uma preferência de GPO, uma configuração definida usando o modelo administrativo do aplicativo Workspace opcional ou uma configuração manual do parâmetro **HDXoverUDP** no registro ou no arquivo de configuração do cliente.
4. Em máquinas VDA multissessão, certifique-se de que os ouvintes UDP estão ativos. Abra um prompt de comando na máquina VDA e execute `netstat -a -p udp`. Para obter mais informações, consulte Como confirmar o protocolo HDX Enlightened Data Transport.
5. Inicie uma sessão direta internamente, ignorando o Citrix Gateway, e verifique o protocolo em uso. Se a sessão usar o EDT, o VDA estará pronto para usar o EDT para conexões externas por meio do Citrix Gateway.
6. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo Citrix Gateway:
   - Certifique-se de que a confiabilidade da sessão está ativada
   - Certifique-se de que o Gateway tenha o DTLS ativado
7. Verifique se as regras de firewall apropriadas foram configuradas nos firewalls de rede e nos firewalls em execução nas máquinas VDA.
8. Verifique se as conexões de usuários exigem uma MTU não padrão. Conexões com uma MTU efetiva inferior a 1500 bytes causam fragmentação de pacotes EDT, que, por sua vez, pode afetar o desempenho ou, até mesmo, causar falhas no início da sessão. Esse problema é comum ao usar VPN, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Para obter informações sobre como resolver esse problema, consulte a seção Descoberta de MTU em EDT.

Interoperabilidade com Citrix SD-WAN

A otimização WAN do Citrix SD-WAN (WANOP) oferece compactação indexada com token entre sessões (desduplicação de dados), incluindo cache de vídeo baseado em URL, e fornece redução significativa

da largura de banda. A redução ocorre se duas ou mais pessoas em um escritório assistir ao mesmo vídeo recuperado pelo cliente, ou transferir ou imprimir partes significativas do mesmo arquivo ou documento. Além disso, ao executar os processos de redução de dados ICA e compactação de trabalho de impressão no dispositivo da filial, a WANOP oferece descarregamento de CPU do servidor VDA e permite maior escalabilidade do servidor Citrix Virtual Apps and Desktops.

Atualmente, o SD-WAN WANOP não suporta EDT. No entanto, não há necessidade de desativar o transporte adaptativo se o SD-WAN WANOP estiver em uso. Quando um usuário inicia uma sessão que passa por uma SD-WAN com WANOP ativado, isso define a sessão automaticamente para usar TCP como protocolo de transporte. Sessões não WANOP continuam a usar o EDT sempre que possível.

HDX Direct (Preview técnico)

June 28, 2023

Ao acessar os recursos fornecidos pela Citrix, o HDX Direct permite que os dispositivos do cliente estabeleçam uma conexão direta segura com o VDA se houver uma linha de visão direta.

> **Importante:**
>
> O HDX Direct está atualmente na versão Preview técnica. Para enviar feedback ou relatar problemas, use este formulário.

Requisitos

A seguir estão os requisitos para usar o HDX Direct:

- Plano de controle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2303 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2303 ou posterior
- Aplicativo Workspace
  - Windows: versão 2303 ou posterior
- Nível de acesso
  - Citrix Workspace
  - Citrix Gateway Service

  - NetScaler Gateway

- Firewall
  - Máquina VDA
    - TCP 443 de entrada (ICA por TCP)
    - UDP 443 de entrada (ICA por EDT)
  - Rede

Protocolo	Porta	Origem	Destino
TCP	443	Cliente	VDA
UDP	443	Cliente	VDA

Configuração

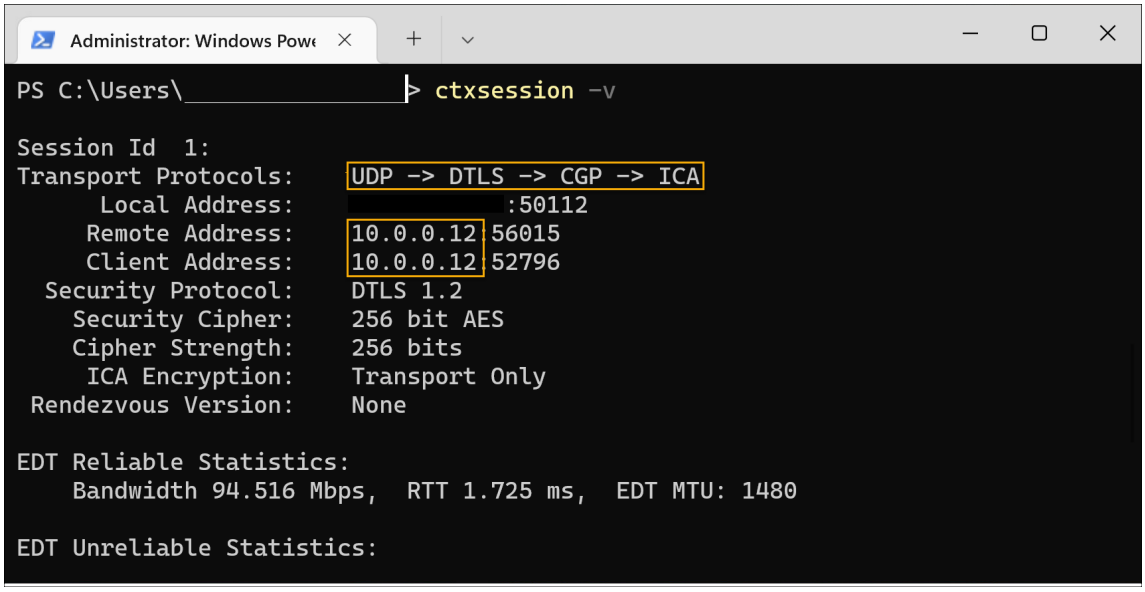
O HDX Direct está desativado por padrão. Você pode configurar esse recurso usando a configuração HDX Direct na política da Citrix.

- **Allowed**: o HDX Direct está ativado e tenta estabelecer uma conexão direta com o host da sessão quando uma sessão está conectada.
- **Prohibited**: a configuração padrão. O HDX Direct está desativado e impede que o cliente tente se conectar diretamente ao host da sessão quando conectado por meio de um Gateway.

Para confirmar que o HDX Direct estabeleceu com êxito uma conexão direta, use o utilitário CtxSession.exe na máquina VDA.

Para usar o utilitário CtxSession.exe, inicie um prompt de comando ou PowerShell dentro da sessão e execute ctxsession.exe -v. Se uma conexão HDX Direct foi estabelecida com sucesso, você verá o seguinte:

- Protocolo de transporte
  - UDP > DTLS > CGP > ICA (se estiver usando EDT)
  - TCP > SSL > CGP > ICA (se estiver usando TCP)
- O endereço remoto e o endereço do cliente são iguais



Considerações

A seguir estão algumas considerações sobre o uso do HDX Direct:

- Ao usar máquinas não persistentes para seus aplicativos e áreas de trabalho virtuais, não habilite o HDX Direct na imagem mestre/modelo para evitar gerar certificados para a máquina virtual (VM) mestre.

Como funciona

O HDX Direct permite que os clientes estabeleçam uma conexão direta com o host da sessão quando a comunicação direta está disponível. Quando as conexões diretas são feitas usando o HDX Direct, a criptografia em nível de rede (TLS/DTLS) é usada para protegê-las, aproveitando os certificados autoassinados.

Há três estágios que abrangem diferentes partes do recurso: pré-lançamento, lançamento e pós-lançamento.

Etapa de pré-lançamento

Esse é o estágio inicial, que abrange a criação e o gerenciamento de certificados. Essas tarefas são gerenciadas pelos seguintes serviços na máquina VDA, e são configuradas para serem executadas automaticamente na inicialização da máquina:

- Citrix ClxMtp Service: responsável pela geração e rotação do certificado CA.

- Citrix Certificate Manager Service: responsável por gerar e gerenciar o certificado CA raiz autoassinado, as chaves dos certificados da máquina e os certificados da máquina.

Veja a seguir uma visão geral do processo de gerenciamento de certificados:

1. Os serviços começam na inicialização da máquina.
2. O Citrix ClxMtp Service cria chaves se nenhuma tiver sido criada ainda.
3. O Citrix Certificate Manager Service verifica se o HDX Direct está ativado. Se não estiver, o serviço para sozinho.
4. Se o HDX Direct estiver ativado, o Citrix Certificate Manager Service verifica se há um certificado CA raiz autoassinado. Se não houver, é criado um certificado raiz autoassinado.
5. Quando um certificado CA raiz está disponível, o Citrix Certificate Manager Service verifica se há um certificado de máquina autoassinado. Se não houver, o serviço gera chaves e cria um novo certificado usando o FQDN da máquina.
6. Se houver um certificado de máquina existente criado pelo Citrix Certificate Manager Service e o nome do assunto não corresponder ao FQDN da máquina, um novo certificado será gerado.

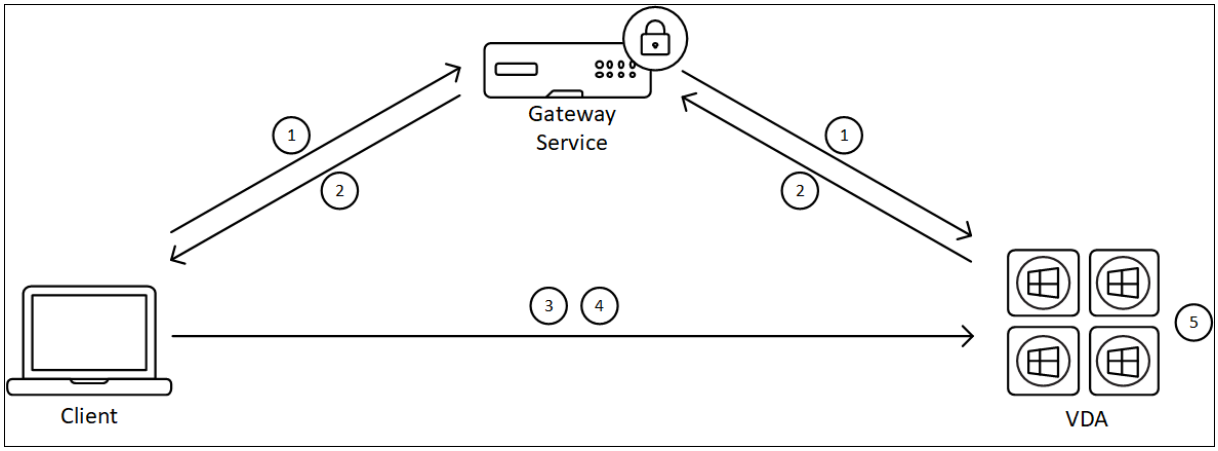
> **Nota:**
>
> O Citrix Certificate Manager Service gera certificados RSA que utilizam chaves de 2048 bits.

Etapa de lançamento

Para estabelecer com êxito uma conexão HDX Direct segura, o cliente deve confiar nos certificados usados para proteger a sessão. Para facilitar, o VDA envia suas informações de certificado ao agente quando uma sessão está sendo intermediada. Posteriormente, o agente envia essas informações ao Workspace para serem incluídas no arquivo ICA que é enviado ao cliente para iniciar a sessão.

Etapa pós-lançamento

Depois que uma sessão é intermediada com sucesso, a sessão é iniciada. A seguir você tem uma visão geral do processo de conexão HDX Direct:



1. O cliente estabelece uma conexão com o VDA por meio do Gateway Service.
2. Após uma conexão bem-sucedida, o VDA envia o FQDN da máquina VDA e uma lista de seus endereços IP para o cliente.
3. O cliente examina os endereços IP para ver se consegue acessar o VDA diretamente.
4. Se o cliente conseguir acessar o VDA diretamente com qualquer um dos endereços IP compartilhados, o cliente estabelecerá uma conexão direta segura com o VDA.
5. Quando a conexão direta é estabelecida com êxito, a sessão é transferida para a nova conexão, e a conexão com o Gateway Service é encerrada.

Problemas conhecidos

A seguir estão os problemas conhecidos com o HDX Direct:

- A conexão HDX Direct pode falhar quando o Rendezvous está desativado.
- A conexão HDX Direct pode falhar ao iniciar sessões a partir de um site do Citrix Virtual Apps and Desktops 2303 no local.
- O aplicativo Workspace pode falhar se o VDA estiver em execução no Windows 11.

Dispositivos

June 28, 2023

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 com tela de toque
- Dispositivos seriais

- Teclados especiais
- Dispositivos TWAIN
- Webcams
- Dispositivos WIA

Dispositivo USB otimizado x genérico

Um dispositivo USB otimizado é aquele para o qual o aplicativo Citrix Workspace tem suporte específico. Por exemplo, a capacidade de redirecionar webcams usando o canal virtual HDX Multimedia. Um dispositivo genérico é um dispositivo USB para o qual não há suporte específico no aplicativo Citrix Workspace.

Por padrão, o redirecionamento USB genérico não pode redirecionar dispositivos USB com suporte otimizado de canal virtual, a menos que seja colocado no modo Genérico.

Em geral, você obtém melhor desempenho para dispositivos USB no modo Otimizado do que no modo Genérico. No entanto, há casos em que um dispositivo USB não tem funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos recursos.

Com dispositivos USB de armazenamento em massa, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados pelas políticas da Citrix. As principais diferenças são:

Se o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estiverem ativados e um dispositivo de armazenamento em massa for inserido antes ou depois que uma sessão é iniciada, ele será redirecionado usando o mapeamento da unidade cliente.

Quando essas condições são verdadeiras, o dispositivo de armazenamento em massa é redirecionado usando o redirecionamento USB genérico:

- Tanto o redirecionamento USB genérico quanto as políticas de mapeamento da unidade cliente são ativados.
- Um dispositivo é configurado para redirecionamento automático.
- Um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão.

Para obter mais informações, consulte http://support.citrix.com/article/CTX123015.

Recurso	Client drive mapping	Redirecionamento USB genérico
Ativado por padrão	Sim	Não

Recurso	Client drive mapping	Redirecionamento USB genérico
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 oferecem suporte ao uso de diferentes DPIs entre monitores. Você pode verificar o DPI (% de dimensionamento) usando o Painel de Controle do Windows > Opções de exibição. Se estiver usando um dispositivo cliente Windows 8.1 ou Windows 10, habilitar a opção **Deixe-me escolher um nível de escala para todos os meus vídeos** no Painel de Controle do Windows > Opções de exibição configura os monitores adequadamente. Para obter mais informações, consulte o artigo do Knowledge Center CTX201696.

Unidades cliente mapeadas

Como precaução de segurança, quando um usuário faz logon no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades cliente sem a permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis residentes em unidades cliente mapeadas, substitua esse padrão editando o registro no servidor. Para obter informações sobre a configuração do registro, consulte Unidades cliente mapeadas na lista de recursos gerenciados por meio do registro.

O Citrix Virtual Apps and Desktops 7 2006 é a primeira versão que contém esse local de registro. Versões anteriores do Citrix Virtual Apps and Desktops usavam um local de registro diferente.

Dispositivos USB genéricos

June 28, 2023

A tecnologia HDX fornece **suporte otimizado** para a maioria dos dispositivos USB mais difundidos. Estes dispositivos incluem:

- Monitores
- Mouses

- Teclados
- Telefones VoIP
- Fones de ouvido
- Webcams
- Scanners
- Câmeras
- Impressoras
- Unidades
- Leitores de cartões inteligentes
- Tablets de desenho
- Mesas gráficas para assinatura

O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes de alta latência ou sensíveis à segurança.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não têm suporte otimizado ou quando esse é inadequado. Para obter mais informações sobre o redirecionamento USB genérico, consulte Redirecionamento USB genérico.

Para obter mais informações sobre dispositivos USB e o aplicativo Citrix Workspace para Windows, consulte Configuração do redirecionamento de dispositivo USB composto e [Configuração do suporte USB].(/en-us/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

Dispositivos móveis e com tela de toque

June 28, 2023

Modo tablet para dispositivos de tela sensível ao toque usando o Windows Continuum

O Continuum é um recurso do Windows 10 que se adapta à maneira como o dispositivo cliente é usado. Esta versão do suporte ao Continuum, incluindo a mudança dinâmica de modos, está disponível a partir do VDA versão 7.16 e Citrix Receiver para Windows versão 4.10.

O Windows 10 VDA detecta a presença de um teclado ou mouse em um cliente ativado por toque e coloca o cliente no modo desktop. Se não houver teclado nem mouse presentes, o Windows 10 VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão. Também ocorre na conexão ou desconexão dinâmica do teclado ou do mouse.

O recurso é ativado por padrão. Para desativar esta versão do recurso, edite as configurações de Tablet mode toggle policy settings no artigo de configurações de política do ICA.

Para a versão do recurso incluída no XenApp 7.14 e 7.15 LTSR e XenDesktop 7.14 e 7.15 LTSR, use as configurações do registro para desativar o recurso. Para obter mais informações, consulte Modo tablet para dispositivos de tela sensível ao toque.

O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores.
- A tela Iniciar e todos os aplicativos que você iniciar abrem em uma tela cheia.
- A barra de tarefas contém um botão de voltar.
- Ícones excluídos da barra de tarefas.

Você tem acesso ao Explorador de Arquivos.

O **modo desktop** oferece a interface de usuário tradicional onde você interage da mesma maneira que faz ao usar PC e um teclado e mouse.

O modo Tablet requer a versão mínima do Citrix Hypervisor 8.2 CU1 LTSR. O Citrix Hypervisor se integra ao Citrix Virtual Desktops VDA, alterando o Hypervisor para habilitar as configurações de firmware virtual para dispositivos 2 em 1. O Windows 10 carrega o driver GPIO no computador virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro do computador virtual.

O aplicativo Citrix Workspace para HTML5 (a versão light) não oferece suporte aos recursos do Windows Continuum.

Execute o comando XenServer CLI para permitir a comutação laptop/tablet:
xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

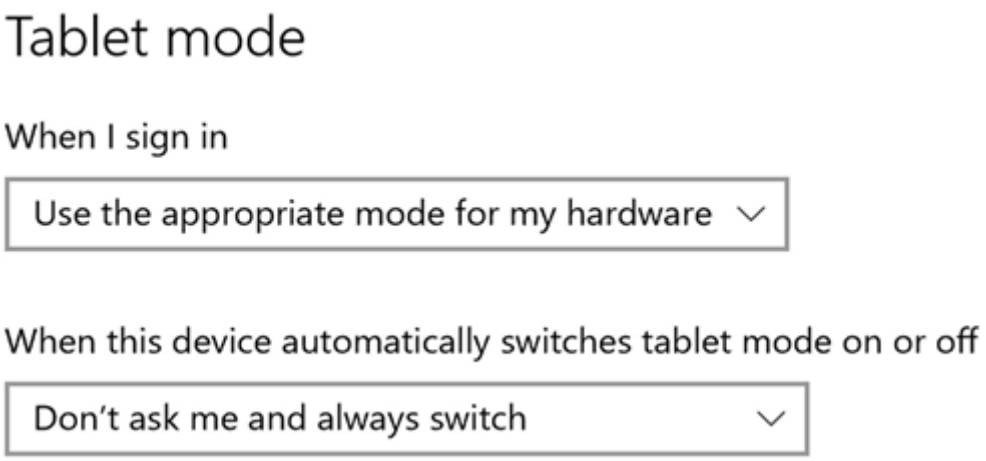
> **Importante:**
>
> A atualização da imagem base de um catálogo de máquinas existente após alterar a configuração de metadados não afeta nenhuma máquina virtual provisionada anteriormente. Depois de alterar a imagem base da VM do XenServer, crie um catálogo, escolha a imagem base e provisione uma nova máquina MCS (Machine Creation Services).

Antes de iniciar uma sessão:

Recomendamos que você navegue até **Settings > System > Tablet Mode** no VDA antes de iniciar uma sessão e defina as seguintes opções nos menus suspensos:

- Use the appropriate mode for my hardware
- Don't ask me and always switch

Se você não definir essas opções antes de iniciar a sessão, defina as opções depois de iniciar a sessão e reiniciar o VDA.



Canetas Microsoft Surface Pro e Surface Book

Apoiamos a funcionalidade padrão da caneta com aplicações baseadas em Windows Ink. Essa funcionalidade requer um Virtual Delivery Agent em execução em Microsoft Windows 10 versão 1809 no mínimo e dispositivos clientes usando o aplicativo Citrix Workspace para Windows versão 1902 no mínimo. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e modelo de caneta. Por exemplo, a pressão da caneta pode ser de até 4096 níveis. Esse recurso é ativado por padrão.

Para uma demonstração do Windows Ink e da funcionalidade da caneta, clique neste gráfico:

Requisitos do sistema

- Citrix Virtual Apps and Desktops: versão mínima 1903.
- Aplicativo Citrix Workspace para Windows versão mínima 1902
- Microsoft Windows 10 versão mínima 1809

Para desativar ou ativar esse recurso, consulte Canetas Microsoft Surface Pro e Surface Book na lista de recursos gerenciados pelo registro.

Portas seriais

June 28, 2023

A maioria dos PCs novos não tem portas seriais (COM) incorporadas. As portas são fáceis de adicionar usando conversores USB. Os aplicativos adequados para portas seriais geralmente envolvem sensores, controladores, leitores de cheques antigos, pads e assim por diante. Alguns dispositivos USB de porta COM virtual usam drivers específicos do fornecedor no lugar dos drivers fornecidos pelo Windows (usbser.sys). Esses drivers permitem que você force a porta COM virtual do dispositivo USB para que ele não mude mesmo se conectado a diferentes soquetes USB. Isto pode ser feito no **Gerenciador de dispositivos > Portas (COM e LPT) > Propriedades** ou no aplicativo que controla o dispositivo.

O mapeamento de porta COM do cliente permite que os dispositivos anexados às portas COM no ponto de extremidade do usuário sejam usados durante sessões virtuais. Você pode usar esses mapeamentos como qualquer outro mapeamento de rede.

Para cada porta COM, um driver no sistema operacional atribui um nome de link simbólico, como COM1 e COM2. Os aplicativos usam então o link para acessar a porta.

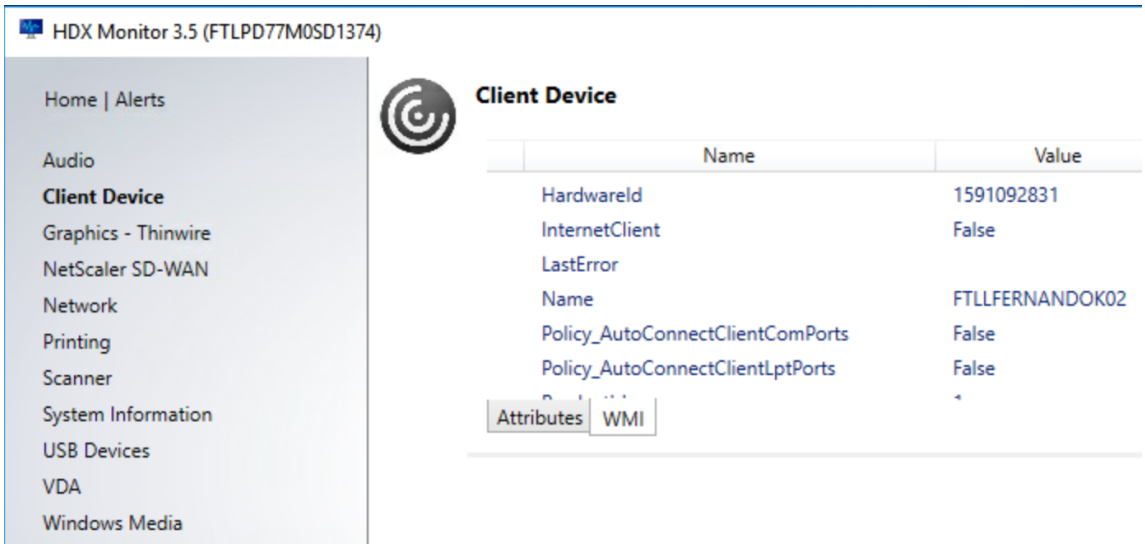
> **Importante:**
>
> Como um dispositivo pode se conectar ao ponto de extremidade usando USB diretamente, isso não significa que ele pode ser redirecionado usando o redirecionamento USB genérico. Alguns dispositivos USB funcionam como portas COM virtuais, os quais os aplicativos podem acessar da mesma maneira que a porta serial física. O sistema operacional pode abstrair portas COM e tratá-las como compartilhamentos de arquivos. Dois protocolos comuns para COM virtual são CDC ACM ou MCT. Quando conectado através de uma porta RS-485, os aplicativos podem não funcionar de todo. Obtenha um conversor de RS-485 em RS232 para usar o RS-485 como uma porta COM.
>
> **Importante:**
>
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um bloco de assinatura) consistentemente somente se ele estiver conectado a COM1 ou COM2 na estação de trabalho cliente.

Mapear uma porta COM do cliente para uma porta COM do servidor

Você pode mapear portas COM do cliente para uma sessão Citrix de três maneiras:

- Políticas do Studio. Para obter mais informações sobre políticas, consulte Configurações da política de redirecionamento de porta.
- Prompt de comando de VDA.
- Ferramenta de configuração de Área de Trabalho Remota (Serviços de Terminal).

1. Ative as políticas **Client COM port redirection** e **Auto connect client COM ports Studio**. Depois de aplicadas, algumas informações estão disponíveis no HDX Monitor.



2. Se a função **Auto connect client COM ports** não conseguir mapear a porta, você poderá mapear a porta manualmente ou usar scripts de logon. Faça logon no VDA, e em uma janela de prompt de comando, digite:

   NET USE COMX: \\CLIENT\COMZ:

   Ou

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   X é o número da porta COM no VDA (as portas 1 a 9 estão disponíveis para mapeamento). **Z** é o número da porta COM do cliente que você quer mapear.

   Para confirmar que a operação foi bem-sucedida, digite **NET USE** em um prompt de comando VDA. A lista que aparece contém unidades mapeadas, portas LPT e portas COM mapeadas.

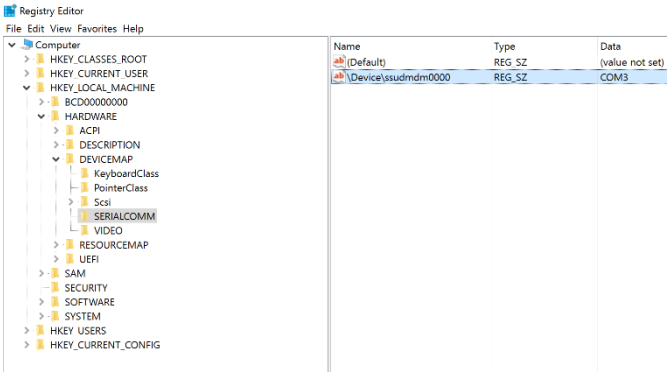
3. Para usar essa porta COM em uma área de trabalho virtual ou aplicativo, instale o aplicativo de dispositivo do usuário e aponte-o para o nome da porta COM mapeado. Por exemplo, se você mapear COM1 no cliente para COM3 no servidor, instale seu aplicativo de dispositivo de porta COM no VDA e aponte-o para COM3 durante a sessão. Use esta porta COM mapeada como você faria uma porta COM no dispositivo do usuário.

> **Importante:**
>
> O mapeamento de porta COM não é compatível com TAPI. Você não pode mapear dispositivos da Windows Telephony Application Programming Interface (TAPI) às portas COM do cliente. A TAPI define uma maneira padrão para que os aplicativos controlem funções telefônicas para chamadas de dados, fax e voz. A TAPI gerencia a sinalização, incluindo discagem, atendimento e término de chamadas. Além disso, serviços suplementares, como espera, transferência e chamadas em conferência.

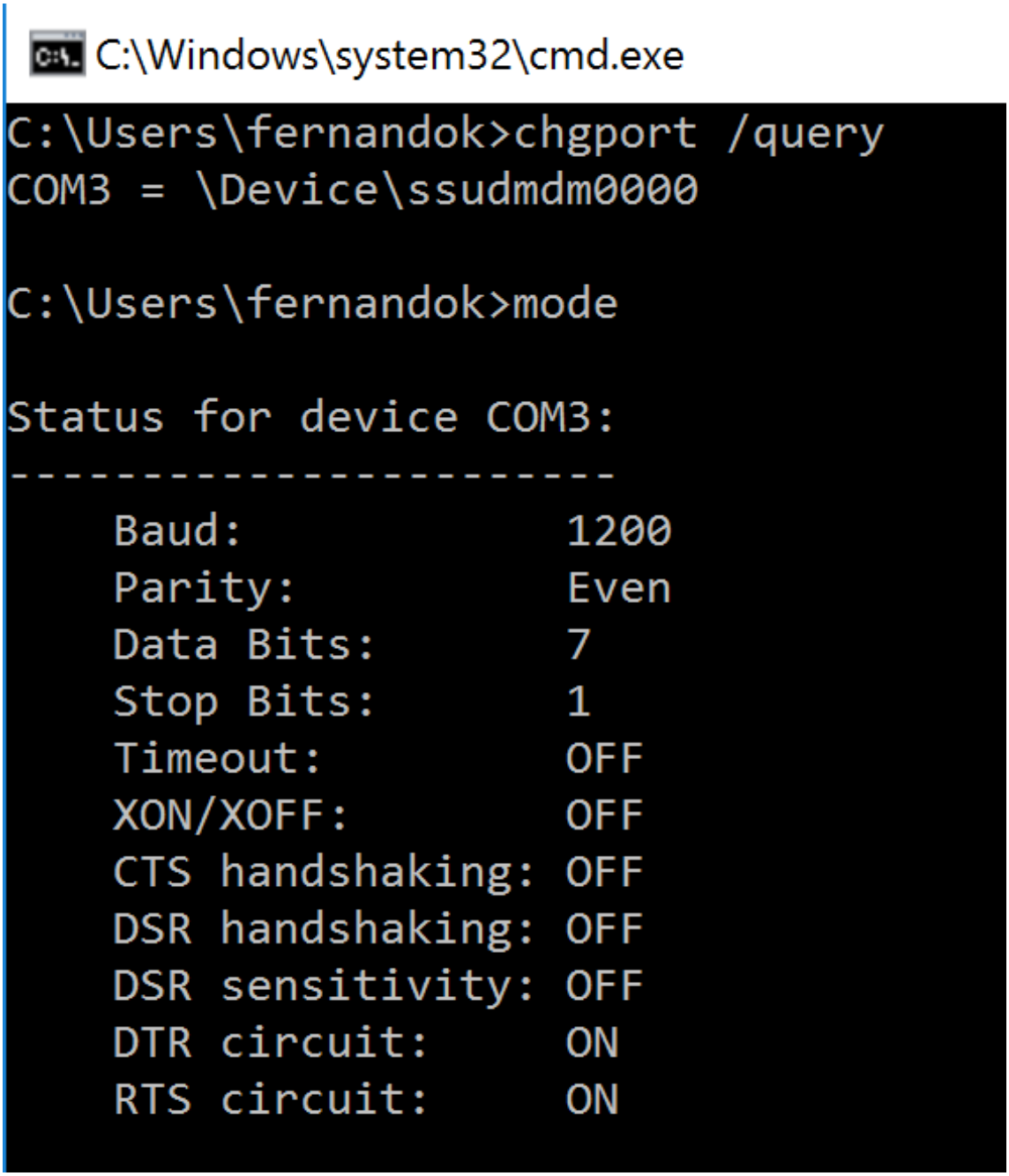
Solução de problemas

1. Você deverá ser capaz de acessar o dispositivo diretamente do ponto de extremidades, sem passar pelo Citrix. Embora a porta não seja mapeada para o VDA, você não está conectado a uma sessão Citrix. Siga todas as instruções de solução de problemas que acompanham o dispositivo e primeiro verifique se ele funciona localmente.
   Quando um dispositivo é conectado a uma porta COM serial, é criada uma chave de registro na

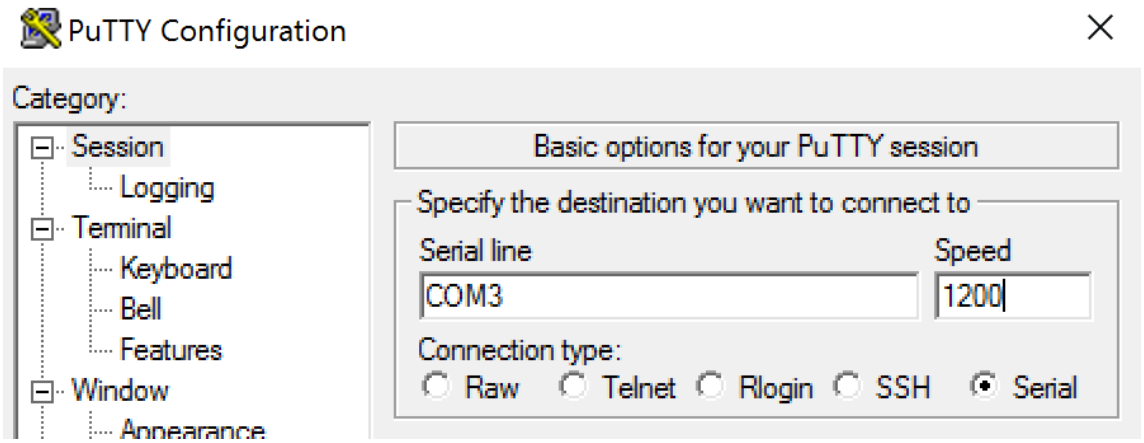
estrutura de registro mostrada aqui:



Você também pode encontrar essas informações no prompt de comando executando **chgport/-query**.



Se as instruções de solução de problemas do dispositivo não estiverem disponíveis, tente abrir uma sessão PuTTY. Escolha **Session** e em **Serial line** especifique sua porta COM.



Você pode executar **MODE** em uma janela de comando local. A saída pode indicar a porta COM em uso e os bits Baud/Parity/Data Bits/Stop, de que você precisa em sua sessão do PuTTY. Se a conexão PuTTY for bem-sucedida, pressione **Enter** para ver o feedback no dispositivo. Os caracteres que você digitar poderão ser repetidos na tela ou respondidos. Se esta etapa não for bem-sucedida, você não poderá acessar o dispositivo a partir de uma sessão virtual.

2. Mapeie a porta COM local para o VDA (usando políticas ou **NET USE COMX: \\CLIENT\COMZ:**) e repita os mesmos procedimentos do PuTTY na etapa anterior, mas desta vez no PuTTY do VDA. Se o PuTTY não mostrar o erro **Unable to open connection to COM1. Unable to open serial port**, outro dispositivo pode estar usando COM1.

3. Execute **chgport /query**. Se o driver serial do Windows integrado no VDA estiver atribuindo automaticamente \Device\Serial0 a uma porta COM1 do seu VDA, faça o seguinte:
   A. Abra o CMD no VDA e digite **NET USE.**

   B. Exclua todos os mapeamentos existentes (por exemplo, COM1) no VDA.

   NET USE COM1 /DELETE

   C. Mapeie o dispositivo para o VDA.

   NET USE COM1: \\CLIENT\COM3:

   D. Aponte o aplicativo no VDA para COM3.

   Por fim, tente mapear sua porta COM local (por exemplo, COM3) para uma porta COM diferente no VDA (que não seja a COM1, por exemplo, COM3). Verifique se o seu aplicativo está apontando para essa porta:
   NET USE COM3: \\CLIENT\COM3

4. Se você vir agora a porta mapeada, o PuTTY está funcionando, mas sem passar dados, pode ser uma condição de corrida. O aplicativo pode conectar e abrir a porta antes que ela seja mapeada, impedindo-a de ser mapeada. Experimente uma das seguintes soluções:

- Abra um segundo aplicativo publicado no mesmo servidor. Aguarde alguns segundos para que a porta seja mapeada e abra então o aplicativo real que tenta usar a porta.
- Ative as políticas de redirecionamento de porta COM do Editor de Política de Grupo no Active Directory em vez do Studio. Essas políticas são o **Client COM port redirection** e **Auto connect client COM ports**. As políticas aplicadas desta maneira podem ser processadas antes das políticas do Studio, garantindo que a porta COM seja mapeada. As políticas da Citrix são enviadas para o VDA e armazenadas em: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Use este script de logon para o usuário ou, em vez de publicar o aplicativo, publique um script.bat que primeiro exclua qualquer mapeamento no VDA, remapeie a porta COM virtual e, em seguida, inicie o aplicativo:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\ COM2:
MODE COM1: BAUD=1200 (ou qualquer valor necessário)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (ou qualquer valor necessário)
START C:\Program Files\<Caminho do seu software>\
```

5. O Process Monitor da Sysinternals é a ferramenta de último recurso. Ao executar a ferramenta no VDA, encontre e filtre objetos como COM3, picaser.sys, CdmRedirector, mas especialmente <seu_app>.exe. Podem aparecer erros como Acesso negado ou similares.

Teclados especiais

June 28, 2023

Teclados Bloomberg

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

O Citrix Virtual Apps and Desktops é compatível com o teclado Starboard Bloomberg modelo 5, modelo 4 (e o modelo 3 anterior). Este teclado apresenta características especiais que os clientes do setor financeiro usam para acessar dados do mercado financeiro e realizar as negociações rapidamente.

> **Importante:**
>
> Recomendamos que você use o teclado Bloomberg com apenas uma sessão. Não recomendamos usar o teclado com várias sessões simultâneas (um cliente para várias sessões).

O teclado Bloomberg é um dispositivo composto USB que compreende vários dispositivos USB em um mesmo compartimento físico:

- Teclado.
- Leitor de impressão digital.
- Dispositivo de áudio com teclas para aumentar e diminuir o volume e silenciar o alto-falante e o microfone. Este dispositivo inclui alto-falante integrado, microfone e tomada para o microfone e fone de ouvido.
- Hub USB para conectar todos esses dispositivos ao sistema.

Requisitos:

- A sessão à qual o aplicativo Citrix Workspace para Windows está se conectando deve oferecer suporte a dispositivos USB.
- Aplicativo Citrix Workspace 2207 para Linux, no mínimo, para oferecer suporte ao teclado Bloomberg modelo 5.
- Aplicativo Citrix Workspace 2109 para Windows, no mínimo, para oferecer suporte ao teclado Bloomberg modelo 5.
- Aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver para Windows 4.8, no mínimo, para oferecer suporte ao teclado Bloomberg modelo 3 e 4.
- Aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver for Windows 4.12, no mínimo, para usar o modo KVM (dois cabos USB com um roteado através do KVM) para o modelo 4.

Para obter informações sobre como configurar teclados Bloomberg no aplicativo Citrix Workspace para Windows, consulte Configurar teclados Bloomberg.

Para habilitar o suporte ao teclado Bloomberg, consulte Teclados Bloomberg na lista de recursos gerenciados por meio do registro.

Verifique o suporte:

Para determinar se o suporte ao teclado Bloomberg está habilitado no aplicativo Citrix Workspace, verifique se o Desktop Viewer relata corretamente os dispositivos do teclado Bloomberg.

Cenário de desktop:

Abra o Desktop Viewer. Se o suporte para o teclado Bloomberg estiver habilitado, o Desktop Viewer mostra três dispositivos sob o ícone USB:

Para o teclado Bloomberg 5:

- Módulo biométrico Bloomberg Bloomberg LP
- Teclado Bloomberg LP (dispositivo composto, com duas interfaces)
- Teclado com áudio Bloomberg LP (dispositivo composto, com três interfaces)

Para teclados Bloomberg 3 e 4:

- Scanner de impressão digital Bloomberg
- Características do teclado Bloomberg
- Teclado Bloomberg LP 2013

Cenário de aplicativo sem interrupção:

Abra o menu **Connection Center** no ícone da área de notificação do aplicativo Citrix Workspace. Se o suporte para o teclado Bloomberg estiver habilitado, os três dispositivos aparecerão no menu **Devices**.

A marca de seleção em cada um desses dispositivos indica que eles são remotos para a sessão.

Dispositivos TWAIN

June 28, 2023

Requisitos

- O scanner deve estar em conformidade com TWAIN.
- Instale os drivers TWAIN no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, através de USB).
- Verifique se o scanner está usando o driver TWAIN local e não o Serviço de Aquisição de Imagens do Windows.
- Verifique se não há nenhuma política aplicada à conta de usuário que é usada para o teste, e que esteja limitando a largura de banda dentro da sessão de ICA. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Para obter informações sobre as configurações de política, consulte Configurações da política de dispositivos TWAIN.

Webcams

June 28, 2023

Streaming de webcam de alta definição

Podem ser usadas webcams por aplicativos de videoconferência em execução dentro da sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão começa, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo de videoconferência. Quando a webcam e o aplicativo suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Damos suporte a resoluções de webcam até 1920x1080.

Esse recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para obter uma lista de plataformas de aplicativos Citrix Workspace que suportam o redirecionamento de webcam HDX, consulte Citrix Workspace app feature matrix.

Para obter mais informações sobre streaming de webcam de alta definição, consulte Videoconferência HDX e compactação de vídeo na webcam.

Você pode usar uma chave de registro para desativar e ativar o recurso e, em seguida, configurar uma resolução específica. Para obter informações, consulte Streaming de webcam de alta definição e Resolução de webcam de alta definição na lista de recursos gerenciados pelo registro.

Dispositivos WIA

June 28, 2023

Requisitos

- O scanner deve estar em conformidade com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, através de USB).
- Verifique se o scanner está usando o Serviço de Aquisição de Imagens do Windows local e não o driver TWAIN.
- Verifique se não há nenhuma política aplicada à conta de usuário que é usada para o teste, e que esteja limitando a largura de banda dentro da sessão de ICA. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Lista de permissões de aplicativos de Aquisição de Imagens do Windows

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento do scanner de Aquisição de Imagens do Windows. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém Aquisição de Imagens do Windows. Por padrão, nenhum aplicativo tem acesso a Aquisição de Imagens do Windows.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração de Lista de permissões de aplicativos de Aquisição de Imagens do Windows na lista de recursos gerenciados pelo registro.

Para obter informações sobre as configurações de política, consulte WIA devices policy settings.

Gráficos

June 28, 2023

Os elementos gráficos do Citrix HDX incluem um extenso conjunto de tecnologias de codificação e aceleração gráfica que otimiza a entrega de aplicativos gráficos avançados do Citrix Virtual Apps and Desktops. As tecnologias gráficas oferecem a mesma experiência de uso que de um desktop físico ao trabalhar remotamente com aplicativos virtuais com uso intensivo de gráficos.

Você pode usar software ou hardware para renderização gráfica. A renderização de software requer uma biblioteca de terceiros chamada software rasterizer. Por exemplo, o Windows inclui o WARP rasterizer para gráficos baseados em DirectX. Às vezes, você pode preferir usar um software renderer alternativo. A renderização de hardware (aceleração de hardware) requer um processador gráfico (GPU).

O HDX Graphics oferece uma configuração de codificação padrão otimizada para os casos de uso mais comuns. Ao usar as políticas da Citrix, os administradores de TI também podem definir várias configurações relacionadas a gráficos para atender a diferentes requisitos e oferecer a experiência desejada ao usuário.

Thinwire

Thinwire é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que os gráficos gerados em um computador sejam transmitidos, normalmente através de uma rede, para outro computador para exibição. Os gráficos são gerados como resultado de uma entrada do usuário, por exemplo, pressionamentos de teclas ou ações do mouse.

HDX 3D Pro

Os recursos do HDX 3D Pro no Citrix Virtual Apps and Desktops permitem que você forneça áreas de trabalho e aplicativos com melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta apenas a aceleração da GPU do DirectX.

Aceleração da GPU para SO Windows de sessão única

Usando o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de áreas de trabalho ou aplicativos hospedados em computadores com SO de sessão única. O HDX 3D Pro dá suporte a computadores host físicos (inclusive estações de trabalho desktop, blade e rack) e tecnologias de virtualização GPU e GPU Passthrough oferecidas pelo Citrix Hypervisor, vSphere e Hyper-V (somente passagem).

Usando GPU Passthrough, você pode criar VMs com acesso exclusivo a hardware dedicado de processamento gráfico. Você pode instalar várias GPUs no hipervisor e atribuir VMs a cada uma dessas GPUs individualmente.

Usando a virtualização da GPU, várias máquinas virtuais podem acessar diretamente o poder de processamento gráfico de uma única GPU física.

Aceleração da GPU para SO multissessão Windows

O HDX 3D Pro permite que aplicativos gráficos pesados em execução em sessões de SO multissessão Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não diminui a velocidade de processamento da CPU do servidor. Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não tem mais suporte. Em vez disso, use o Thinwire com o transporte adaptativo ativado.

Framehawk é uma tecnologia de exibição remota para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE). O Framehawk supera os desafios da interferência espectral e da propagação multipath e oferece uma experiência de usuário fluida e interativa aos usuários de áreas de trabalho e aplicativos virtuais.

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a deter e ativar o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um estorvo para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que seja uma camada de texto. A marca d'água pode ser exibida em toda a tela da sessão sem

alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte a VDA.

Informações correlatas

- HDX 3D Pro
- Aceleração da GPU para SO Windows de sessão única
- Aceleração da GPU para SO multissessão Windows
- Framehawk
- Thinwire
- Marca d'água de sessão baseada em texto

HDR (High Dynamic Range) de 10 bits

June 28, 2023

Com sessões de área de trabalho virtual de HDR de 10 bits, você pode usar recursos aprimorados de codificação e decodificação para renderizar imagens e vídeos de alta qualidade com uma ampla gama de cores e maior contraste e brilho. Além disso, você pode personalizar o nível de luminância branca, o EDID (Extended Display Identification Data) e a qualidade visual para melhorar a experiência do usuário.

Requisitos do sistema

Ponto de extremidade:

- Aplicativo Citrix Workspace para Windows 2209 ou posterior
- NVIDIA GPUs com suporte à decodificação HEVC de 10 bits no ponto de extremidade
- Monitores compatíveis com HDR de 10 bits

Servidor:

- VDA 2209 ou posterior com SO Windows de sessão única
- NVIDIA GPUs com suporte à codificação HEVC 444 de 10 bits no VDA

Políticas necessárias

Ponto de extremidade:

- Enable H.265 decoding for graphics

Servidor:

- Optimize for 3D Graphics workload
- Graphics Status Indicator (opcional)

Configurações do servidor

Quando você inicia uma sessão Citrix em um monitor de ponto de extremidade habilitado para HDR de 10 bits, a sessão HDR é habilitada por padrão. Em sessões HDR com vários monitores, todos os monitores de ponto de extremidade devem ter o HDR de 10 bits ativado. As sessões HDR são compatíveis com os modos de janela e tela inteira.

Nível de branco de referência

Essa configuração define o nível de luminância branca por valor nit. Ela controla o brilho relativo da tela HDR na sessão. O valor padrão é 80 nits. Defina a seguinte chave de registro para definir um valor nit diferente:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_DWORD
- Nome: RefWhiteLevel

Para ativar a configuração, você deve redimensionar sua sessão ou desconectá-la e reiniciá-la.

Substituição de EDID

Você pode configurar o VDA para usar o EDID do monitor de ponto de extremidade em suas sessões HDR. Isso permite que você aproveite ao máximo os recursos de exibição do monitor combinando a gama de cores e a faixa de luminância. Por padrão, as sessões HDR pressupõem uma tela com compatibilidade HDR1000.
Você pode exportar o EDID do monitor do ponto de extremidade usando NVIDIA ou outras ferramentas. Aplique-o ao VDA usando a seguinte chave de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_BINARY
- Nome: EDIDOverride

Quando você armazena o EDID no registro, ele não deve conter vírgulas, espaços ou caracteres especiais. Para ativar o EDID de substituição, faça logoff e inicie uma nova sessão.

Experiência visual sem perdas

Habilite as seguintes políticas para ter uma experiência visualmente sem perdas:

- Allow Visual Lossless Compression
- Visual Quality: Always Lossless ou Build to Lossless

Depois que as políticas forem definidas, você poderá controlar a qualidade da sessão HDR usando o indicador de Status Gráfico, no controle deslizante de Qualidade de Imagem, ou alternando para o modo de pixel perfeito.

Outras considerações

- Em GPUs virtuais, você pode iniciar sessões HDR de 10 bits em até quatro monitores.
- A sessão Citrix é revertida para o modo não HDR de 8 bits nas seguintes instâncias:
  - Se algum monitor de ponto de extremidade não tiver HDR de 10 bits habilitado
  - Ativar o compartilhamento de tela
  - Configurar um layout de exibição virtual no VDA
  - Mudar para o modo de pixel perfeito sem definir a política "Allow Visually Lossless Compression"

HDX 3D Pro

June 28, 2023

Os recursos do HDX 3D Pro no Citrix Virtual Apps and Desktops permitem que você forneça áreas de trabalho e aplicativos com melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta apenas a aceleração da GPU do DirectX.

Para obter as configurações de política HDX 3D Pro, consulte Optimize for 3D graphics workload.

Todos os aplicativos Citrix Workspace com suporte podem ser usados com gráficos 3D. Para obter o melhor desempenho com cargas de trabalho 3D complexas, monitores de alta resolução, configurações de vários monitores e aplicativos de alta taxa de quadros, recomendamos as versões mais recentes do aplicativo Citrix Workspace para Windows e Citrix Workspace para Linux. Para obter mais informações sobre versões compatíveis do aplicativo Citrix Workspace, consulte Lifecycle Milestones for Citrix Workspace app.

Exemplos de aplicações profissionais 3D incluem:

- Aplicações de design, fabricação e engenharia assistidas por computador (CAD/CAM/CAE)
- Software do Sistema de Informação Geográfica (SIG)
- Sistema de comunicação de arquivamento de imagens (PACS) para imagens médicas
- Aplicativos que usam as versões mais recentes OpenGL, DirectX, NVIDIA CUDA e OpenCL e WebGL
- Aplicativos não gráficos de uso intensivo computacional que usam GPUs NVIDIA Compute Unified Device Architecture (CUDA) para computação paralela

O HDX 3D Pro oferece a melhor experiência do usuário em qualquer largura de banda:

- Em conexões WAN: ofereça uma experiência de usuário interativa sobre conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de uma área de trabalho local em conexões LAN.

  Você pode substituir estações de trabalho complexas e caras por dispositivos de usuário mais simples movendo o processamento gráfico para o data center para gerenciamento centralizado.

HDX 3D Pro fornece aceleração de GPU para computadores com sistema operacional Windows de sessão única e computadores com sistema operacional Windows multissessão. Para obter mais informações, consulte Aceleração da GPU para SO Windows de sessão única and Aceleração da GPU para SO multissessão Windows.

HDX 3D Pro é compatível com as tecnologias de passagem de GPU e virtualização de GPU oferecidas pelos seguintes Hypervisors, além do bare metal:

- Citrix Hypervisor
  - Passagem de GPU com NVIDIA GRID, AMD e Intel GVT-D
  - Virtualização de GPU com NVIDIA GRID, AMD e Intel GVT-g
  - Consulte a compatibilidade de hardware na Lista de compatibilidade de hardware do Hypervisor.

Use a ferramenta HDX Monitor para validar a operação e a configuração das tecnologias de visualização HDX e para diagnosticar e solucionar problemas de HDX. A ferramenta está disponível na pasta **Support** na mídia de instalação do Citrix Virtual Apps and Desktops.

Aceleração da GPU para SO Windows multissessão

June 28, 2023

O HDX 3D Pro permite que aplicativos com muitos gráficos em execução em sessões de SO multissessão Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Movendo

a renderização do OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não diminui a velocidade de processamento da CPU do servidor. Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

Como o Windows Server é um sistema operacional multiusuário, vários usuários podem compartilhar uma GPU acessada pelo Citrix Virtual Apps sem a necessidade de virtualização de GPU (vGPU).

Em instruções que incluem a edição do registro, tenha cuidado: editar o registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Compartilhamento de GPU

O compartilhamento de GPU permite a renderização de hardware de GPU de aplicativos OpenGL e DirectX em sessões de área de trabalho remota. Tem as seguintes características:

- Pode ser usado em máquinas virtuais ou bare metal para aumentar a escalabilidade e o desempenho dos aplicativos.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não requer o desempenho de renderização de uma GPU dedicada).
- Não requer configurações especiais.

Uma GPU pode ser atribuída à máquina virtual do Windows Server nos modos de passagem completa ou de GPU virtual (vGPU) seguindo os requisitos do fornecedor do Hypervisor e da GPU. Implantações bare-metal em computadores físicos do Windows Server também têm suporte.

O compartilhamento de GPU não depende de nenhuma placa gráfica específica.

- Para máquinas virtuais, selecione uma placa gráfica compatível com o Hypervisor em uso. Para obter uma lista de compatibilidade de hardware do Citrix Hypervisor, consulte a Lista de compatibilidade de hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de exibição habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desative todas, exceto uma delas, usando o Gerenciador de Dispositivos.

A escalabilidade usando o compartilhamento de GPU depende de vários fatores:

- Os aplicativos que estão sendo executados
- A quantidade de RAM de vídeo que eles consomem
- O poder de processamento da placa gráfica

Alguns aplicativos lidam com escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha no driver da placa gráfica. Limite o número de usuários simultâneos para evitar esses problemas.

Para confirmar que a aceleração da GPU está ocorrendo, use uma ferramenta de terceiros, como GPU-Z. O GPU-Z está disponível em http://www.techpowerup.com/gpuz/.

- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso e permite o uso de codificação de hardware para codificação H.264 (quando disponível). Se tal hardware não estiver disponível, o VDA recorre à codificação baseada em CPU usando o codec de vídeo do software. Para obter mais informações, consulte Configurações da política de gráficos.

Renderização DirectX, Direct3D e WPF

As renderizações DirectX, Direct3D e WPF só estão disponíveis em servidores com uma GPU que dá suporte a uma versão de interface de driver de exibição (DDI) de 9ex, 10 ou 11.

- No Windows Server 2008 R2, o DirectX e o Direct3D não exigem configurações especiais para usar uma única GPU.
- No Windows Server 2012 e posteriores, as sessões de Serviços de Ambiente de Trabalho Remoto (RDS) no servidor Host de Sessão de Área de Trabalho Remota usam o Driver de Renderização Básico da Microsoft como o adaptador padrão. Para usar a GPU nas sessões do RDS no Windows Server 2012 e posterior, ative a configuração **Usar o adaptador gráfico padrão de hardware para todas as sessões dos Serviços de Área de Trabalho Remota** na política de grupo **Política do Computador Local** > **Configuração do Computador** > **Modelos Administrativos** > **Componentes do Windows** > **Serviços de Área de Trabalho Remota** > **Host da Sessão da Área de Trabalho Remota** > **Ambiente de Sessão Remota**
- Para permitir que os aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no Registro do servidor executando sessões do sistema operacional multisessão do Windows. Para obter informações sobre a configuração do Registro, consulte Windows Presentation Foundation (WPF) rendering na lista de recursos gerenciados por meio do registro.

Aceleração de GPU para aplicações CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desativada por padrão.

Para usar os recursos POC de aceleração CUDA, faça as configurações do registro. Para obter informações, consulte GPU acceleration for CUDA or OpenCL applications na lista de recursos gerenciados por meio do registro.

Aceleração da GPU para SO Windows de sessão única

June 28, 2023

Usando o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de áreas de trabalho ou aplicativos hospedados em computadores com SO de sessão única. O HDX 3D Pro dá suporte a computadores host físicos (inclusive estações de trabalho desktop, blade e rack) e tecnologias de virtualização GPU e GPU Passthrough oferecidas pelo Citrix Hypervisor, vSphere, Nutanix e Hyper-V (somente passagem).

HDX 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para um desempenho ideal de WAN e sem fio. HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como a técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que dão suporte a NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que dão suporte a NVENC.
- Opção de compressão sem perdas para casos de uso especializados. O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde são necessários gráficos perfeitos em pixels, como imagens médicas. A verdadeira compactação sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

  Ao usar compactação sem perdas:

  - O indicador de sem perdas, um ícone de área de notificação, notifica o usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração de política de **Visual Quality** especifica **Build to lossless**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.
  - O comutador sem perdas permite que o usuário mude ao modo sempre sem perdas a qualquer momento dentro da sessão. Para selecionar ou desmarcar **Lossless anytime within a session**, clique com o botão direito do mouse no ícone e clique em **Switch to pixel perfect** ou use o atalho ALT+SHIFT+1.

    Para compactação sem perdas: HDX 3D Pro usa o codec sem perdas para compactação, independentemente do codec selecionado através da política.

    Para compactação com perdas: HDX 3D Pro usa o codec original, o padrão ou o selecionado através da política.

    As configurações do comutador sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Always lossless** na configuração Política de **Visual quality**.

- Você pode substituir o atalho padrão, ALT+SHIFT+1, para selecionar ou desmarcar Lossless within a session. Defina uma nova configuração de registro em HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HD
  - Nome: HKEY_LOCAL_MACHINE_HotKey, Tipo: String
  - O formato para configurar uma combinação de atalhos é C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val. As chaves devem ser separadas por vírgula ",". A ordem das chaves não importa.
  - A, C, S, W e K são chaves, onde C=Control, A=ALT, S=SHIFT, W=Win e K=uma chave válida. Os valores permitidos para K são 0—9, a—z e qualquer código de chave virtual.
  - Por exemplo:
    - Para F10, defina K=0x79
    - Para Ctrl + F10, defina C=1, K=0x79
    - Para Alt + A, defina A=1, K=a ou A=1, K=A ou K=A, A=1
    - Para Ctrl + Alt + 5, defina C=1, A=1, K=5 ou A=1, K=5, C=1
    - Para Ctrl + Shift + F5, defina A = 1, S=1, K=0x74

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

- Suporte de monitor múltiplo e de alta resolução. Para máquinas de SO de sessão única, o HDX 3D Pro suporta dispositivos do usuário com até quatro monitores. Os usuários podem organizar seus monitores em qualquer configuração e podem misturar monitores com diferentes resoluções e orientações. O número de monitores é limitado pelos recursos da GPU do computador host, do dispositivo do usuário e da largura de banda disponível. HDX 3D Pro suporta todas as resoluções de monitor e é limitado apenas pelos recursos da GPU no computador host.
- Resolução dinâmica. Você pode redimensionar a janela da área de trabalho virtual ou do aplicativo para qualquer resolução. **Nota**: O único método com suporte para mudar a resolução é redimensionando a janela de sessão VDA. Não há suporte para alterar a resolução de dentro da sessão VDA (por meio de **Painel de Controle \ > Aparência** e **Personalização > Exibição \ > Resolução da Tela**).
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro suporta placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passagem de GPU e compartilhamento de GPU. A vGPU NVIDIA permite que várias VMs tenham acesso direto e simultâneo a uma única GPU física, usando os mesmos drivers gráficos NVIDIA implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar HDX 3D Pro com vDGA para cargas de trabalho RDS e VDI.

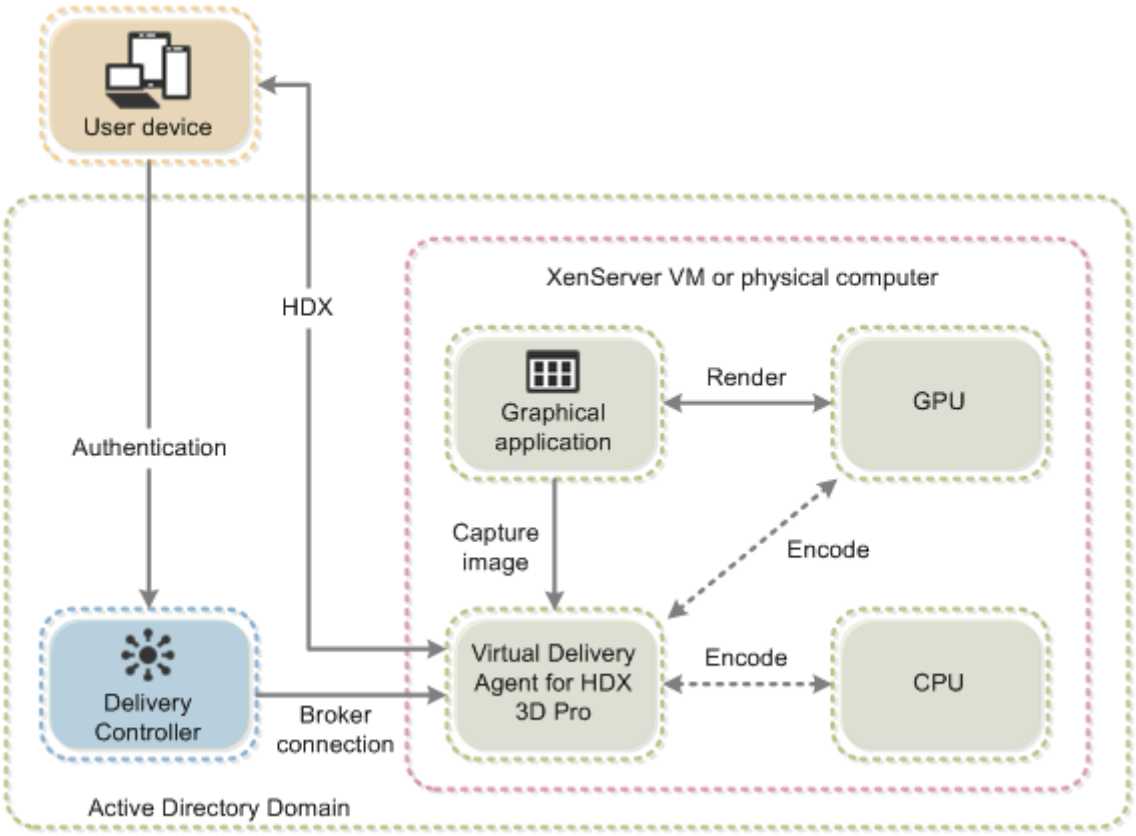
- Suporte para VMware vSphere/ESX usando NVIDIA vGPU e AMD MxGPU.
- Suporte para Microsoft HyperV com atribuição de dispositivo discreto no Windows Server 2016.
- Suporte para gráficos de data center com a família de processadores Intel Xeon E3. O HDX 3D Pro suporta vários monitores (até 3), apagamento de console, resolução personalizada e alta taxa de quadros com a família de processadores Intel suportada. Para obter mais informações, consulte http://www.citrix.com/intel e http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Suporte para AMD RapidFire nas placas de servidor AMD FirePro série S. O HDX 3D Pro suporta vários monitores (até 6), apagamento do console, resolução personalizada e alta taxa de quadros. Observação: o suporte HDX 3D Pro para AMD MxGPU (virtualização de GPU) funciona apenas com vGPUs VMware vSphere. O Citrix Hypervisor e o Hyper-V são compatíveis com a passagem da GPU. Para obter mais informações, consulte AMD Virtualization Solution.
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e processadores gráficos Intel Iris Pro. Uma configuração de política (ativada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para codificação H.264 (quando disponível). Se esse hardware não estiver disponível, o VDA recorre à codificação baseada em CPU usando o codec de vídeo do software. Para obter mais informações, consulte Configurações da política de gráficos.

Como mostrado na figura a seguir:

- Quando um usuário faz logon no aplicativo Citrix Workspace e acessa o aplicativo virtual ou desktop, o Controlador autentica o usuário. O Controller então entra em contato com o VDA para HDX 3D Pro para intermediar uma conexão com o computador que hospeda o aplicativo gráfico.

O VDA para HDX 3D Pro usa o hardware apropriado no host para comprimir visualizações da área de trabalho completa ou apenas do aplicativo gráfico.

- As exibições da área de trabalho ou do aplicativo e as interações do usuário com elas são transmitidas entre o computador host e o dispositivo do usuário. Esta transmissão é feita através de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



Otimize a experiência do usuário HDX 3D Pro

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em uma filial), recomendamos que você use a configuração de política de **Overall session bandwidth limit** para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que a largura de banda disponível não oscile extremamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações na largura de banda disponível ao longo das sessões do usuário podem afetar negativamente o desempenho.

Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário nesse cenário, determine a largura de banda necessária por usuário em períodos de pico e limite os usuários a esse valor sempre.

Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo do Knowledge Center CTX128190.

Thinwire

June 28, 2023

Introdução

O Thinwire, uma parte da tecnologia Citrix HDX, é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que os gráficos gerados em um computador sejam transmitidos, normalmente através de uma rede, para outro computador para exibição.

Uma solução remota de exibição bem-sucedida fornece uma experiência de usuário altamente interativa que é semelhante à de um PC local. O Thinwire oferece essa experiência usando uma variedade de técnicas complexas e eficientes de análise de imagem e compactação. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de visualização remota.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso geral de negócios e é usado como a tecnologia de controle remoto de exibição padrão no Citrix Virtual Apps and Desktops.

HDX 3D Pro

Em sua configuração padrão, o Thinwire pode fornecer gráficos 3D ou altamente interativos e usar uma unidade de processamento gráfico (GPU), se presente. No entanto, recomendamos ativar o modo HDX 3D Pro usando políticas **Optimize for 3D graphics workload** ou **Visual quality > Build to lossless** para cenários em que as GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264 ou H.265) para codificar toda a tela usando aceleração de hardware se houver uma GPU. Isso proporciona uma experiência mais fluida para gráficos profissionais 3D. Para obter mais informações, consulte H.264 Build to lossless, HDX 3D Pro e Aceleração de GPU para sistema operacional Windows de sessão única.

Requisitos

O Thinwire é otimizado para sistemas operacionais modernos, incluindo Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 e Windows 7. Para o Windows Server 2008 R2, recomenda-se o modo gráfico legado. Use os Modelos de política Citrix integradas, o SO legado de alta escalabilidade de servidor e o OS de legado otimizado para WAN para fornecer as combinações recomendadas da Citrix de configurações de política para esses casos de uso.

> **Nota:**
>
> Não oferecemos suporte ao modo gráfico legado nesta versão. Ele é incluído para compatibilidade com versões anteriores quando são usados o XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores VDA com Windows 7 e Windows 2008 R2.

- A configuração de política que determina o comportamento do Thinwire, **Use video codec for compression**, está disponível nas versões VDA no Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.6 FP3 e versões posteriores. A opção **Usar codec de vídeo quando preferida** é a configuração padrão nas versões VDA Citrix Virtual Apps and Desktops 7 1808 ou versões posteriores e XenApp e XenDesktop 7.9 e versões posteriores.
- Todos os aplicativos Citrix Workspace oferecem suporte ao Thinwire. Alguns aplicativos do Citrix Workspace podem oferecer suporte a recursos do Thinwire que outros não oferecem, por exemplo, gráficos de 8 ou 16 bits para uso reduzido da largura de banda. O suporte para esses recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos de servidor (CPU, memória) em cenários de vários monitores e de alta resolução. É possível ajustar a quantidade de recursos que o Thinwire usa, no entanto, o uso da largura de banda pode aumentar como resultado.
- Em cenários de baixa largura de banda ou alta latência, considere habilitar gráficos de 8 ou 16 bits para melhorar a interatividade. A qualidade visual pode ser afetada, especialmente em profundidade de cor de 8 bits.

Métodos de codificação

O Thinwire pode operar em dois modos de codificação diferentes, dependendo da política e dos recursos do cliente:

- Thinwire tela cheia H.264 ou H.265
- Thinwire com H.264 ou H.265 seletivo

O controle remoto GDI legado usa o driver de controle remoto XPDM e não um codificador bitmap do Thinwire.

Configuração

O Thinwire é a tecnologia de exibição remota padrão.

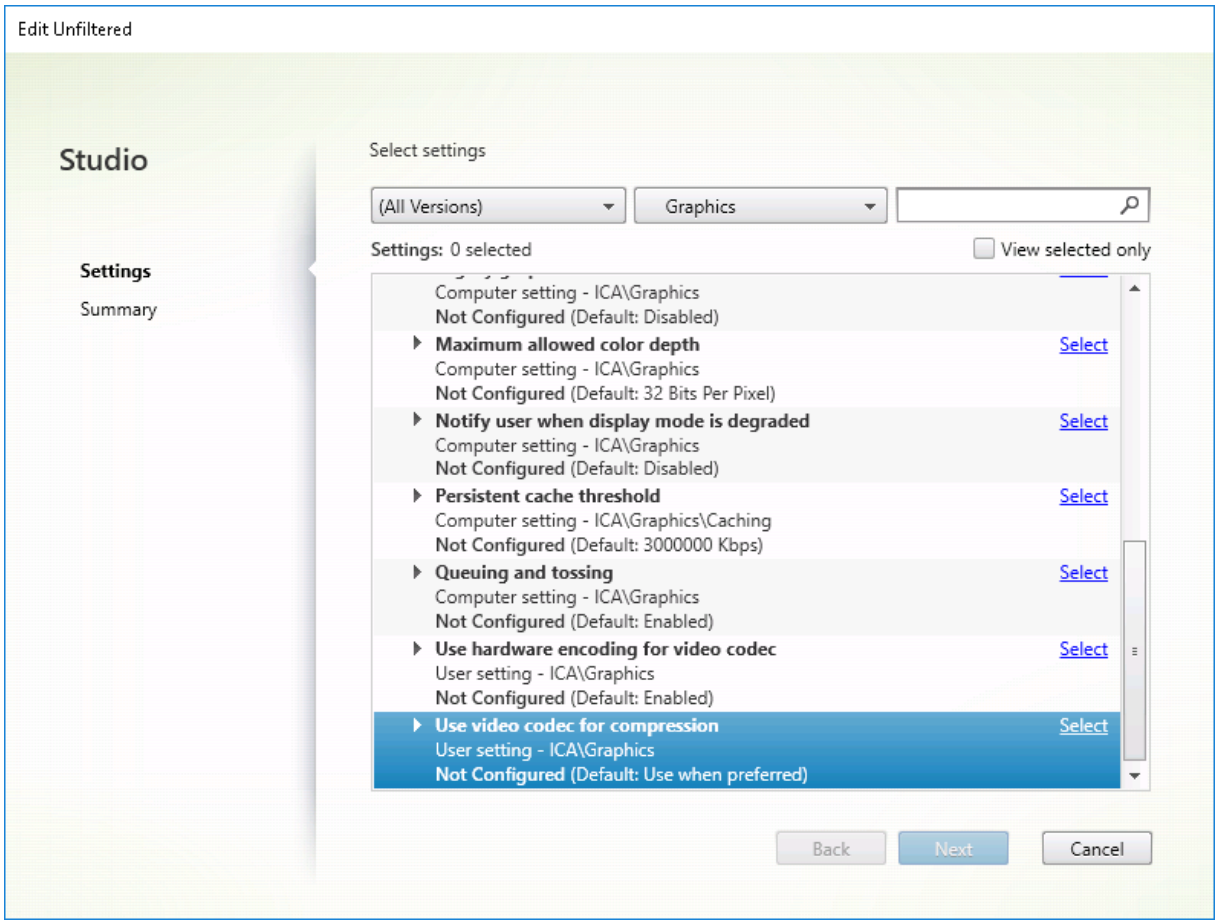
A seguinte configuração de política de gráficos define o padrão e fornece alternativas para diferentes casos de uso:

- Use video codec for compression

  - **Use video codec when preferred**. Essa é a configuração padrão. Nenhuma configuração adicional é necessária. Manter essa configuração como padrão garante que o Thinwire seja selecionado para todas as conexões Citrix e seja otimizado para escalabilidade, largura de banda e qualidade de imagem superior para cargas de trabalho típicas de desktop. Isso é funcionalmente equivalente a **For actively changing regions**.

- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:

  - **For actively changing regions**. A tecnologia de exibição adaptável no Thinwire identifica imagens em movimento (vídeo, 3D em movimento) e usa H.264 ou H.265 apenas na parte da tela onde a imagem está se movendo.
  - **For the entire screen**. Fornece Thinwire com tela cheia H.264 ou H.265 para otimizar a experiência do usuário e largura de banda melhoradas em casos com uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visually lossless** está desativada), a imagem final não é pixel perfeita (sem perdas) e não pode ser adequada para determinados cenários. Nesses casos, considere usar, em vez disso, H.264 Build to lossless.



Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de exibição remota. O Thinwire

dá suporte a todas elas.

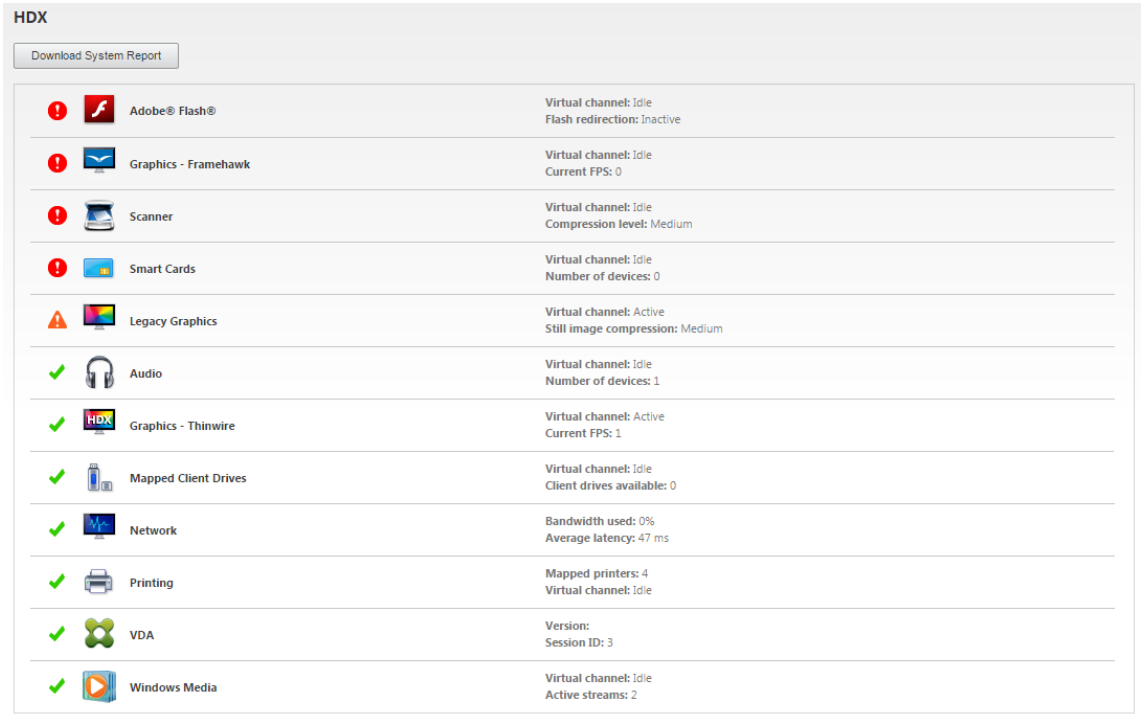
- Profundidade de cor preferida para gráficos simples
- Target frame rate
- Visual quality

Para obter as combinações recomendadas da Citrix de configurações de política para diferentes casos de uso comercial, use os Modelos de política da Citrix incorporados. Os modelos de **High Server Scalability** e **Very High Definition User Experience** usam o Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos usuários.

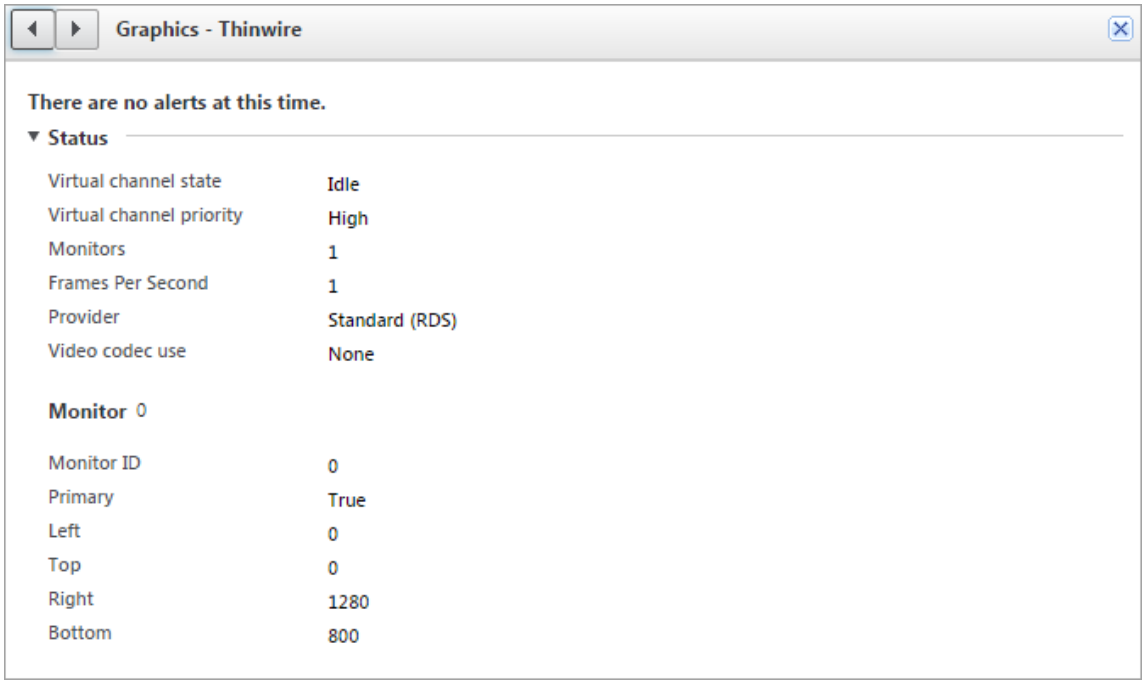
Monitoramento do Thinwire

Você pode monitorar o uso e o desempenho do Thinwire no Citrix Director. A visualização de detalhes do canal virtual HDX contém informações úteis para solução de problemas e monitoramento do Thinwire em qualquer sessão. Para exibir métricas relacionadas ao ThinWire:

1. No Director, procure um usuário, computador ou ponto de extremidade, abra uma sessão ativa e clique em **Details**. Ou você pode selecionar **Filters** > **Filters** > **All Sessions**, abrir uma sessão ativa e clicar em **Details**.
2. Role para baixo até o painel **HDX**.



3. Selecione **Graphics - Thinwire**.



Codec de compressão sem perdas (MDRLE)

Em uma sessão de área de trabalho típica, a maioria das imagens é composta por gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas por meio do codec 2DRLE. No lado do cliente do aplicativo Citrix Workspace, esses elementos são decodificados usando o decodificador 2DRLE do lado do aplicativo Citrix Workspace para exibição de sessão.

No XenApp e no XenDesktop 7.17, adicionamos um codec MDRLE de taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este codec novo não afeta a escalabilidade do servidor.

Largura de banda mais baixa geralmente significa melhor interatividade de sessão (especialmente em links compartilhados ou restritos) e custos reduzidos. Por exemplo, o consumo esperado de largura de banda ao usar o codec MDRLE é aproximadamente 10 a 15% menor em comparação com o XenApp e o XenDesktop 7.15 LTSR para cargas de trabalho típicas tipo Office.

A configuração não é exigida para o codec MDRLE. Se o aplicativo Citrix Workspace oferecer suporte à decodificação MDRLE, o VDA usará a codificação VDA MDRLE e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA recorrerá automaticamente à codificação 2DRLE.

Requisitos de MDRLE:

- Citrix Virtual Apps and Desktops versão mínima 7 1808 VDAs.
- XenApp e XenDesktop versão mínima 7.17 VDAs

- Aplicativo Citrix Workspace para Windows versão mínima 1808
- Citrix Receiver para Windows versão mínima 4.11

Modo Progressivo

O Citrix Virtual Apps and Desktops 1808 introduziu o modo progressivo e o habilitou por padrão. Em condições de rede restritas (padrão: largura de banda < 2 Mbps, ou latência > 200 ms), o Thinwire aumentou a compactação de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens fortemente compactadas têm a sua nitidez ajustada progressivamente, de forma aleatória, quando a atividade da tela for interrompida. Embora compactar e ajustar a nitidez desta forma melhore a interatividade geral, isso reduz a eficiência do cache e aumenta o uso da largura de banda.

A partir do Citrix Virtual Apps and Desktops 1906, o modo progressivo é desativado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada em condições de rede e flutua entre um valor mínimo e máximo pré-definido para cada configuração de **qualidade Visual**. Como não há nenhuma etapa explícita de ajuste de nitidez, o Thinwire otimiza a entrega de imagens e mantém a eficiência do cache, proporcionando quase todos os benefícios do modo progressivo.

Alteração do comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a seguinte chave de registro: Para obter informações, consulte Progressive mode na lista de recursos gerenciados por meio do registro.

H.264 Build to lossless

Build to lossless é uma configuração especial do Thinwire que otimiza a entrega de gráficos para interatividade e qualidade final da imagem. Você pode habilitar essa configuração definindo a política **Visual quality** como **Build to lossless**.

Build to lossless comprime a tela usando H.264 (ou H.265) durante a atividade da tela e nitidez para pixel perfeito (sem perdas) quando a atividade é interrompida. A qualidade de imagem H.264 (ou H.265) adapta-se aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de nitidez é executada gradualmente, dando uma resposta imediata se o usuário iniciar a atividade da tela logo após o início do ajuste de nitidez começar. Por exemplo, selecionando um modelo e girando-o.

H.264 **Build to lossless** oferece todas as vantagens de tela cheia H.264 ou H.265, incluindo aceleração de hardware, mas com o benefício adicional de uma tela final garantidamente sem perdas. Isso é fundamental para cargas de trabalho do tipo 3D que exigem uma imagem final com pixels perfeitos.

Por exemplo, manipulação de imagens médicas. Além disso, o H.264 **Build to lossless** usa menos recursos do que a tela cheia H.264 4:4:4. Como resultado, usar **Build to lossless** geralmente resulta em uma taxa de quadros mais alta do que H.264 visualmente sem perdas 4:4:4.

> **Nota:**
>
> Além da política de **Visual quality**, defina a política **Use video codec** como **Use when preferred** (padrão) ou **For actively changing regions**. Você pode reverter para não H.264 Build to lossless definindo a política **Use video codec** como **Do not use video codec**. Isso resulta em imagens em movimento codificadas com JPEG em vez de H.264 (ou H.265).

Marca d'água de sessão baseada em texto

June 28, 2023

As marcas d'água de sessão baseadas em texto ajudam a deter e ativar o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um estorvo para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que é uma camada de texto exibida em toda a tela de sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte a VDA.

> **Importante:**
>
> A marca d'água de sessão baseada em texto não é um recurso de segurança. A solução não impede completamente o roubo de dados, mas possibilita algum nível de dissuasão e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar esse recurso, recomendamos que você combine esse recurso com outras soluções de segurança, conforme aplicável.

A marca d'água da sessão é texto e é aplicada à sessão fornecida ao usuário. A marca d'água da sessão contém informações para rastrear o roubo de dados. Os dados mais importantes são a identidade do usuário de logon da sessão atual na qual a imagem da tela foi tirada. Para rastrear o vazamento de dados de forma mais eficaz, inclua outras informações, como endereço de protocolo de internet do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as Configurações da política de marca d'água da sessão para configurar o posicionamento e a aparência da marca d'água na tela.

Requisitos:

Virtual Delivery Agents:

SO multissessão 7.17
SO de sessão única 7.17

Limitações:

- As marcas d'água da sessão não têm suporte em sessões em que o acesso ao aplicativo local, o redirecionamento de mídia do Windows, o MediaStream, o redirecionamento de conteúdo do navegador e o redirecionamento de vídeo HTML5 são usados. Para usar a marca d'água da sessão, verifique se esses recursos estão desativados.
- A marca d'água da sessão não é suportada e não aparece se a sessão estiver sendo executada em modos acelerados por hardware de tela cheia (codificação H.264 ou H.265 em tela cheia).
- Se você definir essas políticas de HDX, as configurações de marca d'água não terão efeito e não será exibida nenhuma marca d'água na exibição da sessão.

Use hardware encoding for video codec como **Enabled**
Use video codec for compression como **For the entire screen**

- Se você definir essas políticas de HDX, o comportamento é indeterminado e a marca d'água não poderá ser exibida.

  Use hardware encoding for video codec como **Enabled**
  Use video codec for compression como **Use video codec when preferred**

  Para garantir que a marca d'água seja exibida, defina **Use hardware encoding for video codec** como **Disabled**, ou defina **Use video codec for compression** como **For actively changing regions** ou **Do not use video codec**.
- A marca d'água da sessão dá suporte apenas ao modo gráfico do Thinwire.
- Se você usar Session Recording, a sessão gravada não incluirá a marca d'água.
- Se você usar a assistência remota do Windows, a marca d'água não será exibida.
- Se um usuário pressionar a tecla **Print Screen** para capturar a tela, a tela capturada no lado VDA não inclui as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

Compartilhamento de tela

June 28, 2023

O compartilhamento de tela permite que um usuário compartilhe uma sessão do Citrix Virtual Desktops com outras pessoas, incluindo conteúdo da tela, teclado e controles do mouse.

Requisitos do sistema

- Windows: VDA com SO de sessão única ou multissessão
- Linux: consulte a documentação do Linux VDA para obter mais informações sobre o compartilhamento de sessões do Linux.
- Somente sessões da área de trabalho 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).

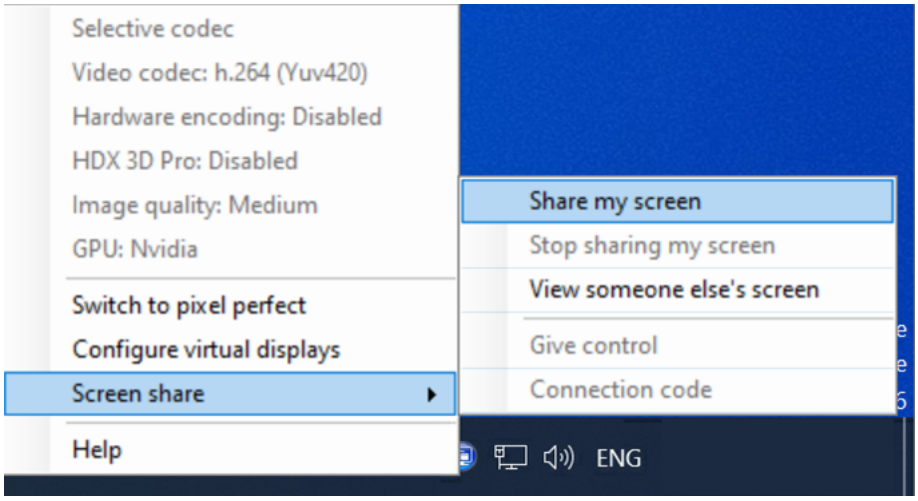
Configuração

O compartilhamento de tela deve ser ativado usando as políticas da Citrix. Por padrão, o compartilhamento de tela está desativado. Configure a política de compartilhamento de tela para ativar ou desativar a função e atribuir o intervalo de portas de rede utilizável.

Ative a política do indicador de status gráfico para exibir a interface do usuário que inclui controles para compartilhamento e conexão com sessões.

Compartilhamento de sessão

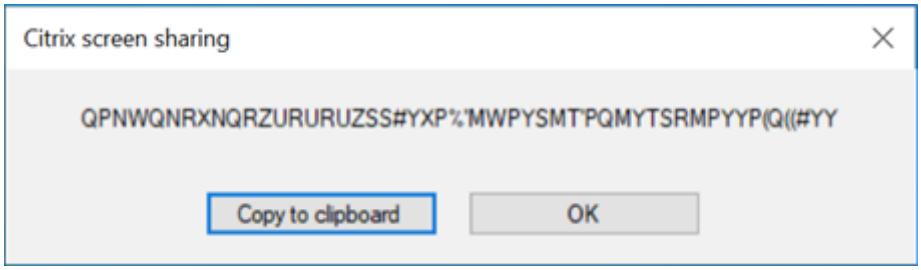
Para compartilhar uma sessão, procure o ícone do indicador de status gráfico HDX na área de notificação do Windows. Clique com o botão direito do mouse nele para exibir o menu e selecione **Compartilhamento de tela > Compartilhar minha tela**.



Clique em **Copiar para a área de transferência** ou selecione e copie manualmente a cadeia de caracteres inteira exibida na caixa de diálogo. A cadeia de caracteres pode ser colada no aplicativo de

sua escolha, como um e-mail ou cliente de mensagens instantâneas, para ser distribuída a outros usuários.

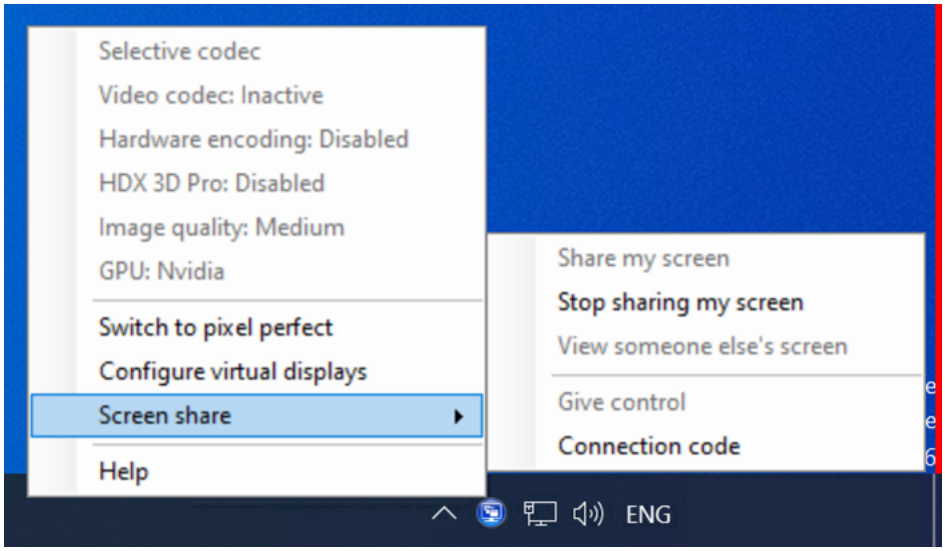
Clique em **OK** ou no **x** para fechar a caixa de diálogo. O código de conexão pode ser recuperado com a opção de menu **Compartilhamento de tela > Código de conexão** enquanto a sessão está sendo compartilhada.



Um contorno vermelho aparece ao redor da tela como um indicador de que a sessão agora está sendo compartilhada e é visível pelas outras pessoas.

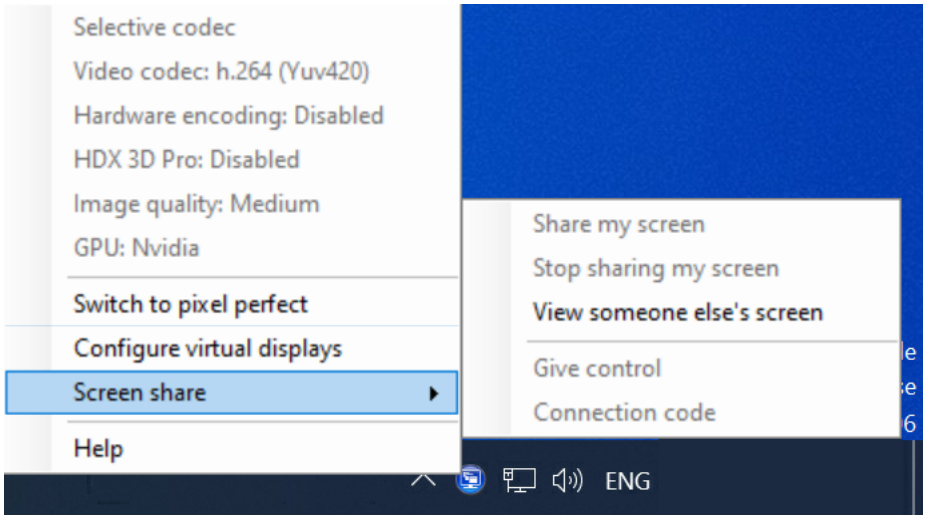
Os controles de mouse e teclado também podem ser compartilhados com outros usuários usando a opção de menu **Compartilhamento de tela > Dar o controle**.

Use a opção de menu **Compartilhamento de tela > Parar de compartilhar minha tela** para interromper o compartilhamento da sessão e desconectar todos os usuários.

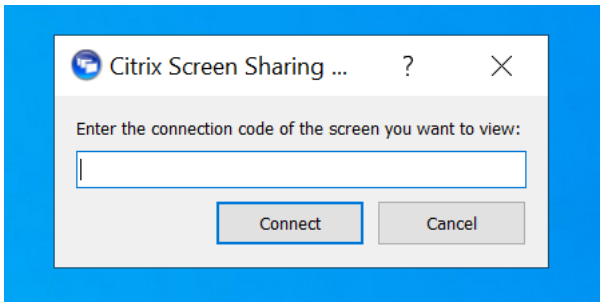


Conectar-se a uma sessão compartilhada

Para se conectar à sessão 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 > Ver a tela de outra pessoa**.

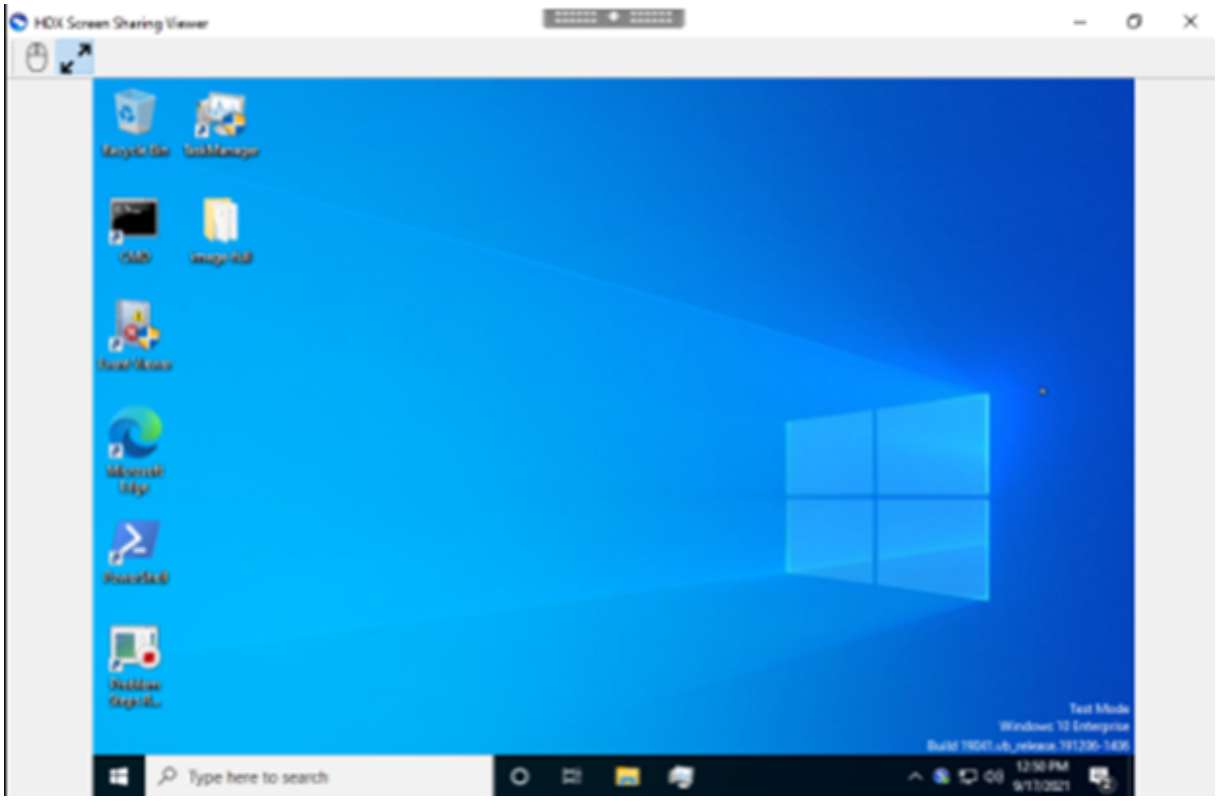


Na caixa de texto, digite ou cole a cadeia de conexão fornecida pelo usuário que vai compartilhar a sessão. Clique em **Conectar** para estabelecer a conexão.



Você pode solicitar o controle de teclado e mouse clicando no ícone do mouse no canto superior esquerdo da janela do **Visualizador de compartilhamento de tela HDX**.

Para se desconectar da sessão compartilhada, feche a janela do **Visualizador de compartilhamento de tela HDX** a qualquer momento.



Outras considerações

- O aplicativo visualizador de compartilhamento de tela está incluído com o VDA em *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* e pode ser implantado como um aplicativo publicado usando um Virtual Apps Server. Esse modelo de implantação alternativo permite a colaboração com usuários que não têm acesso a uma área de trabalho virtual.
- O número de usuários autorizados a se conectar a uma sessão compartilhada pode ser limitado usando o intervalo de portas de rede na política de compartilhamento de tela. É necessária uma porta por usuário. O intervalo padrão permite 100 usuários no máximo.
- Todos os monitores conectados à sessão são compartilhados. Você não pode selecionar monitores individuais.
- O codec de vídeo H.265 não é suportado.

Layout de exibição virtual

June 28, 2023

A interface do usuário de configuração de exibição virtual permite definir um layout de exibição virtual por monitor de sessão no VDA, dentro de uma sessão ao vivo. Esse recurso permite que você divida

cada monitor de sessão de forma independente em vários monitores virtuais. Você pode dividir em um total de 8 monitores virtuais na área de trabalho remota. Além disso, você pode atualizar o monitor principal da sessão e as configurações de DPI das exibições.

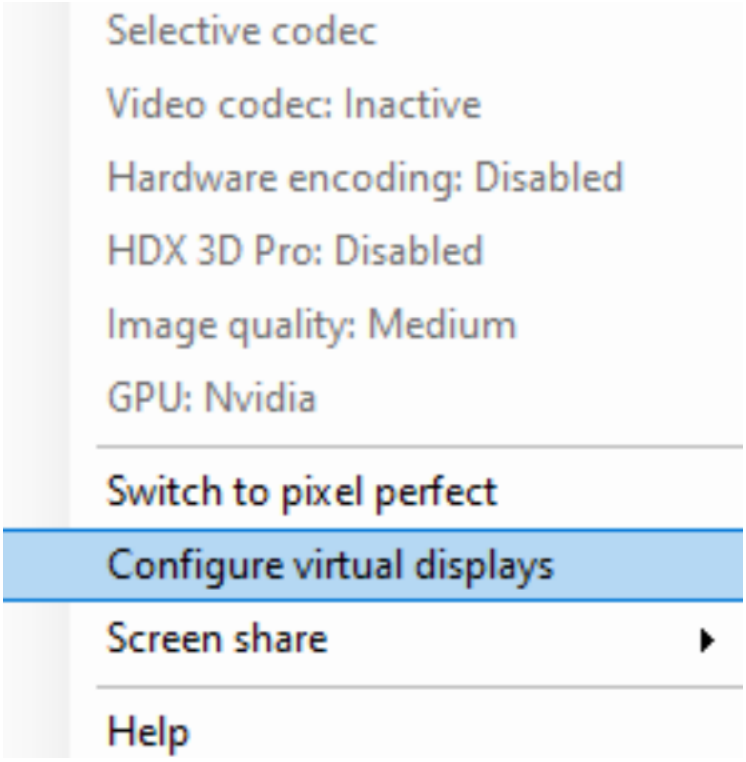
A configuração de exibição virtual é armazenada por usuário por dispositivo cliente. A configuração se aplica a todas as conexões subsequentes de um determinado cliente para um usuário específico. Ela persiste no redimensionamento geral da sessão, desconexão ou reconexão da sessão e logoff ou logon da sessão. A redefinição do layout de exibição virtual configurada ocorre no redimensionamento da sessão e na alteração no número de monitores da sessão.

Requisitos do sistema

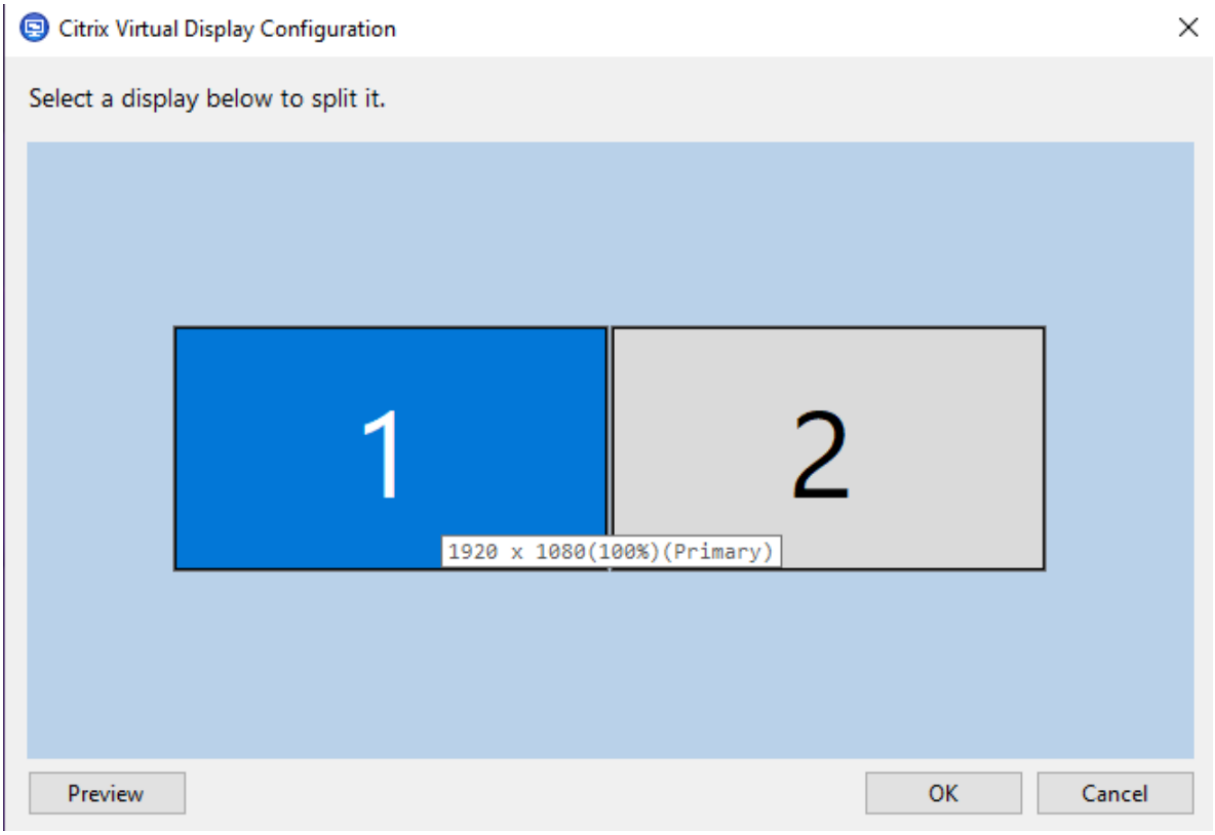
- Windows: VDA com SO de sessão única ou multissessão
- A política Graphics status indicator deve estar ativada
- Somente sessões de área de trabalho podem ser configuradas.

Configuração

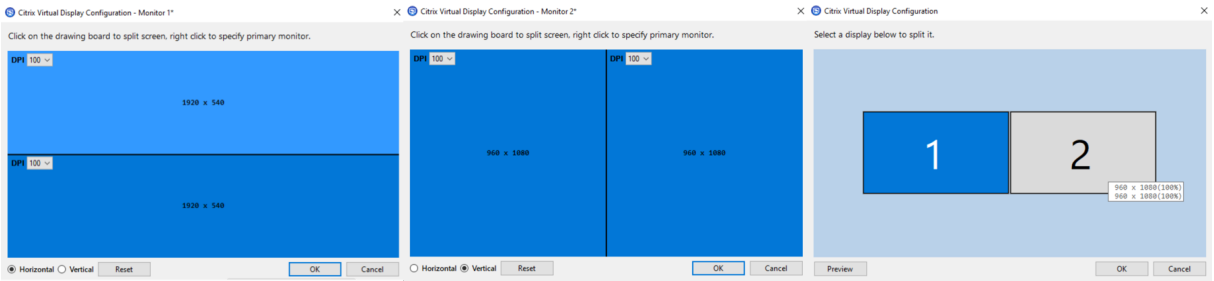
Para configurar o layout de exibição virtual, clique com o botão direito do mouse no ícone do indicador de status gráfico e selecione a opção Configure virtual displays. A interface do usuário de configuração de exibição virtual é iniciada.



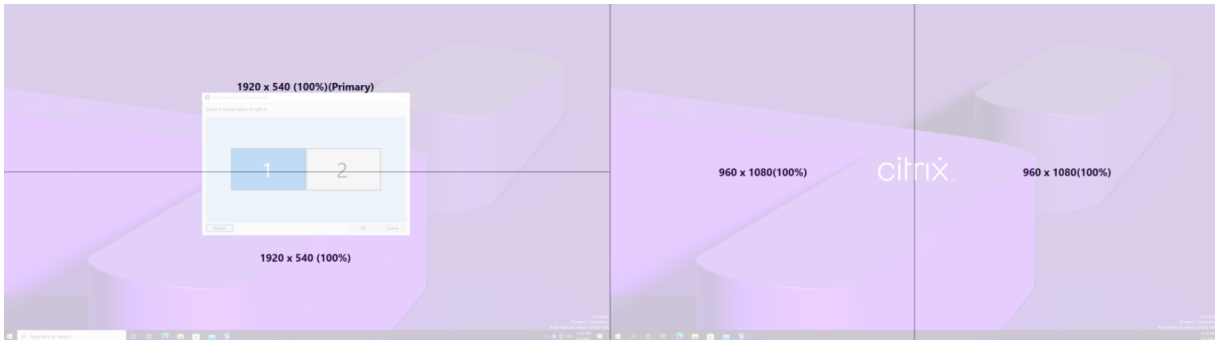
A interface do usuário mostra o layout de exibição da sessão atual, com azul indicando o monitor principal da sessão. Você pode ver a dica de ferramenta de configurações de exibição quando passa o mouse sobre uma tela de exibição. A dica de ferramenta fornece informações sobre o layout de exibição virtual atual definido em um determinado monitor de sessão.



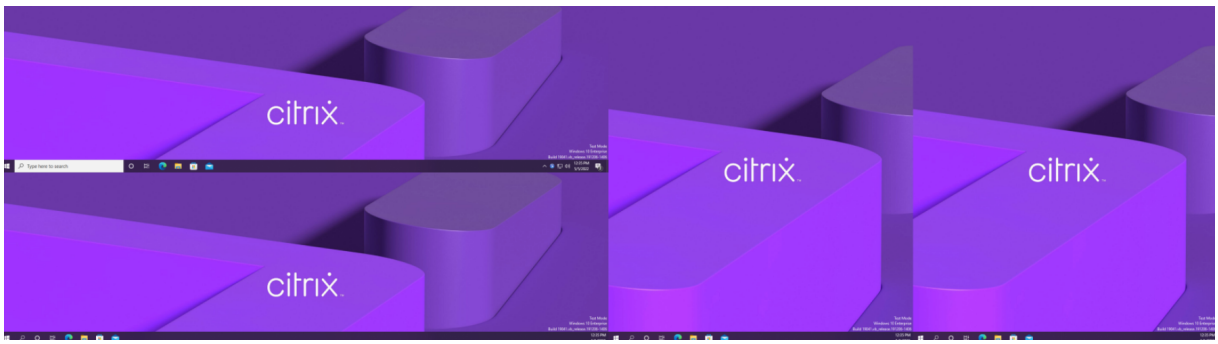
Selecione uma tela para fazer a transição para uma IU interativa, que permite configurar exibições virtuais para o monitor de sessão selecionado. Você pode desenhar linhas horizontais ou verticais para separar a tela em monitores virtuais. A tela é dividida de acordo com as porcentagens especificadas das resoluções do monitor da sessão. Clique com o botão direito do mouse em uma tela virtual para marcá-la como o monitor principal e use a lista suspensa DPI para definir o fator de escala preferido para a exibição na tela virtual. Depois de definir um layout de exibição virtual, clique em **OK** para salvar temporariamente o layout ou em **Cancel** para descartar as alterações. Você pode usar **Reset** para desfazer a configuração e restaurar o layout original do monitor da sessão.



Para visualizar o layout de exibição virtual configurado no momento, clique no botão **Preview**. Uma janela é exibida para destacar a posição esperada e a resolução das exibições virtuais na sessão.



Clique em **OK** para aplicar e salvar imediatamente o layout de exibição virtual. Clique em **Cancelar** para fechar a interface do usuário e descartar todas as alterações.



Outras considerações

- A resolução mínima de exibição virtual necessária é de 640 x 480.
- O DPI de exibição virtual definido por meio da interface do usuário depende do suporte de dimensionamento do sistema operacional da resolução de tela especificada.
- Não use esse recurso simultaneamente com o recurso de exibição virtual existente no aplicativo Citrix Workspace.
- A funcionalidade de visualização não é suportada no Server 2016.

Multimídia

June 28, 2023

A pilha de tecnologia HDX suporta a entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia de renderização do lado do servidor

- Redirecionamento de multimídia de renderização do lado do cliente

Esta estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, ao mesmo tempo em que maximiza a escalabilidade do servidor para reduzir o custo por usuário.

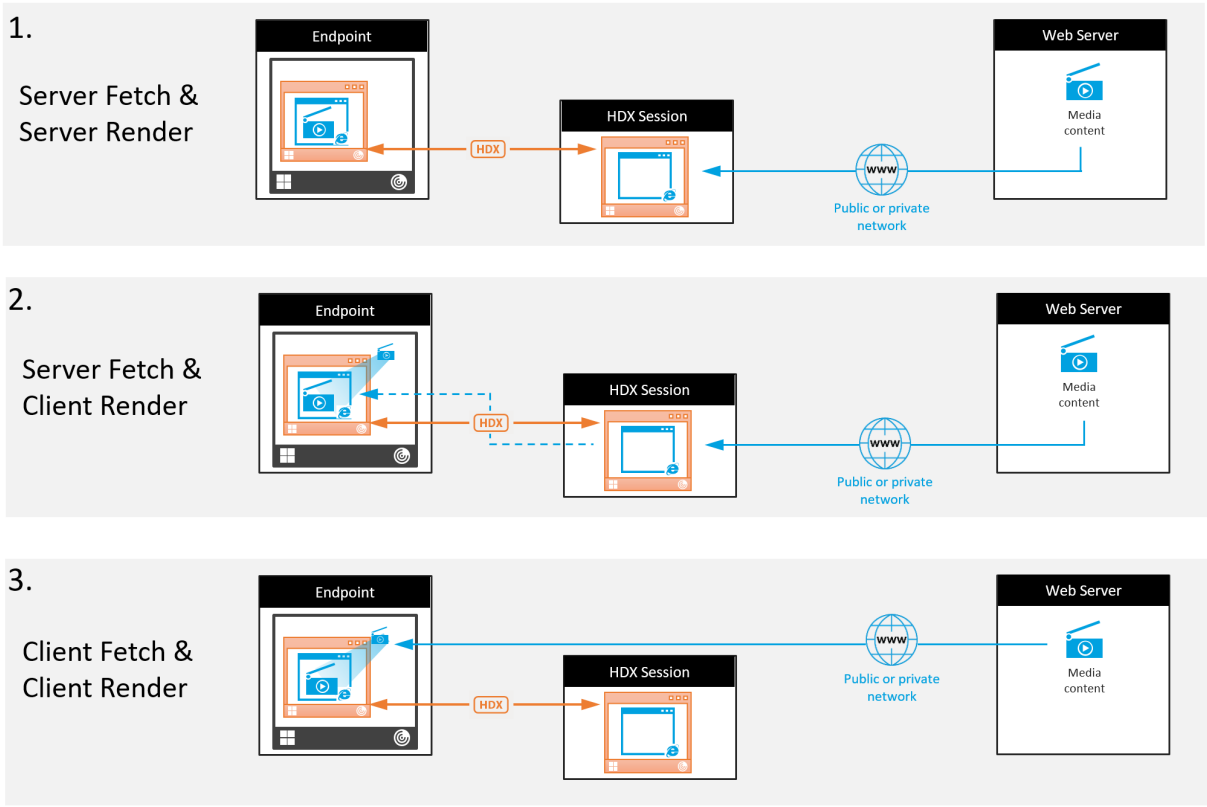
Com a entrega de multimídia renderizada pelo servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor Citrix Virtual Apps and Desktops pelo aplicativo. O conteúdo é comprimido e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo é de computação intensiva, a entrega de multimídia renderizada pelo servidor se beneficia imensamente da aceleração de hardware integrada. Por exemplo, o suporte ao DirectX Video Acceleration (DXVA) libera a CPU executando a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

Como a maioria dos servidores não oferece nenhuma aceleração de hardware para compressão de vídeo, a escalabilidade do servidor é afetada negativamente se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter a alta escalabilidade do servidor redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

- O redirecionamento do Windows Media livra o servidor de uma grande variedade de formatos de mídia normalmente associados ao Windows Media Player.
- O vídeo HTML5 se popularizou e a Citrix introduziu uma tecnologia de redirecionamento para esse tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento de contato, Redirecionamento de host para cliente e Acesso a aplicativos locais, ao conteúdo multimídia.

Juntando essas tecnologias, se você não configurar o redirecionamento, o HDX fará a renderização do lado do servidor.
Se você configurar o redirecionamento, o HDX usará Obtenção de servidor e Renderização de cliente ou Obtenção de cliente e Renderização de cliente. Se esses métodos falharem, o HDX volta à Renderização do lado do servidor conforme necessário e está sujeito à Política de Prevenção de Fallback.

Exemplos de cenários



Cenário 1. (Obtenção de servidor e Renderização de servidor):

1. O servidor obtém o arquivo de mídia de sua origem, decodifica-o e apresenta o conteúdo para um dispositivo de áudio ou dispositivo de exibição.
2. O servidor extrai a imagem ou o som apresentados do dispositivo de exibição ou do dispositivo de áudio, respectivamente.
3. O servidor opcionalmente o comprime e, em seguida, o transmite para o cliente.

Essa abordagem incorre em um alto custo de CPU, um alto custo de largura de banda (se a imagem/-som extraídos não forem comprimidos de forma eficiente) e tem baixa escalabilidade de servidor.

Os canais virtuais Thinwire e Audio lidam com essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para clientes. Usando essa abordagem, a decodificação acontece no servidor e funciona para uma maior variedade de dispositivos e formatos.

Cenário 2. (Obtenção de servidor e Renderização de cliente):

Esta abordagem depende de sua capacidade de interceptar o conteúdo de mídia antes que ele seja decodificado e apresentado ao dispositivo de áudio ou exibição. O conteúdo de áudio/vídeo comprimido é enviado ao cliente, onde é decodificado e apresentado localmente. A vantagem dessa abordagem é que ele é descarregado para os dispositivos cliente, economizando ciclos da CPU no servidor.

No entanto, isso também introduz alguns requisitos adicionais de hardware e software para o cliente. O cliente deve ser capaz de decodificar cada formato que possa vir a receber.

Cenário 3. (Obtenção de cliente e Renderização de cliente):

Esta abordagem depende de sua capacidade de interceptar a URL de conteúdo de mídia antes que ela seja obtida da origem. A URL é enviada para o cliente de onde o conteúdo de mídia é obtido, decodificado e apresentado localmente. Essa abordagem é conceitualmente simples. Sua vantagem é que ela economiza ciclos da CPU no servidor e largura de banda porque o servidor envia somente comandos de controle. No entanto, o conteúdo de mídia nem sempre é acessível aos clientes.

Estrutura e plataforma:

Os sistemas operacionais de sessão única (Windows, Mac OS X e Linux) fornecem estruturas multimídia que permitem o desenvolvimento mais rápido de aplicativos multimídia. Esta tabela lista algumas das estruturas multimídia mais populares. Cada estrutura divide o processamento da mídia em várias etapas e usa uma arquitetura baseada em pipeline.

Estrutura	Plataforma
DirectShow	Windows (98 e posterior)
Media Foundation	Windows (Vista e posterior)
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 do Windows Media	Sim

Recursos de áudio

January 3, 2024

Você pode configurar e adicionar as seguintes configurações de política Citrix a uma política que otimiza os recursos de áudio HDX. Para obter detalhes de uso, além de relacionamentos e dependências com outras configurações de política, consulte Configurações de políticas de áudio, Configurações de política de largura de banda e Configurações de políticas de conexões multi-stream.

Áudio adaptativo

Com o áudio adaptativo, você não precisa configurar manualmente as políticas de qualidade de áudio no VDA. O áudio adaptativo otimiza as configurações do seu ambiente e substitui formatos obsoletos de compactação de áudio para fornecer uma excelente experiência ao usuário.

O áudio adaptativo está ativado por padrão. Para desativar o áudio adaptativo, consulte Configurações da política de áudio.

> **Importante:**
>
> Recomendamos fornecer áudio por meio de User Datagram Protocol (UDP) em vez de TCP quando aplicativos de áudio em tempo real forem necessários. Somente o Windows Virtual Delivery Agent (VDA) dá suporte a áudio por UDP.
>
> A criptografia de áudio UDP usando DTLS está disponível somente entre o Citrix Gateway e o aplicativo Citrix Workspace. Portanto, às vezes pode ser preferível usar o transporte TCP. O TCP oferece suporte à criptografia TLS de ponta a ponta do aplicativo VDA para o Citrix Workspace.
>
> Para obter mais informações sobre áudio adaptativo e áudio UDP, consulte Transporte de áudio em tempo real por UDP e faixa de portas UDP de áudio.

Qualidade de áudio

Em geral, maior qualidade de som consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para dispositivos do usuário. A compactação de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações de política Citrix para configurar os níveis de compactação que devem ser aplicados aos arquivos de som.

Como padrão, a configuração de **política de qualidade de áudio** é definida como Áudio de alta definição quando o transporte TCP é usado. A política é definida como Medium - otimizado para fala quando é usado o transporte UDP (recomendado). A configuração de **áudio de alta definição** fornece áudio estéreo de alta fidelidade, mas consome mais largura de banda do que outras

configurações de qualidade. Não use essa qualidade de áudio para aplicativos de chat por voz ou chat por vídeo não otimizados (como softphones). A razão disso é que ele pode introduzir latência no caminho de áudio, o que não é adequado para comunicações em tempo real. Recomendamos a configuração otimizada para política de fala para áudio em tempo real, independentemente do protocolo de transporte selecionado.

Quando a largura de banda é limitada, por exemplo, conexões via satélite ou dial-up, se a qualidade de áudio for reduzida para **Baixa**, é consumida a menor largura de banda possível. Nessa situação, crie políticas separadas para usuários em conexões de baixa largura de banda para que os usuários em conexões de alta largura de banda não sejam prejudicados.

Para obter detalhes de configuração, consulte Configurações de política de áudio. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Diretrizes de largura de banda para reprodução e gravação de áudio:

- Áudio adaptativo (padrão)
  - Taxa de bits: variável adaptativa
  - Número de canais: 2 (estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 48000 Hz
  - Profundidade de bits: 16 bits
- High quality
  - Taxa de bits: ~ 100 kbps (mín. 75, máx. 175 kbps) para reprodução/ ~ 70 kbps para captura de microfone
  - Número de canais: 2 (estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 44100 Hz
  - Profundidade de bits: 16 bits
- Qualidade média (recomendada para VoIP)
  - Taxa de bits: ~ 16 kbps (mín. 20, máx. 40 kbps) para reprodução, ~ 16 kbps para captura de microfone
  - Número de canais: 1 (Mono) para reprodução e captura
  - Frequência: 16000 Hz (banda larga)
  - Profundidade de bits: 16 bits
- Baixa qualidade
  - Taxa de bits: ~ 11 kbps (mín. 10; máx. 25 kbps) para reprodução, ~11 kbps para captura de microfone
  - Número de canais: 1 (Mono) para reprodução e captura
  - Frequência: 8000 Hz (banda estreita)
  - Profundidade de bits: 16 bits

Client audio redirection

Para permitir que os usuários recebam áudio de um aplicativo em um servidor por meio de alto-falantes ou outros dispositivos de som no dispositivo do usuário, deixe a configuração de **Client audio redirection** em **Allowed**. Esse é o padrão.

O mapeamento de áudio do cliente coloca carga extra nos servidores e na rede. No entanto, proibir o redirecionamento de áudio do cliente desativa toda a funcionalidade de áudio HDX.

Para obter detalhes de configuração, consulte Configurações de política de áudio. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Client microphone redirection

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Enabled** no valor padrão (Allowed).

Por segurança, os dispositivos do usuário alertam seus usuários quando os servidores em que eles não confiam tentam acessar os microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar esse alerta no aplicativo Citrix Workspace.

Para obter detalhes de configuração, consulte Configurações de política de áudio. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Audio Plug N Play

A configuração de política Áudio Plug and Play permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração é **Enabled** por padrão. O Áudio Plug and Play permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até que a sessão do usuário tenha começado.

Essa configuração se aplica apenas aos computadores do sistema operacional Windows multi-ssessão.

Para obter detalhes de configuração, consulte Configurações de política de áudio.

Limite de largura de banda de redirecionamento de áudio e percentual de limite de largura de banda de redirecionamento

A configuração de política de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para uma reprodução e gravação de áudio em uma sessão.

A configuração de porcentagem de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima para redirecionamento de áudio como uma porcentagem da largura de banda disponível total.

Por padrão, é especificado zero (sem máximo) para as duas configurações. Se os dois ajustes estiverem configurados, aquele com o limite mais baixo da largura de banda será usado.

Para obter detalhes sobre a configuração, consulte Configurações da política de largura de banda. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

Transporte de áudio em tempo real por UDP e faixa de portas UDP de áudio

Por padrão, o transporte de áudio por User Datagram Protocol (UDP) em tempo real é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam transporte de áudio em tempo real por UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar o UDP/RTP para áudio para garantir a melhor experiência possível do usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio por UDP tem preferência em relação a EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que não seja adiciona nenhuma latência em conexões com alta perda de pacotes.

> **Importante:**
>
> Quando o Citrix Gateway não está no caminho, os dados de áudio transmitidos com UDP não são criptografados. Se o Citrix Gateway estiver configurado para acessar os recursos do Citrix Virtual Apps and Desktops, o tráfego de áudio entre o dispositivo de ponto de extremidade e o Citrix Gateway será protegido por meio do protocolo DTLS.

A faixa de porta UDP de áudio especifica o intervalo de números de porta que o Windows VDA usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é 16500 a 16509.

> **Nota:**
>
> Se o transporte em tempo real de áudio sobre UDP não for necessário para o áudio adaptativo, a Citrix recomenda definir a configuração de política como Desativado. Isso ajuda a evitar que os clientes do aplicativo Citrix Workspace solicitem conexões UDP abertas ou disparem a exibição de janelas de diálogo indesejadas de configuração de firewall do cliente do aplicativo Citrix Workspace.

Para obter detalhes sobre o transporte em tempo real de áudio sobre UDP, consulte Configurações da política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações da política de conexões multi-stream. Lembre-se de ativar as configurações de áudio do cliente no dispositivo do usuário.

O áudio sobre UDP requer o Windows VDA. Para obter políticas com suporte no Linux VDA, consulte Lista de suporte de políticas.

Políticas de configuração de áudio para dispositivos do usuário

1. Carregue os modelos de diretiva de grupo seguindo a configuração de Group Policy Object administrative template.
2. No Editor de Política de Grupo, expanda **Administrative Templates > Citrix Components > Citrix Workspace > User Experience**.
3. Para **Client audio settings**, selecione **Not Configured**, **Enabled** ou **Disabled**.
   - **Not Configured**. Por padrão, o redirecionamento de áudio é ativado com áudio de alta qualidade ou as configurações de áudio personalizadas previamente configuradas.
   - **Enabled**. Ativa o redirecionamento de áudio com as opções selecionadas.
   - **Disabled**. Desativa o redirecionamento de áudio.
4. Se você selecionar **Ativado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Enable Real-Time Transport** e defina o intervalo de portas de entrada para abrir no firewall local do Windows.
6. Para usar o áudio UDP com o Citrix Gateway, selecione **Permitir transporte em tempo real através do gateway**. Configure o Citrix Gateway com DTLS. Para obter mais informações, consulte este artigo.

Como administrador, se você não tiver controle sobre dispositivos de ponto de extremidade para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o áudio UDP. Por exemplo, para trazer seus próprios dispositivos ou computadores domésticos.

1. No computador com StoreFront, abra C:\inetpub\wwwroot\Citrix\<nome do armazenamento>\App_Data\default.ica com um editor como o bloco de notas.
2. Faça as seguintes entradas na seção [Application].

   ; This text enables Real-Time Transport

   EnableRtpAudio=true

   ; This text allows Real-Time Transport Through gateway

   EnableUDPThroughGateway=true

   ; This text sets audio quality to Medium

   AudioBandwidthLimit=1

   ; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

Se você ativar o áudio UDP (User Datagram Protocol) editando default.ica, o áudio UDP estará ativado para todos os usuários que estão usando esse armazenamento.

Evitar eco durante conferências multimídia

Os usuários em conferências de áudio ou vídeo podem ouvir um eco. Geralmente ocorrem ecos quando há alto-falantes e microfones muito próximos uns dos outros. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX fornece uma opção de cancelamento de eco (ativada por padrão) que minimiza o eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Verifique se os dispositivos não estão muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração de registro para desativar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados pelo registro.

Softphones

Um softphone é um software que atua como uma interface de telefone. O softphone pode ser usado para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Com um softphone, você pode discar números de telefone e realizar outras funções telefônicas usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para usar softphones.

- **Control mode**. O softphone hospedado controla um telefone físico. Nesse modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.
- **HDX RealTime optimized softphone support (recommended)**. O mecanismo de mídia é executado no dispositivo do usuário e o tráfego do protocolo Voice over Internet flui ponto a ponto. Para ver exemplos, consulte:
  - HDX Optimization for Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone for VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin Zoom VDI
  - Genesys PureEngage Cloud

  - Dispositivo de ditado Nuance Dragon PowerMic

- **Local App Access**. Um recurso do Citrix Virtual Apps and Desktops que permite que um aplicativo como um softphone seja executado localmente no dispositivo do usuário Windows, mas parece perfeitamente integrado à área de trabalho virtual/publicada. Este recurso passa todo o processamento de áudio para o dispositivo do usuário. Para obter mais informações, consulte Acesso ao aplicativo local e redirecionamento de URL.
- **HDX RealTime generic softphone support.** Protocolo VoIP por ICA.

Suporte softphone genérico

O suporte genérico de softphone permite que você hospede um softphone não modificado no XenApp ou no XenDesktop no data center. O tráfego de áudio passa pelo protocolo Citrix ICA (de preferência usando UDP/RTP) para o dispositivo do usuário que executa o aplicativo Citrix Workspace.

O suporte genérico de softphone é um recurso do HDX RealTime. Esta abordagem para a funcionamento do softphone é especialmente útil quando:

- Não há nenhuma solução otimizada disponível para o funcionamento do softphone e o usuário não está usando um dispositivo Windows onde pode ser usado o acesso ao aplicativo local.
- O mecanismo de mídia que é necessário para o funcionamento otimizado do softphone não está instalado no dispositivo do usuário ou não está disponível para a versão do sistema operacional em execução no dispositivo do usuário. Nesse cenário, o Generic HDX RealTime fornece uma valiosa solução de fallback.

Há duas considerações sobre o funcionamento do softphone por meio do Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é fornecido ao ambiente de trabalho virtual/publicado.
- Como o áudio é fornecido de e para o fone de ouvido do usuário, microfone e alto-falantes ou telefone USB.

O Citrix Virtual Apps and Desktops inclui inúmeras tecnologias para oferecer suporte à entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida da eficiência de áudio e largura de banda em tempo real.
- Pilha de áudio de baixa latência.
- Buffer de jitter do lado do servidor para suavizar o áudio quando a latência da rede flutua.
- Marcação de pacotes (DSCP e WMM) para qualidade de serviço.
  - Marcação DSCP para pacotes RTP (Camada 3)
  - Marcação de WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voice over Internet Protocol. O aplicativo Citrix Workspace para Windows oferece os seguintes recursos:

- Buffer de jitter do lado do cliente - Garante áudio sem interrupções, mesmo quando a latência da rede flutua.
- Cancelamento de eco - Permite uma maior variação na distância entre microfone e alto-falantes para colaboradores que não usam um fone de ouvido.
- Áudio Plug and Play - Os dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.
- Roteamento de dispositivos de áudio - Os usuários podem direcionar o toque para alto-falantes, mas o caminho de voz para o fone de ouvido.
- Multi-stream ICA - Permite a qualidade flexível de roteamento baseado em serviço pela rede.
- O ICA é compatível com quatro fluxos TCP e dois UDP. Um dos fluxos UDP dá suporte ao áudio em tempo real via RTP.

Para obter um resumo dos recursos do aplicativo Citrix Workspace, consulte Citrix Receiver Feature Matrix.

Recomendações de configuração do sistema

Hardware e software do cliente:
Para uma qualidade de áudio ideal, recomendamos a versão mais recente do aplicativo Citrix Workspace e um fone de ouvido de boa qualidade com cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac oferecem suporte ao Voice over Internet Protocol. Além disso, o Dell Wyse oferece suporte a Protocolo de Voz via Internet para ThinOS (WTOS).

Considerações sobre a CPU:
Monitore o uso da CPU no VDA para determinar se é necessário atribuir duas CPUs virtuais a cada máquina virtual. Voz e vídeo em tempo real consomem grandes quantidades de dados. A configuração de duas CPUs virtuais reduz a latência de switching de thread. Portanto, recomendamos que você configure duas vCPUs em um ambiente Citrix Virtual Desktops VDI.

Ter duas CPUs virtuais não significa necessariamente duplicar o número de CPUs físicas, porque as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de confiabilidade de sessão, também aumenta o consumo da CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo da CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor potente.

Áudio UDP:
O áudio por UDP fornece excelente tolerância ao congestionamento de rede e perda de pacotes. Recomendamos esse protocolo em vez de TCP quando disponível.

Configuração LAN/WAN:
A configuração adequada da rede é crítica para uma boa qualidade de áudio em tempo real. Tipicamente, você deve configurar LANs virtuais (VLANs) porque os pacotes de broadcast excessivos podem introduzir jitter. Os dispositivos habilitados para IPv6 podem gerar muitos pacotes de transmissão. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configurar para oferecer suporte à Qualidade de Serviço.

Configurações para usar conexões WAN:
Você pode usar o chat de voz através de conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se fornecer softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler SD-WAN entre o data center e o escritório remoto. Com isso, mantém-se uma alta qualidade de serviço. O NetScaler SD-WAN suporta ICA de fluxo múltiplo, incluindo UDP. Além disso, no caso de um único fluxo TCP, é possível distinguir as prioridades de vários canais virtuais ICA para garantir que os dados de áudio em tempo real de alta prioridade recebam tratamento preferencial.

Use o Director ou o HDX Monitor para validar sua configuração HDX.

Conexões remotas de usuários:
o Citrix Gateway oferece suporte ao DTLS para fornecer tráfego UDP/RTP de forma nativa (sem encapsulamento no TCP).
Abra firewalls bidirecionalmente para tráfego UDP pela porta 443.

Seleção de codec e consumo de largura de banda:
entre o dispositivo do usuário e o VDA no data center, recomendamos usar a configuração de codec **otimizada para fala**, também conhecida como áudio de qualidade média. Entre a plataforma VDA e o IP-PBX, o softphone usa qualquer codec configurado ou negociado. Por exemplo:

- O G711 fornece boa qualidade de voz, mas tem uma exigência de largura de banda de 80 kilobits por segundo através de 100 kilobits por segundo por chamada (dependendo dos overheads da Network Layer2).
- G729 fornece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo através de 40 kilobits por segundo por chamada (dependendo dos overheads da Network Layer2).

Fornecer aplicativos de softphone para o ambiente de trabalho virtual

Existem dois métodos pelos quais você pode fornecer um softphone para a área de trabalho virtual XenDesktop:

- O aplicativo pode ser instalado na imagem da área de trabalho virtual.
- O aplicativo pode ser transmitido para a área de trabalho virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciabilidade porque a imagem da área de trabalho virtual é mantida organizada. Depois de ser transmitido para a área de trabalho virtual, o aplicativo é

executado nesse ambiente como se estivesse instalado da maneira usual. Nem todos os aplicativos são compatíveis com App-V.

Fornecimento de áudio de e para o dispositivo do usuário

Generic HDX RealTime dá suporte aos métodos de fornecimento de áudio de e para o dispositivo do usuário:

- **Canal virtual de áudio Citrix**. Geralmente, recomendamos o cana virtual de áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB genérico**. Dá suporte a dispositivos de áudio com botões ou tela (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou LAN com o servidor Citrix Virtual Apps and Desktops.

Canal virtual de áudio Citrix

O canal virtual de áudio Citrix (CTXCAM) bidirecional permite que o áudio seja fornecido de forma eficiente pela rede. O Generic HDX RealTime recebe o áudio do fone de ouvido ou microfone do usuário e o compacta. Em seguida, envia-o por ICA para o aplicativo softphone na área de trabalho virtual. Da mesma forma, a saída de áudio do softphone é compactada e enviada na outra direção para o fone de ouvido ou alto-falantes do usuário. Esta compactação é independente da compactação usada pelo próprio softphone (como G.729 ou G.711). Ela é feita por meio do codec otimizado para fala (qualidade média). Suas características são ideais para Voice over Internet Protocol. Apresenta tempo de codificação rápido e consome apenas aproximadamente 56 quilobits por segundo de largura de banda de rede (28 Kbps em cada direção), pico. Esse codec deve ser explicitamente selecionado no console do Studio porque não é o codec de áudio padrão. O padrão é o codec de áudio HD (alta qualidade). Esse codec é excelente para trilhas sonoras estéreo de alta fidelidade, mas é mais lento para codificar em comparação com o codec otimizado para fala.

Redirecionamento USB genérico

A tecnologia de redirecionamento USB genérico (canal virtual CTXGUSB) da Citrix fornece um meio genérico de dispositivos USB remotos, incluindo dispositivos compostos (áudio e HID) e dispositivos USB isócronos. Essa abordagem é limitada aos usuários conectados a uma LAN. Por esse motivo o protocolo USB tende a ser sensível à latência da rede e requer largura de banda de rede considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones. Esse redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o canal de áudio virtual Citrix tem preferência porque é otimizado para tráfego de áudio. A principal exceção é quando você está usando um dispositivo de áudio com botões. Por exemplo, um telefone USB conectado ao dispositivo do usuário conectado via LAN ao data center. Nesse caso, o Redirecionamento USB Genérico suporta botões no conjunto de telefone ou fone de ouvido que controlam recursos enviando um sinal de volta para o softphone. Não há um problema com botões que funcionam localmente no dispositivo.

Limitação

Você instala um dispositivo de áudio em seu cliente, ativa o redirecionamento de áudio e inicia uma sessão com RDS. Os arquivos de áudio podem não ser reproduzidos e uma é exibida uma mensagem de erro.

Como solução alternativa, adicione esta chave de registro no computador RDS e reinicie a máquina: Para obter informações, consulte Audio limitation na lista de recursos gerenciados por meio do registro.

Redirecionamento de conteúdo do navegador

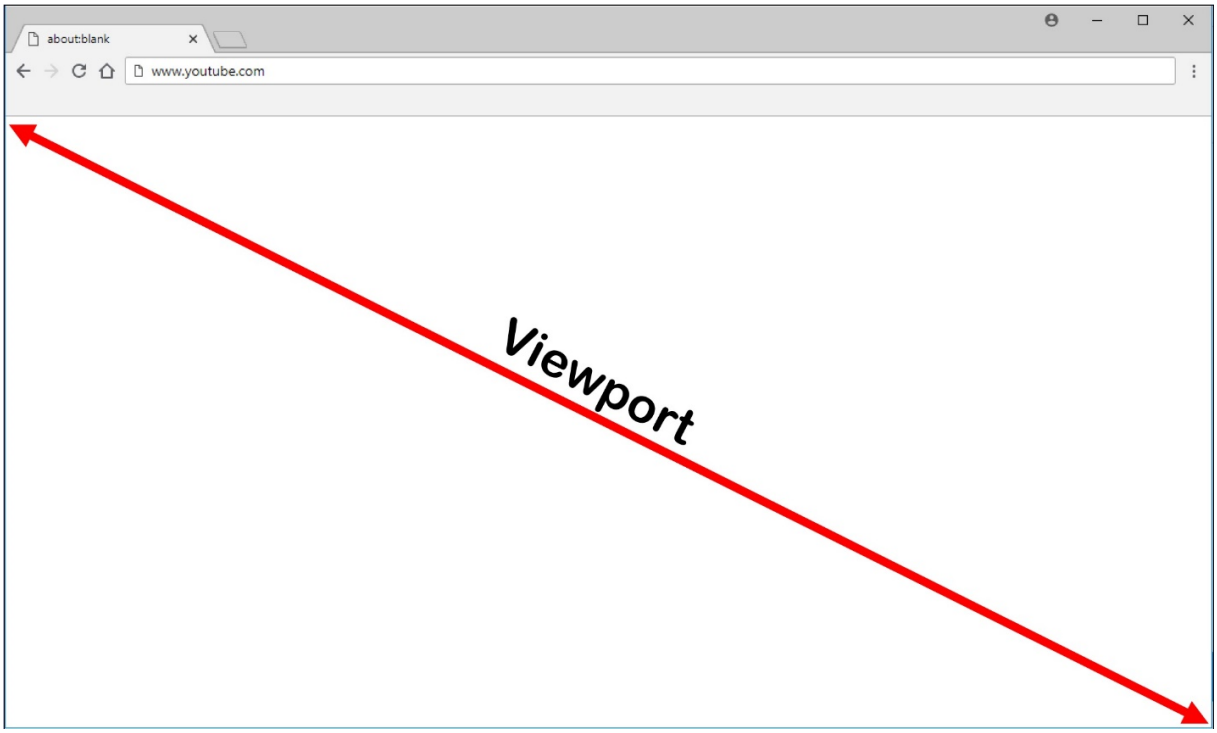
June 28, 2023

O redirecionamento de conteúdo do navegador impede a renderização de páginas da Web na lista de permissão no lado VDA. Esse recurso usa o aplicativo Citrix Workspace para instanciar um mecanismo de renderização correspondente no lado do cliente, que busca o conteúdo HTTP e HTTPS da URL.

> **Nota:**
>
> Você pode especificar que as páginas da Web sejam reorientadas ao lado VDA (e não reorientadas no lado do cliente) usando uma lista de blocos.

Esse mecanismo de layout da Web de sobreposição é executado no dispositivo de ponto de extremidade em vez de no VDA e usa o ponto de extremidade CPU, GPU, RAM e rede.

Somente o visor do navegador é redirecionado. O visor é a área retangular do seu navegador onde o conteúdo é exibido. O visor não inclui coisas como a Barra de Endereços, Barra de Ferramentas **Favoritos**, Barra de Status. Esses itens estão na interface do usuário, que ainda estão sendo executados no navegador no VDA.



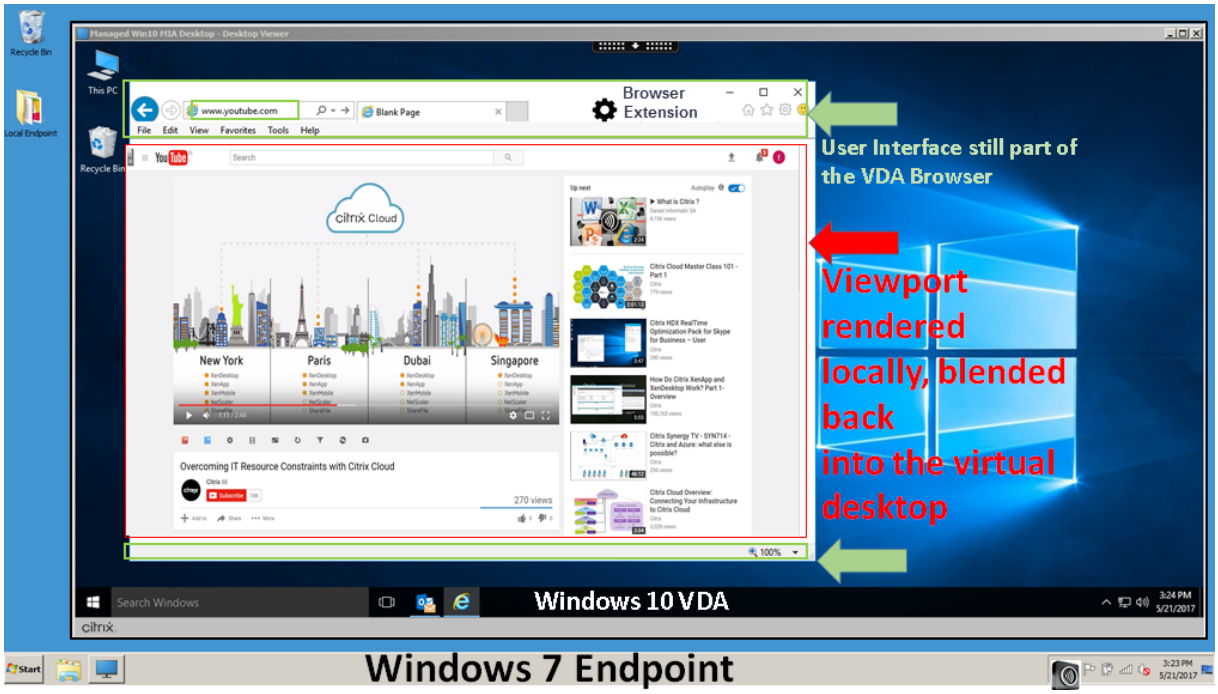
1. Configure uma política do Studio que especifique uma Lista de Controle de Acesso que contém os URLs na lista de permissões para redirecionamento ou a lista de bloqueios que desativa o redirecionamento para caminhos de URL específicos. Para que o navegador no VDA detecte que a URL para a qual o usuário está navegando corresponde à lista de permissões ou não corresponde a uma lista de bloqueios, uma extensão do navegador executa a comparação. A extensão do navegador para o Internet Explorer 11 está incluída na mídia de instalação e é instalada automaticamente. No caso do Chrome, a extensão do navegador está disponível na Chrome Web Store e você pode implantá-la usando as Políticas de Grupo e os arquivos ADMX. As extensões do Chrome são instaladas por usuário. Não é necessário atualizar uma imagem dourada para adicionar ou remover uma extensão.
2. Se for encontrada uma correspondência na lista de permissões (por exemplo `https://www.mycompany.com/`) e não houver correspondência com um URL na lista de bloqueios (por exemplo `https://www.mycompany.com/engineering`), um canal virtual (CTXCSB) instrui o aplicativo Citrix Workspace que é necessário um redirecionamento e retransmite o URL. O aplicativo Citrix Workspace instancia um mecanismo de renderização local e exibe o site.
3. O aplicativo Citrix Workspace combina o site com a área de conteúdo do navegador de desktop virtual sem interrupções.

> **Nota:**
>
> Para obter mais informações sobre o que há de novo e correções para a extensão de redirecionamento de conteúdo do navegador, acesse a Chrome Web Store e pesquise “citrix bcr”para encontrar a extensão.

A cor do logotipo especifica o status da extensão do Chrome. A cor será uma destas três:

- Verde: ativo e conectado.
- Cinza: não ativo/ocioso na guia atual.
- Vermelho: interrompido/não está funcionando.

Você pode depurar o log usando **Options** no menu de extensões.



Aqui estão os cenários de como o aplicativo Citrix Workspace busca conteúdo:

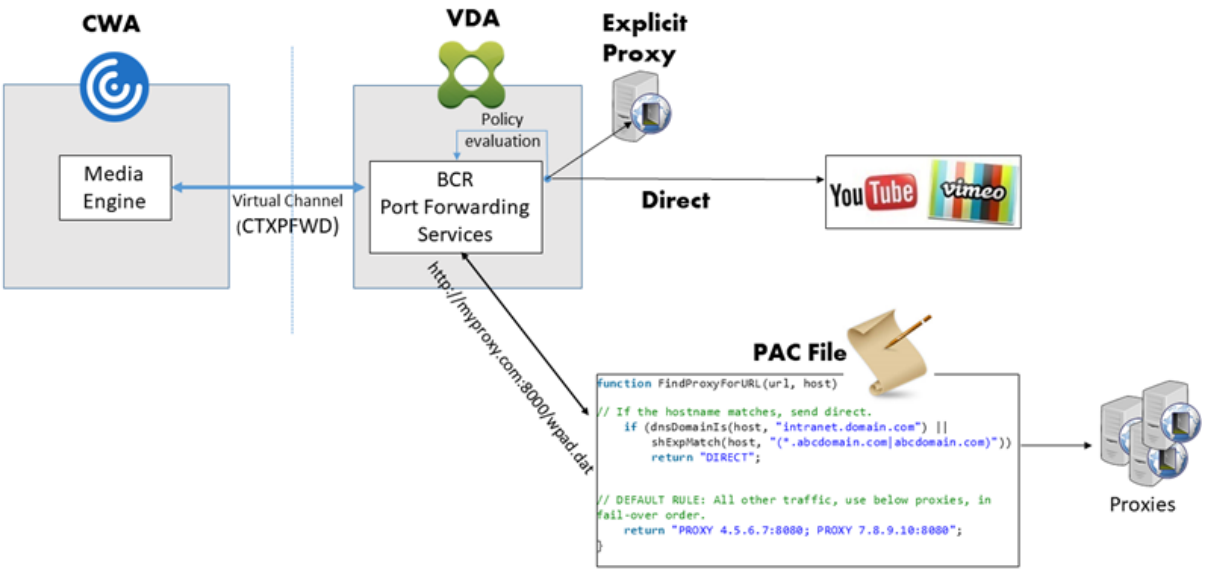
- **Obtenção no servidor e renderização no servidor**: não há redirecionamento porque você não adicionou o site à lista de permissões ou o redirecionamento foi malsucedido. Recorremos à renderização da página da Web no VDA e usamos o Thinwire para tornar os gráficos remotos. Use políticas para controlar o comportamento de fallback. Alto consumo de CPU, RAM e largura de banda no VDA.
- **Obtenção no servidor e renderização no cliente**: o aplicativo Citrix Workspace contata e busca conteúdo do servidor web por meio do VDA usando um canal virtual (CTXPFWD). Essa opção é útil quando o cliente não tem acesso à internet (por exemplo, clientes finos). Baixo consumo de CPU e RAM no VDA, mas a largura de banda é consumida no canal virtual ICA.

  Existem três modos de operação neste cenário. O termo proxy refere-se a um dispositivo proxy que o VDA acessa para obter acesso à Internet.

  Qual opção de política escolher:

  - Proxy explícito –Se você tiver um único proxy explícito no datacenter.
  - Direto ou transparente - Se você não tiver proxies ou se você usar proxies transparentes.

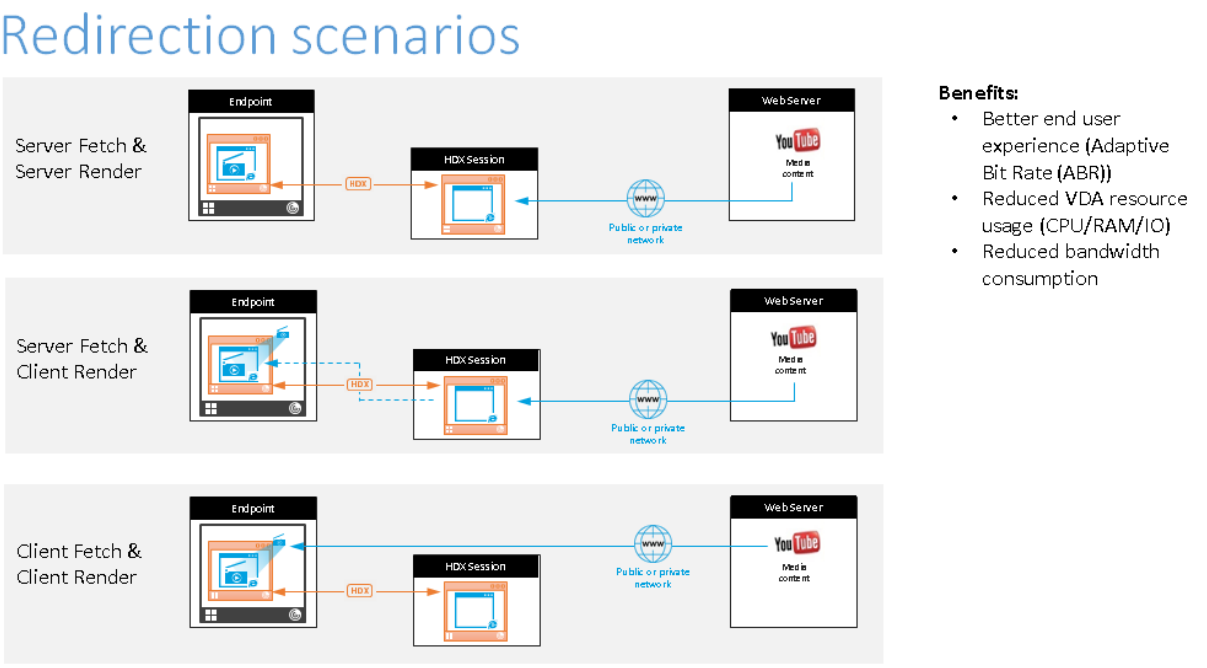
- Arquivos PAC - Se você depender de arquivos PAC para que os navegadores no VDA possam escolher automaticamente o servidor proxy apropriado para buscar um URL especificado.



- **Busca do cliente e renderização do cliente**: como o aplicativo Citrix Workspace entra em contato diretamente com o servidor da Web, ele requer acesso à internet. Esse cenário isenta todo o uso de rede, CPU e RAM do site XenApp e XenDesktop.

  Benefícios:

  - Melhor experiência do usuário final (Taxa de bits adaptável (ABR))
  - Redução do uso de recursos VDA (CPU/RAM/IO)
  - Consumo reduzido de largura de banda



Mecanismo de fallback:

Pode haver momentos em que o redirecionamento do cliente falha. Por exemplo, se a máquina cliente não tiver acesso direto à Internet, uma resposta de erro poderá voltar ao VDA. Nesses casos, o navegador no VDA pode recarregar e renderizar a página no servidor.

Você pode suprimir a renderização do servidor de elementos de vídeo usando a política existente de **prevenção de fallback de mídia do Windows**. Defina esta política para **Reproduzir todo o conteúdo somente no cliente** ou **Reproduzir apenas conteúdo acessível ao cliente no cliente**. Essas configurações bloqueiam a reprodução de elementos de vídeo no servidor se houver falhas no redirecionamento do cliente. Esta política só entra em vigor quando você habilita o redirecionamento de conteúdo do navegador e a política **Lista de Controle de Acesso** contém a URL que oferece fallback. O URL não pode estar na política de lista de bloqueios.

Requisitos do sistema:

Pontos de extremidade Windows:

- Windows 10
- Aplicativo Citrix Workspace 1809 para Windows ou posterior

> **Nota:**
>
> O redirecionamento de conteúdo do navegador é suportado apenas na versão atual (CR) do aplicativo Citrix Workspace para Windows, mas não nas versões LTSR 1912 e 2203.1 do aplicativo Citrix Workspace.

Pontos de extremidade Linux:

- Aplicativo Citrix Workspace 1808 para Linux ou posterior
- Os terminais clientes finos devem incluir WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e 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 ou posterior para Windows no ponto de extremidade 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 configurar estas opções:
    * Limpe o **Enhanced Protected Mode** em: **Internet Options** > **Advanced > Security**
    * Assinale **Enable third-party browser extensions** em: **Internet Options > Advanced > Browsing**

Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo do Knowledge Center https://support.citrix.com/article/CTX230052

Extensão de redirecionamento de conteúdo do navegador Chrome

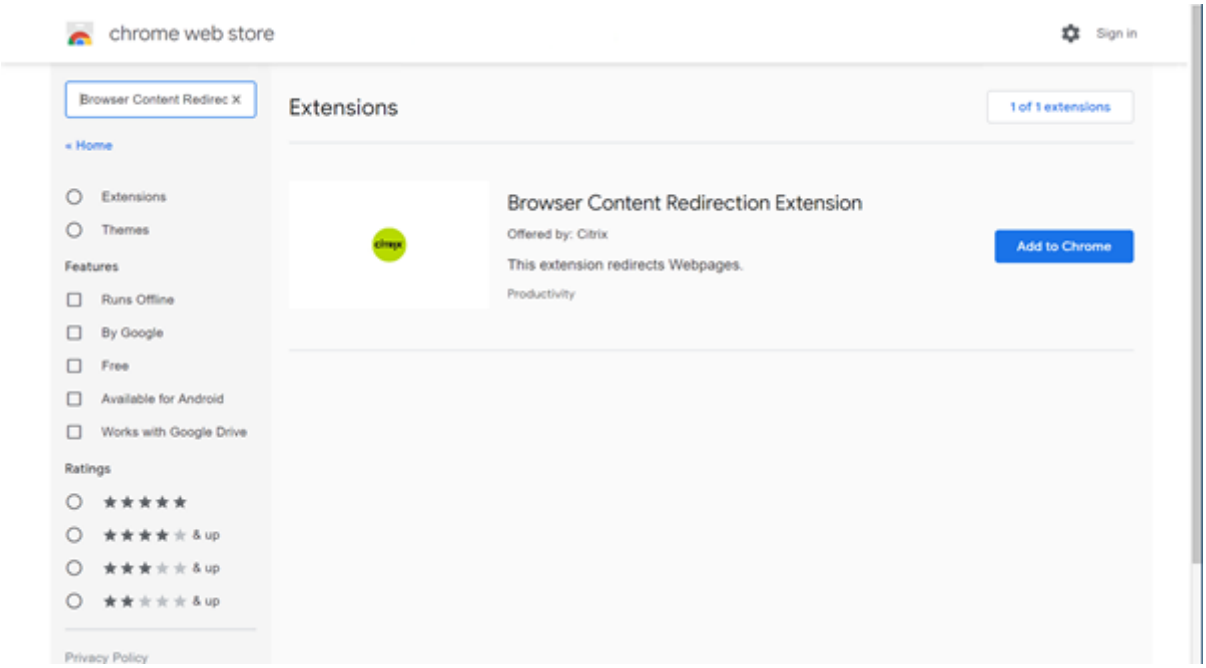
Para usar o redirecionamento de conteúdo do navegador com o Chrome, adicione a extensão de redirecionamento de conteúdo do navegador na Chrome Web Store. Clique em **Add to Chrome** no ambiente do Citrix Virtual Apps and Desktops.

A extensão **não** é necessária na máquina cliente do usuário —somente no VDA.

Requisitos do sistema

- Chrome v66 ou superior
- Extensão de redirecionamento de conteúdo do navegador
- Citrix Virtual Apps and Desktops 7 1808 ou superior
- Aplicativo Citrix Workspace 1809 para Windows ou superior

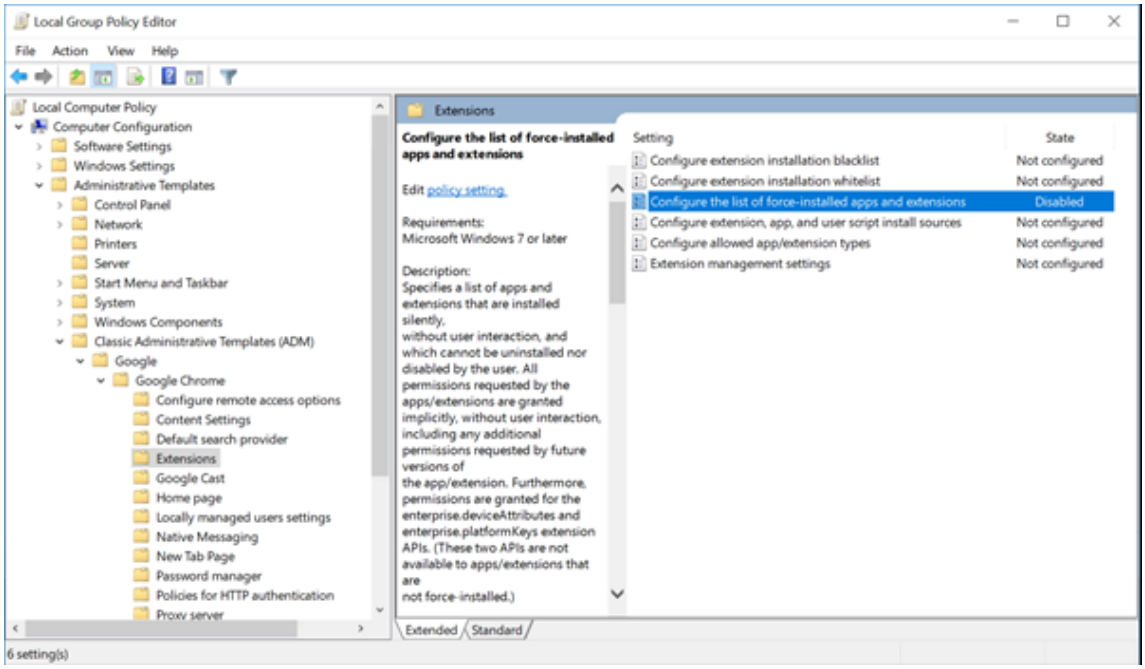
> **Nota:**
>
> O redirecionamento de conteúdo do navegador é suportado apenas na versão atual (CR) do aplicativo Citrix Workspace para Windows, mas não nas versões LTSR 1912 e 2203.1 do aplicativo Citrix Workspace.



Este método funciona para usuários individualmente. Para implantar a extensão em um grande grupo de usuários em sua organização, implante a extensão usando a Política de Grupo.

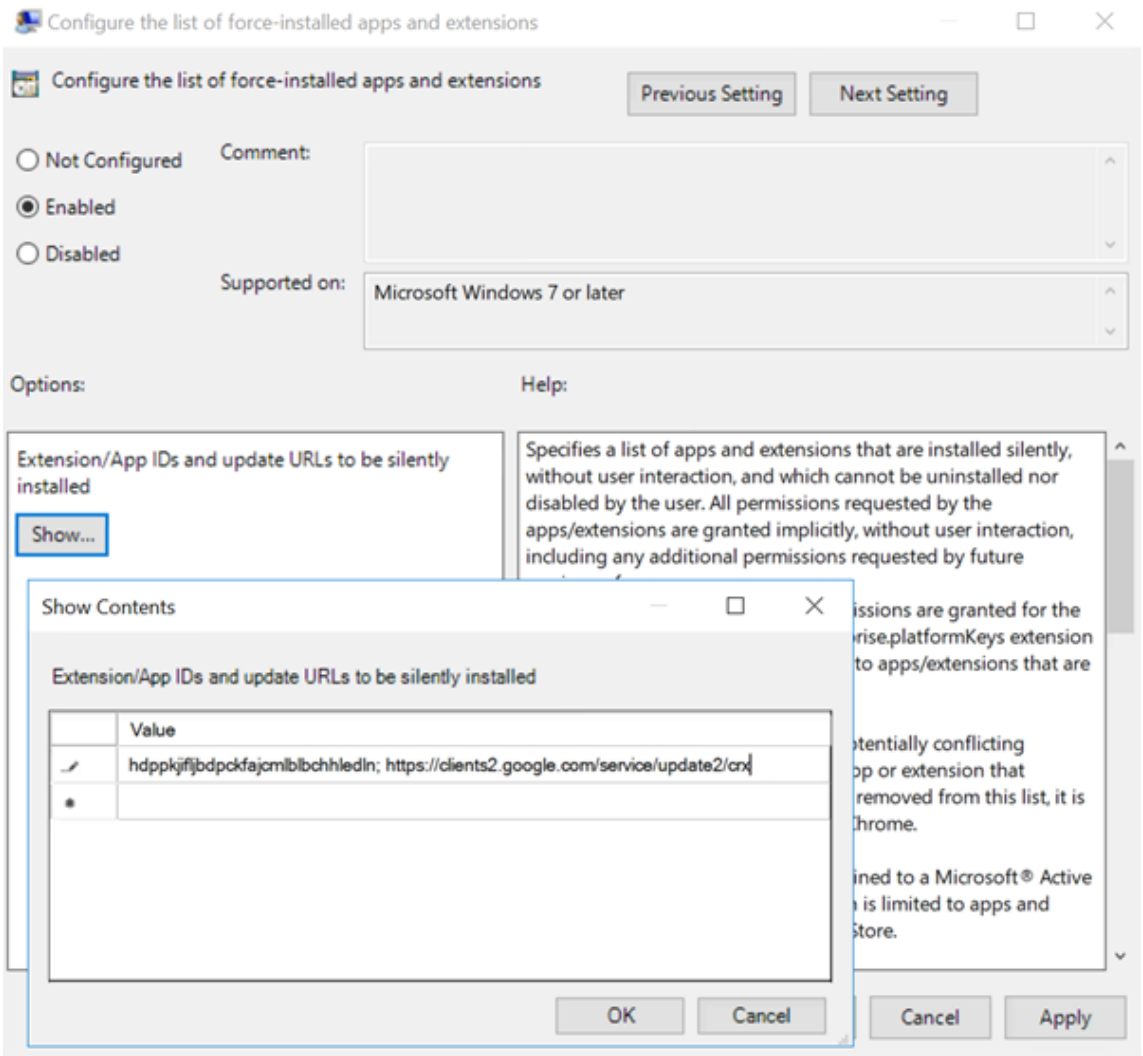
Implantar a extensão usando a Política de Grupo

1. Importe os arquivos do Google Chrome ADMX para o seu ambiente. Para obter informações sobre como baixar modelos de política e instalar e configurar os modelos no Editor de Política de Grupo, consulte Definir políticas do navegador Chrome em PCs gerenciados.
2. Abra o console de Gerenciamento de Diretiva de Grupo e vá para **User Configuration \ Administrative Templates\Classic Administrative Templates (ADM) \ Google\ Google Chrome \ Extensions**. Ative a configuração **Configure the list of force-installed apps and extensions**.



3. Clique em **Show** e digite a seguinte string, que corresponde ao ID da extensão. Atualize o URL para a extensão de redirecionamento de conteúdo do navegador.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```

4. Aplique a configuração e depois de uma atualização do **gpupdate**, o usuário recebe automaticamente a extensão. Se você iniciar o navegador Chrome na sessão do usuário, a extensão já será aplicada e não poderá ser removida.

   Todas as atualizações da extensão são instaladas automaticamente nos computadores dos usuários por meio do URL de atualização especificado na configuração.

   Se a configuração **Configure the list of force-installed apps and extensions** estiver definida como **Disabled**, a extensão será removida automaticamente do Chrome para todos os usuários.

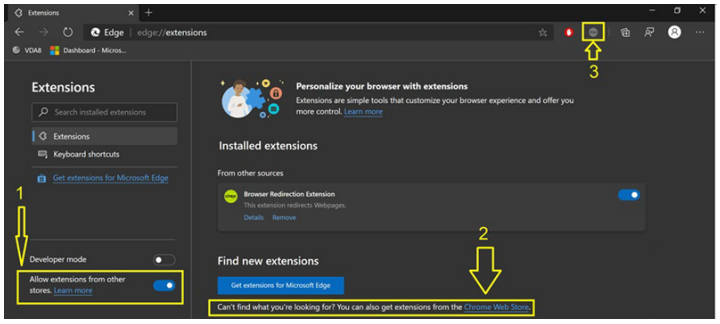
Redirecionamento de conteúdo do navegador Extensão Edge Chromium

Para instalar a extensão de redirecionamento de conteúdo do navegador no Edge, verifique se você tem instalada a versão **83.0.478.37** ou superior do navegador Edge.

1. Clique na opção **Extensions**. Escolha **Manage extension**. Ative **Allow extensions from other**

stores.

2. Clique no link **Chrome Web Store** e a extensão aparece na barra no canto superior direito. Para obter mais informações sobre extensões do Microsoft Edge, consulte Extensões.



Redirecionamento de conteúdo do navegador e DPI

Ao usar o redirecionamento de conteúdo do navegador com o DPI (dimensionamento) definido para algum valor acima de 100% na máquina do usuário, a tela de conteúdo do navegador redirecionado é exibida incorretamente. Para evitar esse problema, não defina o DPI ao usar o redirecionamento de conteúdo do navegador. Outra maneira de evitar o problema é desativar a aceleração da GPU de redirecionamento de conteúdo do navegador para o Chrome criando a chave de registro no computador do usuário. Para obter informações, consulte Redirecionamento de conteúdo do navegador e DPI na lista de recursos gerenciados pelo registro.

Logon único com autenticação integrada do Windows

O redirecionamento de conteúdo do navegador aprimora a sobreposição para usar o esquema Negociar para autenticação em servidores Web configurados com Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA.

Por padrão, o redirecionamento de conteúdo do navegador usa um esquema de autenticação básico que exige que os usuários se autentiquem com suas credenciais VDA sempre que acessarem o servidor da Web. Para logon único, você pode habilitar a configuração de política **Browser content redirection Integrated Windows Authentication support** ou criar uma chave de registro no VDA.

Antes de ativar o logon único, faça o seguinte:

- Configure a infraestrutura Kerberos para emitir tickets para SPNs (nomes principais de serviço) construídos a partir do nome do host. Por exemplo, `HTTP/serverhostname.com`.
- Para busca do servidor: Quando você usa o redirecionamento de conteúdo do navegador no modo de busca do servidor, verifique se o DNS está configurado corretamente no VDA.

- Para busca do cliente: quando você usa o redirecionamento de conteúdo do navegador no modo de busca do cliente, verifique se o DNS está configurado corretamente no dispositivo cliente e que você permite 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 Browser content redirection Integrated Windows Authentication support .

Como alternativa, você pode habilitar o logon único em um servidor Web adicionando uma chave de registro no VDA. Para obter informações, consulte Single sign-on with Integrated Windows Authentication for browser content redirection na lista de recursos gerenciados por meio do registro.

Cabeçalho de solicitação do agente do usuário

O cabeçalho usuário-agente ajuda a identificar solicitações HTTP enviadas pelo redirecionamento de conteúdo do navegador. Essa configuração pode ser útil quando você configura regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas do redirecionamento de conteúdo do navegador, você poderá criar uma regra que contenha o cabeçalho usuário-agente para ignorar determinados requisitos.

Somente dispositivos Windows suportam o cabeçalho de solicitação de agente-usuário.

Por padrão, a string de cabeçalho de solicitação agente-usuário está desabilitada. Para habilitar o cabeçalho agente-usuário para conteúdo renderizado pelo cliente, use o Editor do Registro. Para obter informações, consulte User-agent request header na lista de recursos gerenciados por meio do registro.

Compatibilidade do cliente de redirecionamento de conteúdo do navegador

Você pode usar o WMI para verificar se o seu cliente é compatível com o redirecionamento de conteúdo do navegador. Use qualquer método para acessar os trabalhos do WMI. Veja a seguir um exemplo usando o PowerShell.

1. Abra o PowerShell.
2. Execute `Get-WmiObject -Class CTXBCRStatus`.
3. Verifique o parâmetro `BCR_Capable`.
    - Se `True`, o cliente é compatível com o redirecionamento de conteúdo do navegador.
    - Se `False`, o cliente não é compatível com o redirecionamento de conteúdo do navegador.

Informações adicionais

- Se `CtxBrowserSvc` não estiver disponível, nenhum resultado será exibido ao executar o comando.

- Se `CtxBrowserSvc` nunca tiver sido executado, os resultados retornarão um erro de classe inválido.

Videoconferência HDX e compressão de vídeo na webcam

June 28, 2023

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

As webcams podem ser usadas por aplicativos executados dentro da sessão virtual usando a compactação de vídeo da webcam HDX ou o redirecionamento USB genérico HDX plug-and-play. Use o **Citrix Workspace app > Preferences > Devices** para alternar entre modos. A Citrix recomenda que você sempre use a compactação de vídeo de webcam HDX, se possível. O redirecionamento USB genérico HDX é recomendado somente quando há problemas de compatibilidade de aplicativos com compactação de vídeo HDX ou quando você precisa de funcionalidades nativas avançadas da webcam. Para um melhor desempenho, a Citrix recomenda que o Virtual Delivery Agent tenha pelo menos duas CPUs virtuais.

Para evitar que os usuários mudem a compactação de vídeo da webcam HDX, desative o redirecionamento do dispositivo USB usando as configurações da política em Configurações de política em **ICA policy settings > USB Devices policy**. Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração de microfone e webcam do Desktop Viewer **Don't use my microphone or webcam**.

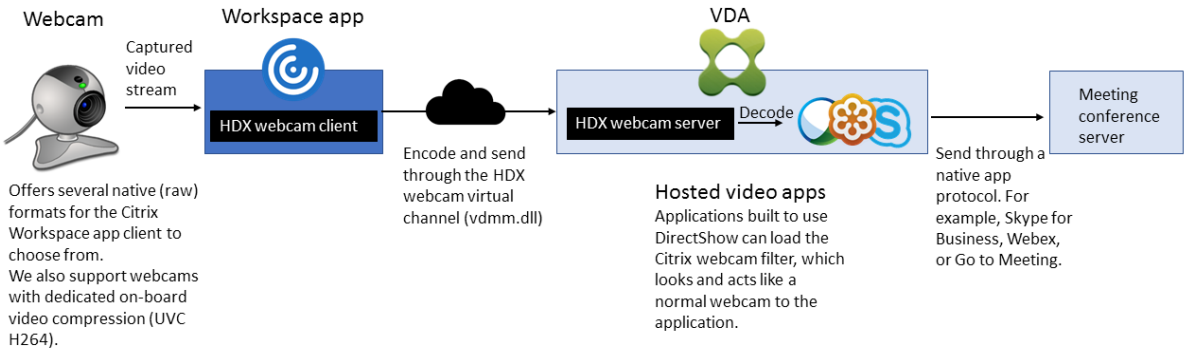
Compactação de vídeo de webcam HDX

A compactação de vídeo da webcam HDX também é chamada de modo **Optimized** de webcam. Esse tipo de compressão de vídeo da webcam envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compactação de webcam HDX não codifica, transcodifica e decodifica vídeo da webcam. Esse recurso é ativado por padrão.

Para desativar o streaming direto de vídeo do servidor para o aplicativo de videoconferência, defina a chave do registro como 0 no VDA. Para obter informações, consulte Compressão de vídeo da webcam na lista de recursos gerenciados por meio do registro.

Se você desabilitar a funcionalidade padrão para recursos de streaming de vídeo, a compactação de vídeo de webcam HDX usará a tecnologia de estrutura multimídia que faz parte do sistema operacional cliente para interceptar vídeo de dispositivos de captura, transcodificar e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do sistema operacional.

O cliente lida com a comunicação com a webcam. Em seguida, o cliente envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua integração lhe proporciona o mesmo efeito em sua área de trabalho. O aplicativo Workspace compacta o vídeo para economizar largura de banda e fornecer melhor resiliência em cenários de WAN.



A política **Multimedia conferencing** deve estar habilitada para compactação de vídeo de webcam HDX. Essa política está ativada por padrão.

Se uma webcam suportar codificação de hardware, a compactação de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compactação de software, edite a chave do registro no cliente. Para obter informações, consulte Compactação de software da webcam na lista de recursos gerenciados por meio do registro.

Requisitos de compactação de vídeo de webcam HDX

A compactação de vídeo de webcam HDX suporta as seguintes versões do aplicativo Citrix Workspace:

Plataforma	Processador
Aplicativo Citrix Workspace para Windows	O aplicativo Citrix Workspace para Windows oferece suporte à compactação de vídeo de webcam para aplicativos de 32 bits e 64 bits no XenApp e XenDesktop 7.17 e versões posteriores. Em versões anteriores, o aplicativo Citrix Workspace para Windows suporta apenas aplicativos de 32 bits.
Aplicativo Citrix Workspace para Mac	O aplicativo Citrix Workspace para Mac 2006 ou posterior suporta compactação de vídeo de webcam para aplicativos de 64 bits no XenApp e XenDesktop 7.17 e posteriores. Em versões anteriores, o aplicativo Citrix Workspace para Mac suporta apenas aplicativos de 32 bits.
Aplicativo Citrix Workspace para Linux	O aplicativo Citrix Workspace para Linux suporta aplicativos de 32 bits e 64 bits na área de trabalho virtual.
Aplicativo Citrix Workspace para Chrome	Como alguns Chromebooks ARM não suportam codificação H.264, apenas aplicativos de 32 bits podem usar a compactação de vídeo de webcam HDX otimizada.

Os aplicativos de vídeo baseados em base de mídia suportam compactação de vídeo de webcam HDX no Windows 8.x ou superior e Windows Server 2012 R2 e superior. Para obter mais informações, consulte o artigo do Knowledge Center CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.
- Webcam compatível com DirectShow (use as configurações padrão da webcam). As webcams capazes de codificação de hardware reduzem o uso da CPU do lado do cliente.
- Para compactação de vídeo de webcam HDX, instale drivers de webcam no cliente, obtidos do fabricante da câmera, se possível. A instalação dos drivers de dispositivo não é necessária no servidor.

Cada webcam oferece taxas de quadros diferentes e tem diferentes níveis de brilho e contraste. Ajustar o contraste da webcam pode reduzir significativamente o tráfego a montante. A Citrix usa as seguintes webcams para validação inicial de recursos:

- Modelos Microsoft LifeCam VX (2000, 3000, 5000, 7000)

- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar a taxa de quadros de vídeo preferida, edite a chave de registro no cliente. Para obter informações, consulte Taxa de quadros de compressão de vídeo da webcam na lista de recursos gerenciados pelo registro.

Streaming de webcam de alta definição

O aplicativo de videoconferência no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão começa, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo. Quando a webcam e o aplicativo de videoconferência suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Damos suporte a resoluções de webcam até 1920x1080.

Esse recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver for Windows, versão mínima 4.10.

Você pode usar uma chave de registro para desativar e habilitar o recurso. Para obter informações, consulte Streaming de webcam de alta definição na lista de recursos gerenciados por meio do registro.

Se a negociação de tipo de mídia falhar, o HDX cai de volta à resolução padrão de 352x288 CIF. Você pode usar chaves de registro no cliente para configurar a resolução padrão. Verifique se a câmera suporta a resolução especificada: Para obter informações, consulte Resolução de webcam de alta definição na lista de recursos gerenciados por meio do registro.

A compactação de vídeo de webcam HDX usa significativamente menos largura de banda em comparação com o redirecionamento USB genérico plug-and-play e funciona bem em conexões WAN. Para ajustar a largura de banda, configure a chave de registro no cliente. Para obter informações, consulte Largura de banda de webcam de alta definição na lista de recursos gerenciados por meio do registro.

Digite um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usam 350000 bps por padrão.

O HDX plug-and-play redirecionamento USB genérico

O redirecionamento USB genérico HDX plug-and-play (isócrono) também é chamado de modo de webcam **genérico**. O benefício do redirecionamento USB genérico HDX plug-and-play é que você não precisa instalar drivers em seu cliente fino/ponto de extremidade. A pilha USB é virtualizada de tal

forma que qualquer coisa que você conecta ao cliente local seja enviada à VM remota. A área de trabalho remota age como se você o conectasse de modo nativo. A área de trabalho do Windows lida com toda a interação com o hardware e executa a lógica plug-and-play para encontrar os drivers corretos. A maioria das webcams funciona se os drivers existirem no servidor e puderem funcionar via ICA. O modo de webcam genérico usa significativamente mais largura de banda (muitos megabits por segundo) porque você está enviando vídeo não compactado para baixo com o protocolo USB pela rede.

Redirecionamento multimídia HTML5

June 28, 2023

O redirecionamento multimídia HTML5 estende os recursos de redirecionamento multimídia do HDX MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento na distribuição on-line de conteúdo multimídia, especialmente para dispositivos móveis, o setor de navegadores desenvolveu formas mais eficientes de apresentar áudio e vídeo.

O Flash é o padrão, mas requer um plug-in, não funciona em todos os dispositivos e causa maior uso de bateria em dispositivos móveis. Empresas como YouTube, Netflix e versões de navegadores mais recentes do Mozilla, Google e Microsoft estão passando para HTML5, tornando-o o novo padrão.

A multimídia baseada em HTML5 tem muitas vantagens em relação aos plug-ins proprietários, incluindo:

- Padrões independentes da empresa (W3C)
- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança criados pelos plug-ins

Downloads progressivos de HTTP

O download progressivo de HTTP é um método de pseudo-streaming baseado em HTTP que é compatível com HTML5. Em um download progressivo, o navegador reproduz um único arquivo (codificado em uma única qualidade) enquanto ele está sendo baixado de um servidor web HTTP. O vídeo é armazenado na unidade como é recebido e é reproduzido a partir dessa unidade. Se você assistir novamente o vídeo, o navegador poderá carregar o vídeo a partir do cache.

Para obter um exemplo de download progressivo, consulte a página de teste de redirecionamento de vídeo HTML5. Para inspecionar os elementos de vídeo na página da Web e encontrar as fontes (formato de contêiner mp4) em tags de vídeo HTML5, use as ferramentas de desenvolvedor no seu navegador:

Comparação entre HTML5 e Flash

Recurso	HTML5	Flash
Requer um player proprietário	Não	Sim
Funciona em dispositivos móveis	Sim	Alguns
Velocidade de execução em diferentes plataformas	Alta	Lenta
Suportado pelo iOS	Sim	Não
Uso de recursos	Menos	Mais
Carga mais rápida	Sim	Não

Requisitos

Oferecemos suporte apenas ao redirecionamento para downloads progressivos no formato mp4. Não oferecemos suporte a WebM e tecnologias de streaming de taxa de bits adaptativa como DASH/HLS.

Oferecemos suporte ao seguinte e usamos políticas para o respectivo controle. Para obter mais informações, consulte Configurações de política multimídia.

- Renderização no lado do servidor
- Obtenção no servidor e renderização no cliente
- Obtenção e renderização do lado do cliente

Versões mínimas do aplicativo Citrix Workspace e Citrix Receiver:

- Aplicativo Citrix Workspace 1808 para Windows
- Citrix Receiver para Windows 4.5
- Aplicativo Citrix Workspace 1808 para Linux
- Citrix Receiver para Linux 13.5

Versão mínima do navegador VDA	SO Windows - versão/compilação/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 7 x86 e x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Versão mínima do navegador VDA	SO Windows - versão/compilação/SP
Firefox 47 Adicione manualmente os certificados ao repositório de certificados do Firefox ou configure o Firefox para procurar certificados de um repositório de certificados confiáveis do Windows. Para obter mais informações, consulte https://wiki.mozilla.org/CA:AddRootToFirefox	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows 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** –Gancho de JavaScript que intercepta comandos de vídeo no site. O HdxVideo.js se comunica com WebSocketService por meio de Secure WebSockets (SSL/TLS).
- **Certificados SSL WebSocket**
  - Para 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)
    Location: **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)
    Location: **Certificates (Local Computer) > Personal > Certificates**.
- **WebSocketService.exe** - É executado no sistema local e executa a terminação SSL e o mapeamento da sessão do usuário. TLS Secure WebSocket escutando em 127.0.0.1, porta 9001.
- **WebSocketAgent.exe** - É executado na sessão do usuário e renderiza o vídeo conforme instruído a partir de comandos WebSocketService.

Como faço para habilitar o redirecionamento de vídeo HTML5?

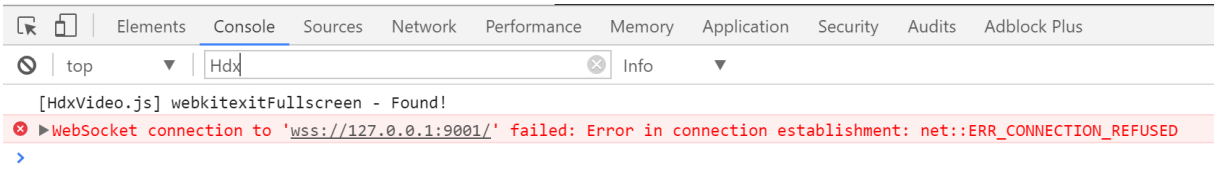
Nesta versão, esse recurso está disponível apenas para páginas da Web controladas. Ele requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas da Web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de taxas de bits adaptativas (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não têm suporte.

Para obter mais informações, consulte *Configurações de política multimídia*.

Dicas de solução de problemas

Podem ocorrer erros quando a página da Web tenta executar HdxVideo.js. Se o JavaScript não carregar, o mecanismo de redirecionamento HTML5 não funcionará. Verifique se não há erros relacionados ao HdxVideo.js inspecionando o console nas janelas de ferramentas de desenvolvedores do seu navegador. Por exemplo:



Otimização para Microsoft Teams

June 28, 2023

A Citrix oferece otimização para Microsoft Teams baseados em desktop usando o Citrix Virtual Apps and Desktops e o aplicativo Citrix Workspace. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

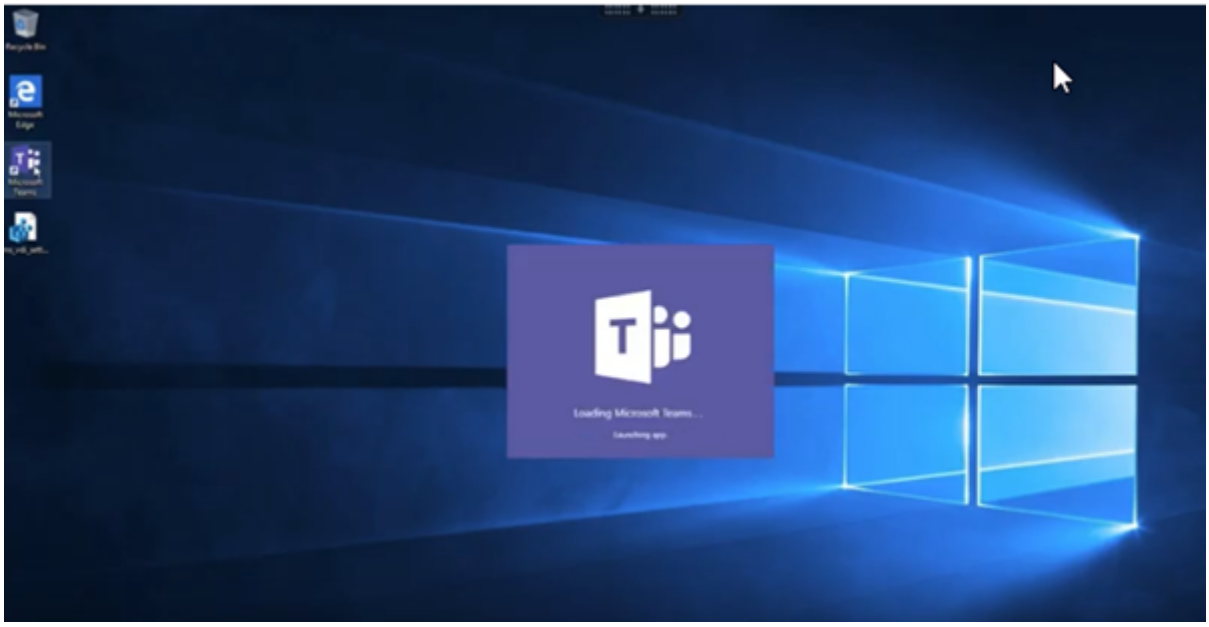
Nossa otimização para o Microsoft Teams inclui serviços HDX do lado do VDA e API para fazer interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O ponto de extremidade decodifica e renderiza a multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem de forma nativa no aplicativo hospedado pelo Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um comando e controle de canal virtual. Isso significa que não há troca de mídia entre o aplicativo Citrix Workspace e o VDA.

Apenas a busca de cliente/renderização do cliente está disponível.

Esta demonstração de vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam o uso da versão mais recente disponível do Microsoft Teams e que a mantenham atualizada.
As versões do aplicativo de desktop Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas.
Versões não suportadas do aplicativo de desktop Microsoft Teams mostram uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Microsoft Teams (Desktop e Mac).

Recomendamos que você siga as diretrizes de instalação em todo o computador do Microsoft Teams. Evite usar o instalador .exe que instala o Microsoft Teams no `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` da linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Quando você define esse parâmetro, o Instalador de Todo o Computador do Microsoft Teams aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro

`ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` somente em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não é atualizado automaticamente sempre que há uma nova versão. Recomendamos esse modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou áreas de trabalho fora de catálogos aleatórios/agrupados do Windows Server ou Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação da VDI).

Suponha que você tem ambientes VDI persistentes dedicados do Windows 10. Você deseja que o aplicativo Microsoft Teams atualize automaticamente e prefere que o Microsoft Teams instale por usuário em `Appdata/Local`. Nesse caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> Recomendamos instalar o VDA antes de instalar o Microsoft Teams na imagem de ouro. Esta ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA foi, desinstale e reinstale o Microsoft Teams.

Para Remote PC Access

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior depois de instalar o VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 ou posterior inclui lógica aumentada executada no momento da inicialização do Microsoft Teams e no momento do login para a detecção do VDA. Essas versões também incluem a identificação do tipo da sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem não detectar e desativar determinados recursos ou elementos da interface do usuário. Por exemplo, salas simultâneas, janelas pop-out de reuniões e chat, ou reações da reunião.

> **Importante:**
>
> Quando você faz roaming de uma sessão local para uma sessão HDX com o Microsoft Teams ainda aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar com o HDX corretamente.
> Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Quando estiver trabalhando no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do Remote PC Access (HDX ou local). Isso porque o Microsoft Teams só pode avaliar o modo VDI no momento da inicialização do aplicativo, não quando ele já está sendo executado em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-up, salas simultâneas ou

> reações à reunião.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações do VDA e do Microsoft Teams em camadas diferentes, você deve criar uma chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em Multimídia.

Recomendações de gerenciamento de perfis

Recomendamos usar o instalador em toda o computador para ambientes Windows Server e VDI em pool no Windows 10.

Quando o sinalizador **ALLUSER =1** é passado para o MSI a partir da linha de comando (o instalador em todo o computador), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~ 300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600—700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**
>
> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em:`HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> Um logon de usuário subsequente aciona a instalação final em **AppData**, em vez disso.

Instalador em toda a máquina

Veja a seguir um exemplo de pastas, atalhos de área de trabalho e registros criados com a instalação do instalador do Microsoft Teams em todo o computador em uma VM de 64 bits do Windows Server 2016:

Pasta:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho da área de trabalho:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registro:

- HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Nome: Teams
- Tipo: REG_SZ
- Valor: C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

> **Nota:**
>
> A localização do registro varia de acordo com os sistemas operacionais subjacentes e o número de bits.

Recomendações, em Recommendations

- Recomendamos desativar o início automático excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do dia de trabalho) sobrecarreguem a CPU da VM.
- Se o Virtual Desktop não tiver uma GPU/vGPU, recomendamos a configuração **Desabilitar a aceleração de hardware GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada `%Appdata%\Microsoft\Teams` em `desktop-config.json`. Você pode usar um script de logon para editar esse arquivo e definir o valor como **true**.
- Se estiver usando o Citrix Workspace Environment Management (WEM), ative o **CPU Spikes Protection** para gerenciar o consumo do processador para o Microsoft Teams.

Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação é diferente. Todos os arquivos são colocados em AppData.

Pasta:

- C:\Users\<username>\AppData\Local\Microsoft\Teams
- C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin
- C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin
- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

Atalho da área de trabalho:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```


Registro:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Melhores práticas

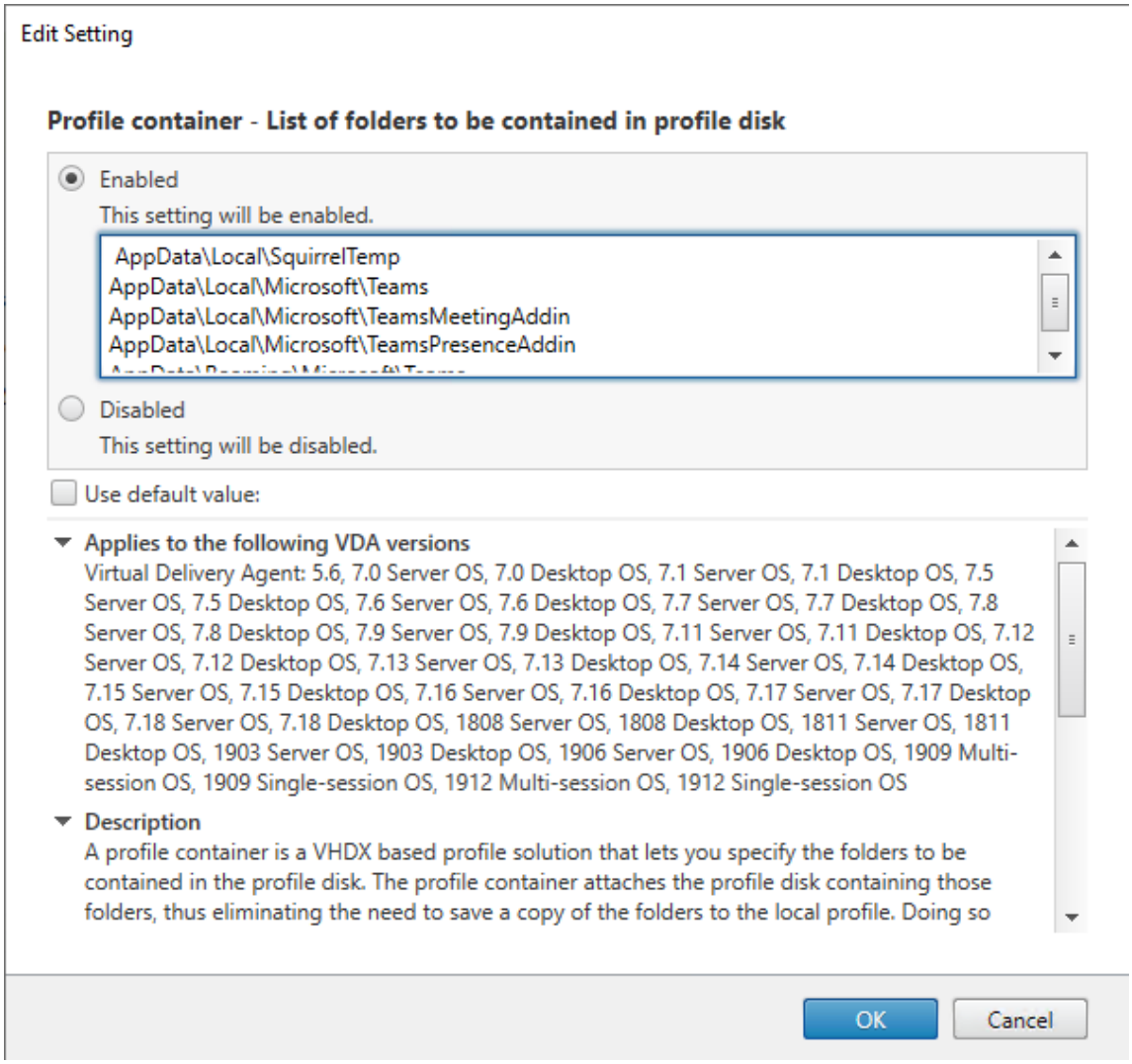
As recomendações de melhor prática baseiam-se nos cenários de caso de uso.
O uso do Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente de dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as informações específicas do usuário apropriadas são armazenadas em cache durante a sessão do usuário. Por exemplo, as informações específicas do usuário incluem dados do usuário, perfil e configurações. Sincronize os dados nessas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Lista de exclusão de conteúdo armazenado em cache do Microsoft Teams para configuração não persistente Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams, conforme descrito na documentação da Microsoft . Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais a configuração não persistente.

Caso de uso: cenário de sessão única Nesse cenário, o usuário final usa o Microsoft Teams em um local de cada vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Por exemplo, em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop e o Microsoft Teams é implantado na área de trabalho virtual como um aplicativo.
Recomendamos ativar o contêiner Citrix Profile e redirecionar diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador de toda a máquina do Microsoft Teams (**ALLUSER=1**) na imagem de ouro.
2. Ative o Citrix Profile Management e configure o armazenamento de perfis de usuário com as permissões apropriadas.
3. Ative a seguinte configuração de política do Profile Management: **File system > Synchronization > Profile container –Lista de pastas que devem estar no disco de perfil**.



Liste todos os diretórios por usuário nessa configuração. Você também pode configurar essas configurações usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

Requisitos do sistema

Versão mínima recomendada - Delivery Controller (DDCs) 1906.2

Se você estiver usando uma versão anterior, consulte Ativar a otimização do Microsoft Teams:

Sistemas operacionais compatíveis:

- Windows Server 2022, 2019, 2016, 2012R2, edições Standard e Datacenter, e com a opção Server Core

Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais compatíveis:

- Windows 11.
- Windows 10 64 bits, versões 1607 e posteriores. Os aplicativos hospedados na máquina virtual são compatíveis com o aplicativo Citrix Workspace para Windows 2109.1 ou versões posteriores.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edições Standard e Datacenter).

Requisitos:

- BCR_x64.msi - o MSI que contém o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não a exclua.

Versão recomendada —aplicativo Citrix Workspace para Windows mais recente CR e versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 bits e 64 bits, incluindo edições Embedded) (suporte para Windows 7 interrompido na versão 2006) (suporte para Windows 8.1 interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas do processador (CPU) suportadas: x86 e x64 (o ARM não é suportado).
- Requisito de ponto de extremidade: CPU dual core de aproximadamente 2,2 a 2,4 GHz que pode dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs de núcleo duplo ou quádruplo com velocidades de base mais baixas (~ 1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Clientes finos HP verificados: t630/t640, t730/t740, mt44/mt45.
- Clientes finos Dell verificados: 5070, 5470 Mobile TC e AIO.
- Clientes finos 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de pontos de extremidade verificados, consulte Clientes finos.
- O aplicativo Citrix Workspace requer um mínimo de 600 MB de espaço livre em disco e 1 GB de RAM.
- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se não estiver presente no sistema.

Os administradores podem ativar/desativar o Microsoft Teams iniciando no modo otimizado alterando a política de otimização do Microsoft Teams. Os usuários que começam no modo otimizado no aplicativo Citrix Workspace não têm a opção de desativar o Microsoft Teams.

Versão mínima - aplicativo Citrix Workspace 2006 para Linux

Para obter mais informações, consulte Otimização para Microsoft Teams na documentação do aplicativo Citrix Workspace para Linux.

Software:

- `GStreamer` 1.0 ou posterior ou Cairo 2
- libc++-9.0 ou posterior
- `libgdk` 3.22 ou posterior
- OpenSSL 1.1.1d
- Distribuição Linux x64

Hardware:

- CPU dual-core mínima de 1,8 GHz que possa dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com uma velocidade base de 1,8 GHz e uma alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de pontos de extremidade verificados, consulte Clientes finos.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desativar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é VDWEBRTC=On. Depois que a atualização for concluída, reinicie a sessão. (É necessária permissão raiz).

Versão mínima - Aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais compatíveis:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 ou posterior.
- macOS Monterey.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Nota:**
>
> O aplicativo Citrix Viewer requer acesso às preferências de segurança e privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência no

> **menu Apple > Preferências do sistema > Segurança e privacidade > guia Privacidade > Screen recording** e selecionam **Citrix Viewer**.

A otimização do Microsoft Teams funciona por padrão se o usuário tiver o aplicativo Citrix Workspace 2012 ou posterior e o macOS 10.15.

Se você deseja desativar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versão mínima –Versão mais recente do aplicativo Citrix Workspace para ChromeOS em execução na versão mais recente do ChromeOS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core de 2,4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desativada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de um único servidor

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) são suportados em um único host físico. Isso é comumente chamado de Citrix Virtual Apps and Desktops Single Server Scalability (SSS). No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade do usuário. A ideia é descobrir quantos usuários ou máquinas virtuais podem ser executados em um único equipamento de hardware executando um hipervisor principal.

> **Nota:**
>
> Esta seção inclui uma orientação para fazer uma estimativa de SSS. A orientação é de alto nível e pode não ser necessariamente específica para sua situação ou ambiente exclusivo. A única maneira de realmente entender o Citrix Virtual Apps and Desktops SSS é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda seguir essa orientação e essas regras simples para fazer uma estimativa rápida apenas da SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar equipamentos de hardware ou tomar qualquer decisão

> financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máximo Turbo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- 6 TB de armazenamento SSD RAID 0 local (11 discos)

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando o Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminologia

- Carga de trabalho do Knowledge Worker: inclui Acrobat Reader, Freemind/Java, Photo viewer, Edge e aplicativos MS Office, como Excel, Outlook, PowerPoint e Word.
- Baseline: os testes de escalabilidade do servidor são executados com a carga de trabalho do Knowledge Worker (sem o Microsoft Teams).
- Carga de trabalho do Microsoft Teams: carga de trabalho típica do Knowledge Worker + Microsoft Teams.

Como é realizado o teste de estresse no Microsoft Teams

- O Microsoft Teams é otimizado com o HDX. Portanto, todo o processamento multimídia é descarregado para o ponto de extremidade ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou eliminados antes do início da carga de trabalho.
- Abra o Microsoft Teams (inicialização a frio).
- Meça o tempo gasto pelo Microsoft Teams para carregar e capturar o foco da janela principal do Microsoft Teams.
- Alterne para a janela de bate-papo usando atalhos de teclado.
- Alterne para a janela do calendário usando atalhos de teclado.
- Envie a mensagem de bate-papo para um usuário específico usando atalhos de teclado.
- Alterne para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- 40% de impacto na escalabilidade com o Microsoft Teams Workload (81 usuários), quando comparado ao Baseline (137 usuários).
- Aumentar a capacidade do servidor em ~40% (na CPU) restaura o número de usuários como com a carga de trabalho Baseline.
- 20% de memória extra necessária com o Microsoft Teams Workload, quando comparado ao Baseline.
- Aumento do tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% em gravações de IOPS, aumento de ~100% em leituras de IOPS. O Microsoft Teams pode ter um impacto significativo no ambiente com armazenamento mais lento.

Matriz de recursos e compatibilidade de versões

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR	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	Aplicativo Citrix Workspace para ChromeOS
Áudio/Vídeo (P2P e conferência)	Versão atual menos 90 dias	1906	1907	Sim	Sim	Sim	2009	2004	2105.5
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	Sim	Sim	Sim	2012	2006	2105.5 (1)

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	Aplicativo Citrix Workspace para ChromeOS
i. Indicador de tela Borda vermelha	Versão atual menos 90 dias	1906	2002	Sim	Sim	Sim	2012	2006	Não
ii. Limitar captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	Não	Sim	Sim	2012	2006	Não
iii. Multimonitor	Versão atual menos 90 dias	1912 CU6+	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 Proxy Server	Versão atual menos 90 dias	N/A	2012 (3)	Não	Sim (3) (5)	Sim (3) (5)	2104 (4)	2101 (4)	2303

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	Aplicativo Citrix Workspace para ChromeOS
Compartilhamento de aplicativos	Versão atual menos 90 dias	2109	2109.1	Não	Não	Não	2203.1	2209	Não
Legendas ao vivo	Versão atual menos 90 dias	N/A (7)	2109.1	Não	Não	Não	2109	2109	2303
e911 dinâmico	Versão atual menos 90 dias	N/A	2112.1	Não	Não	Não	2112	2112	2112
Dar/solicitar controle	Versão atual menos 90 dias	N/A	2112.1	Não	Não	Não	2203.1	2203	2303
Várias janelas	1.5.00.11825	2112	2112.1	Não	Não	Não	2203.1	2203	2303
Transcrições de reuniões	Versão atual menos 90 dias	2112.1	2112	Não	Não	Não	2203.1	2203	2303
Desfoque do fundo	Versão atual menos 90 dias	2112	2207	Não	Não	Não	2301	2212	2303

1. Desativado por padrão, requer que o administrador ative.
2. CD Viewer somente no modo de tela cheia. SHIFT+F2 não suportado.
3. Negociar/Kerberos, NTLM, Basic e Digest. Pac os arquivos também são suportados.
4. Somente anônimo.
5. Somente no SO Windows 10, Windows IoT Client.
6. Recursos atualmente não disponíveis no Microsoft Teams. Para obter informações sobre o ETA, acesse https://www.microsoft.com/ e pesquise o roadmap do Microsoft 365.
7. Se o VDA for 2112 ou superior, a legenda ao vivo só funcionará se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 para Linux ou 2112 para Windows. Isso ocorre porque as legendas ao vivo se comportam de maneira diferente se o Microsoft Teams está no modo de IU de Janela única ou no modo Várias janelas.

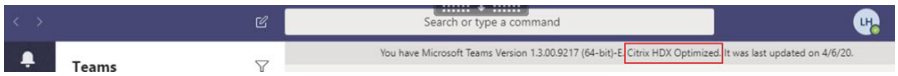
> **Nota:**
>
> Todos os recursos listados no **aplicativo Citrix Workspace para Windows 1912 CU6 (ou posterior)** são aplicáveis ao aplicativo Citrix Workspace para Windows 2203.1 LTSR CU1.

Ativar a otimização do Microsoft Teams

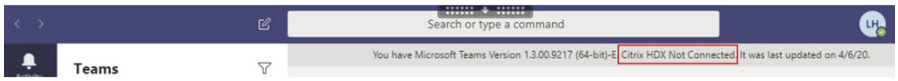
Para habilitar a otimização para o Microsoft Teams, use a política Gerenciar console descrita na política de redirecionamento do Microsoft Teams. Essa política está **ATIVADA** por padrão. Além da ativação dessa política, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima necessária. Se você habilitou a política e a versão do aplicativo Citrix Workspace for suportada, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definida como **1** automaticamente no VDA. O Microsoft Teams lê a chave a ser carregada no modo VDI.

> **Nota:**
>
> Se você estiver usando VDAs da versão 1906.2 ou posterior com versões mais antigas do controlador (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda poderá ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

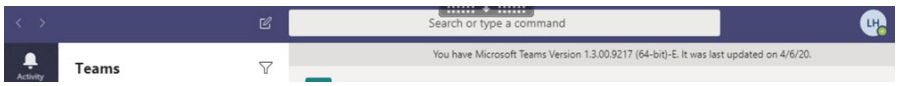
Se você clicar em **About > Version**, a legenda **Citrix HDX Optimized** exibirá:



Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro em partes posteriores da pilha. O erro é mais provável nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, isso indica que o Microsoft Teams não conseguiu carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito no ícone da área de notificação e reinicie. Certifique-se de que a política Gerenciar console não esteja definida como **Prohibited** e que a versão do aplicativo Citrix Workspace seja suportada.



Importante: a sessão se reconecta

- Talvez seja necessário reiniciar o Microsoft Teams para obter uma sessão otimizada para HDX quando sua conectividade mudar. Por exemplo, se você estiver fazendo o roaming de um ponto de extremidade não compatível (aplicativo Workspace para iOS, Android ou versões antigas do Windows/Linux/Mac) para um ponto de extremidade compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou o oposto.
- A reinicialização do Microsoft Teams também é necessária se você tiver instalado o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações de VDI persistentes. Nesses casos, o Microsoft Teams pode atualizar automaticamente enquanto a sessão HDX está no estado desconectado. Portanto, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado em um estado otimizado.
- Ao fazer o roaming de uma sessão local para uma sessão HDX, você precisa reiniciar o Microsoft Teams para otimizar com o HDX. Essa ação é necessária em um cenário de acesso remoto ao PC.

Requisitos de rede

O Microsoft Teams conta com servidores de Processador de Mídia no Microsoft 365 para reuniões ou chamadas multipartes. O Microsoft Teams usa retransmissões de transporte do Microsoft 365 para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Portanto, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Consulte os Princípios de conectividade de rede do Microsoft 365 para obter diretrizes detalhadas sobre o planejamento de rede.

Recomendamos avaliar seu ambiente para identificar os riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem.
Use a Ferramenta de avaliação de rede do Skype for Business para testar se sua rede está pronta para o Microsoft Teams. Para obter informações sobre suporte, consulte Suporte.

Resumo das principais recomendações de rede para o tráfego RTP (Real Time Protocol)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir da filial.
- Planeje e forneça largura de banda suficiente na filial.
- Verifique se há conectividade e qualidade de rede em cada filial.
- Se você precisar usar qualquer um dos itens a seguir na filial, certifique-se de que o tráfego RTP/UDP (manipulado pelo HdxRtcEngine.exe no aplicativo Citrix Workspace) esteja desimpedido.
  - Ignorar servidores proxy
  - Interceptação SSL de rede
  - Dispositivos de inspeção profunda de pacotes
  - VPN hairpin (use tunelamento dividido, se possível)

> **Importante: configuração de túnel dividido de VPN**
>
> O tráfego do HdxRtcEngine.exe deve ser desviado do túnel VPN e ter a permissão de usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira pela qual isso é realizado variará dependendo do produto VPN e da plataforma de máquina usada, mas a maioria das soluções VPN permite a configuração simples da política para aplicar essa lógica. Para obter mais informações com orientações de túnel dividido específicas à plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o SRTP (Secure Real-Time Transport Protocol) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para esse recurso, são usadas chaves simétricas (negociadas com DTLS) para criptografar mídia e controlar mensagens usando a codificação de criptografia AES.

As seguintes métricas são recomendadas para garantir uma experiência positiva do usuário:

Métrica	Ponto de extremidade para Microsoft 365
Latência (um sentido)	< 50 ms
Latência (RTT)	< 100 ms
Perda de pacote	< 1% durante um intervalo de 15s
Jitter entre chegada de pacotes	<30ms durante um intervalo de 15s

Para obter mais informações, consulte Preparar a rede da sua organização para o Microsoft Teams.

Em termos de requisitos de largura de banda, a otimização para o Microsoft Teams pode usar uma grande variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam estes codecs durante o processo do estabelecimento de chamada usando a oferta/resposta do Session Description Protocol (SDP).
As recomendações mínimas da Citrix são:

Tipo	Largura de banda	Codec
Áudio (em cada sentido)	~ 90 kbps	G.722
Áudio (em cada sentido)	~ 60 kbps	Opus*
Vídeo (em cada sentido)	~ 700 kbps	H264 360p a 30 fps 16:9
Compartilhamento de tela	~ 300 kbps	H264 1080p a 15 fps

* O Opus suporta codificação de taxa de bits constante e variável de 6 kbps até 510 kbps.

Opus e H264 são os codecs preferidos para chamadas ponto a ponto e em conferência.

> **Importante:**
>
> Quanto ao desempenho, a codificação é mais cara do que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix Workspace para Linux e Windows. Consulte Encoder performance estimator e Otimização para Microsoft Teams.

Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

  Se você configurar um servidor proxy explícito no VDA e encaminhar conexões para localhost por meio de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Bypass proxy servers for local address** em **Internet Options > Connections > LAN Settings > Proxy Servers** e ignorar `127.0.0.1:9002`.

  Se você usar um arquivo PAC, o script de configuração do proxy VDA do arquivo PAC deverá retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

  Se a filial estiver configurada para acessar a Internet por meio de um proxy, esses aplicativos suportam servidores proxy:

- Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos Pac também têm suporte)
- Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos Pac também têm suporte)
- Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
- Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler configurações de proxy. Esses dispositivos enviam tráfego diretamente para servidores do Microsoft 365 TURN.

> **Importante:**
>
> - Verifique se o dispositivo cliente pode se conectar ao servidor DNS para executar resoluções de DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor Microsoft Teams Relay:
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> Se as solicitações de DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e o estabelecimento de mídia de chamadas em conferência falharão.
>
> - A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não no cliente).

Estabelecimento de chamadas e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão SRTP (Secure Real-Time Transport Protocol) de rede direta via User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia recorre ao TCP/TLS 443.

O mecanismo de mídia HDX dá suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal usando retransmissões em torno de NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Este suporte significa que o ponto de extremidade deve poder executar resoluções DNS.

Considere um cenário em que não há caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está ingressando em uma chamada ou reunião com vários participantes. O

HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP da sub-rede do Microsoft 365 e quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver bloqueado). Para obter mais informações, consulte o diagrama de arquitetura na Configuração de chamada e URLs do Office 365 e intervalos de endereços IP ID 11.

ID	Categoria	Endereços	Portas de destino
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (fallback)

Esses intervalos incluem retransmissões de transporte e processadores de mídia, com front-end por um Azure Load Balancer.
As retransmissões de transporte do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são pontos de extremidade ICE. Além disso, as retransmissões de transporte do Microsoft Teams não terminam a mídia, o TLS, nem realizam nenhuma transcodificação. Elas podem fazer a ponte TCP (se HdxRtcEngine.exe usar TCP) para o UDP quando encaminham o tráfego para outros pares ou processadores de mídia.

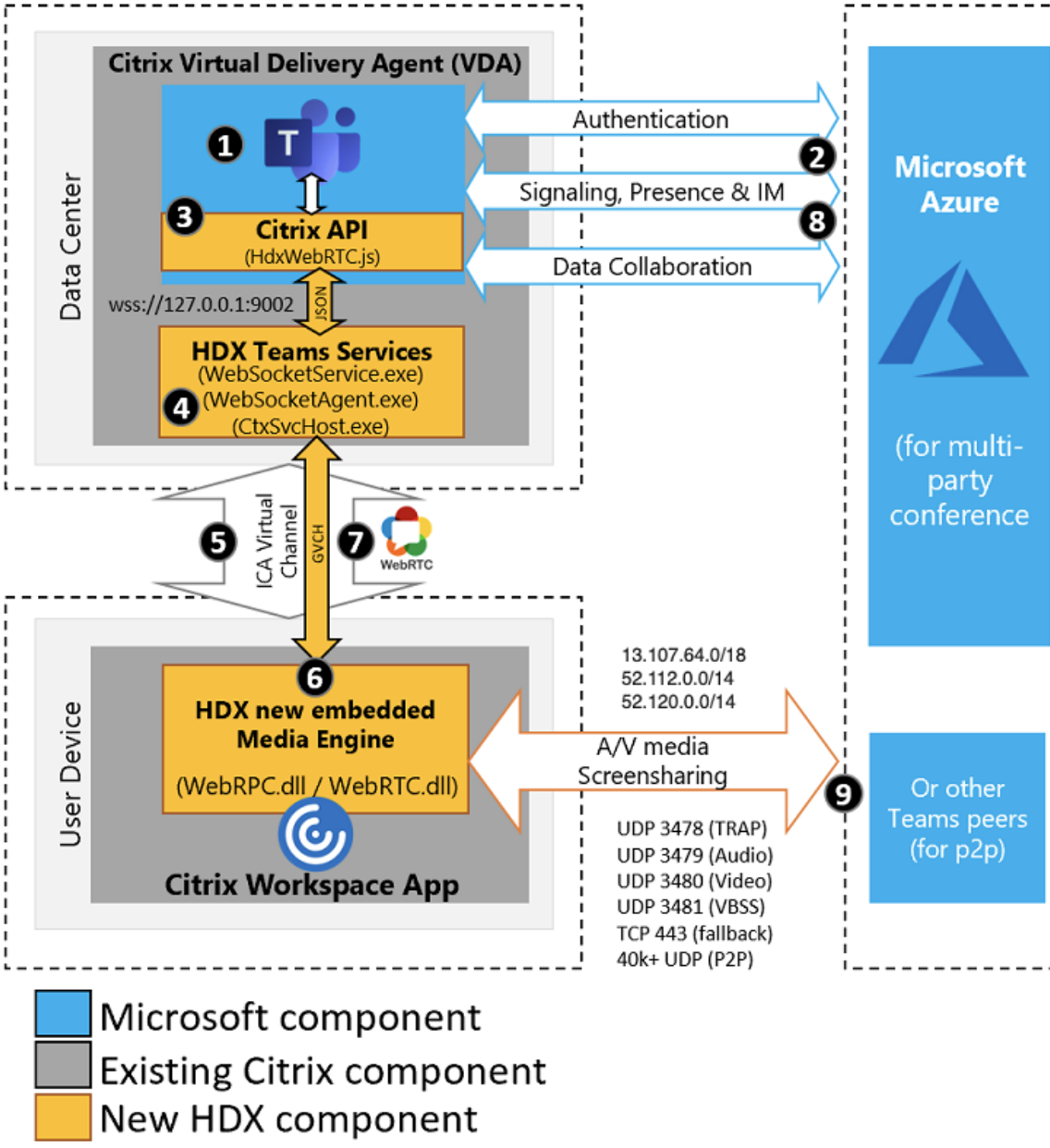
O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com a retransmissão de transporte do Microsoft Teams mais próxima na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e porta 3478—3481 UDP (portas UDP diferentes por carga de trabalho, embora possa haver multiplexação) ou 443 TCP/TLS para fallbacks. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado por TCP, aconselhamos você a projetar suas redes para acomodar o tráfego UDP na filial.

Se o Microsoft Teams for carregado no modo otimizado e o HdxRtcEngine.exe estiver sendo executado no ponto de extremidade, as falhas do ICE podem causar uma falha na configuração da chamada ou áudio/vídeo somente unidirecional. Quando um atendimento não pode ser concluído ou os fluxos de mídia não forem full duplex, verifique primeiramente o **rastreamento Wireshark** no ponto de extremidade. Para obter mais informações sobre o processo de coleta do candidato ICE, consulte "Coletando logs"na seção Suporte.

> **Nota:**
>
> Se os pontos de extremidade não tiverem acesso à Internet, os usuários talvez ainda possam fazer uma chamada ponto a ponto somente se os dois estiverem na mesma LAN. As reuniões não ocorrem. Neste caso, há um intervalo de 30 segundos antes que a configuração de chamada comece.

Configuração de chamada

Use este diagrama de arquitetura como uma referência visual para a sequência de fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.



Arquitetura

1. Inicie o Microsoft Teams.
2. O Microsoft Teams é autenticado no O365. As políticas de locatário são enviadas para o cliente Microsoft Teams e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.

3. O Microsoft Teams detecta que ele está sendo executado em um VDA e faz chamadas de API para a API JavaScript Citrix.
4. O Citrix JavaScript no Microsoft Teams abre uma conexão segura do WebSocket ao WebSocketService.exe em execução no VDA, que gera WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico ligando para o Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe).
6. O wfica32.exe (mecanismo HDX) do aplicativo Citrix Workspace gera um novo processo chamado HdxRtcEngine.exe, que é o novo mecanismo WebRTC usado para a otimização do Microsoft Teams.
7. O mecanismo de mídia Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem iniciar o processamento de solicitações de multimídia.

   ——Chamadas do usuário——

8. O **par A** clica no botão de **chamada**. Teams.exe se comunica com os serviços do Microsoft Teams no Microsoft 365 estabelecendo um caminho de sinalização de ponta a ponta com o **par B**. O Microsoft Teams solicita ao HdxRtcEngine uma série de parâmetros de chamada compatíveis (codecs, resoluções e assim por diante, que é conhecida como oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e daí para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização e quando são concluídas as verificações de conectividade ICE (travessia de NAT e firewall por meio de solicitações de ligação STUN). Então, a mídia Secure Real-Time Transport Protocol (SRTP) flui diretamente entre HdxRtcEngine.exe e o outro par (ou Microsoft 365, se for uma reunião).

Sistema de Telefonia da Microsoft

O Sistema de Telefonia é a tecnologia da Microsoft que permite o controle de chamadas e PBX na nuvem do Microsoft 365 com o Microsoft Teams. A Otimização para Microsoft Teams oferece suporte ao sistema de telefonia com planos de chamadas do Microsoft 365 ou roteamento direto. Com o roteamento direto, você conecta seu próprio controlador de borda de sessão suportado ao sistema de telefonia Microsoft diretamente sem nenhum software local adicional.
Há suporte para filas de chamadas, transferência, encaminhamento, espera, silenciar e retomar uma chamada.

DTMF

O recurso de tons duplos de multifrequência (DTMF) são compatíveis com estas versões do aplicativo Citrix Workspace (ou posterior):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para ChromeOS versão 2111.1

Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado no Microsoft Calling Plans, Operator Connect e Direct Routing, ele permite a você:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace em execução no ponto de extremidade, em vez do cliente Microsoft Teams em execução no VDA.

A lei de Ray Baum exige que o local despachável do chamador de 911 seja transmitido para o Ponto de Atendimento Público Seguro (PSAP) apropriado. O Microsoft Teams Optimization with HDX está em conformidade com a lei de Ray Baum quando usado com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posteriores
- Aplicativo Citrix Workspace para Linux versão 2112 e posteriores
- Aplicativo Citrix Workspace para Mac versão 2112 e posteriores
- Aplicativo Citrix Workspace para ChromeOS versão 2112 e posteriores

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de localização de rede ou emergência:

- Configurações de rede
- Serviço de Informações de Local (LIS)

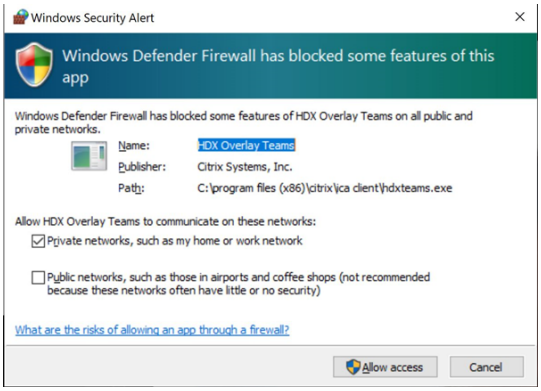
Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de local despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

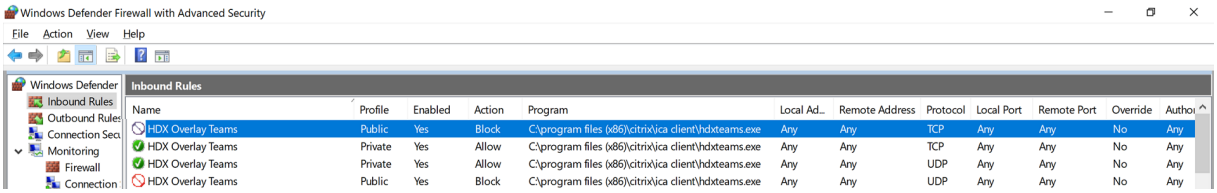
- ID do chassi/ID da porta usando o Link Layer Discovery Protocol (LLDP) para conexões Ethernet/Switch. O Ethernet/Switch (LLDP) é suportado em:
  - Versões 8.1 e 10 do Windows
  - macOS, que requer software de ativação LLDP Para baixar o software de ativação LLDP, acesse `www.microsoft.com` e pesquise o software de ativação LLDP.
  - Linux, que exige que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do cliente fino.
- WLAN BBSID e {IPv4-IPv6; Sub-rede; Endereço MAC} do ponto de extremidade em que o aplicativo Citrix Workspace está instalado.
  - Locais baseados em sub-rede e WiFi são compatíveis com o aplicativo Workspace para Windows, Linux e Mac.
- Latitude e Longitude, se a permissão do usuário for concedida no nível do sistema operacional em que o aplicativo Citrix Workspace está instalado (a permissão é definida como HDX RTC Engine)
  - Compatível com todas as plataformas de aplicativos do Workspace. No entanto, no caso do Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do SO do cliente fino (>sudo apt-get install libgps-dev gpsd lldpd).

Considerações sobre o firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso com as configurações de **firewall do Windows**. O aviso pede aos usuários para permitir a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Firewall do Windows Defender > Segurança Avançada**. Você pode aplicar regras mais restritivas, se desejar.

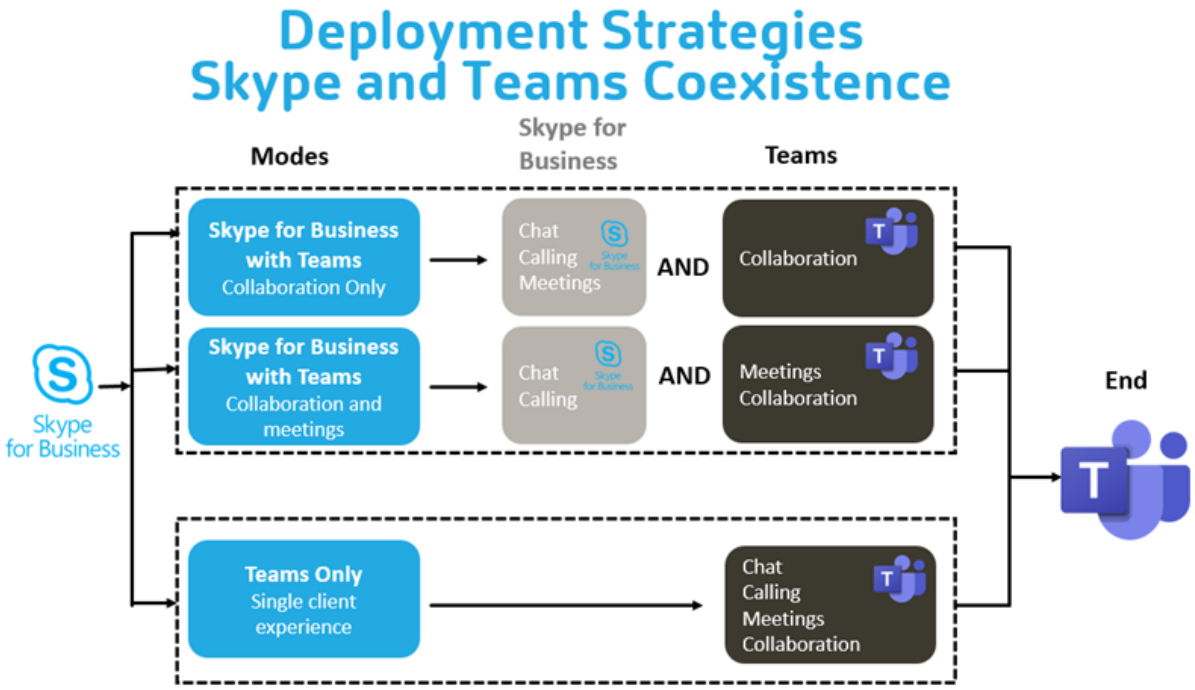


Coexistência do Microsoft Teams e Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado, como duas soluções separadas com recursos sobrepostos.
Para obter mais informações, consulte Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para os mecanismos multimídia do Microsoft Teams, em seguida, honram o conjunto de configurações Alguns exemplos são modos de ilha e colaboração do Skype for Business com o Microsoft Teams. Além disso, colaboração e reuniões do Skype for Business com Microsoft Teams.

O acesso periférico só pode ser concedido a um único aplicativo no momento. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



Citrix SD-WAN: conectividade de rede otimizada para Microsoft Teams

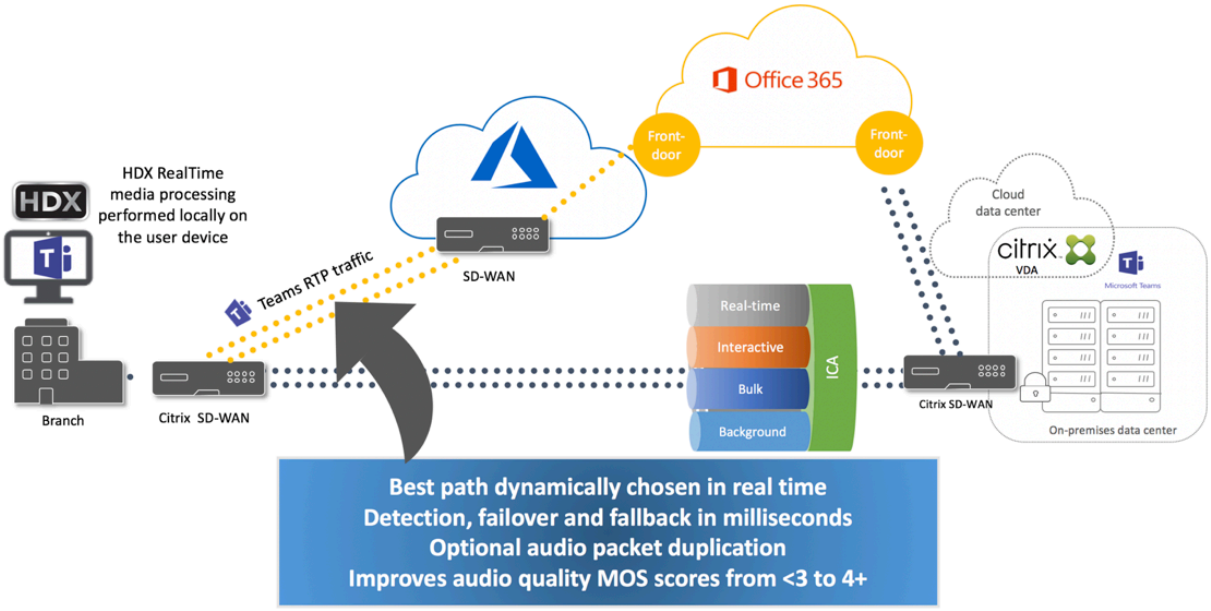
A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio-vídeo do Microsoft Teams dos usuários do aplicativo Citrix Workspace em locais de filiais para um data center antes de ir à Internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço Web do Microsoft 365 baseados em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

As conexões de internet de banda larga de negócios em muitas áreas sofrem de perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio-vídeo do Microsoft Teams quando a integridade da rede é variável ou está degradada.

- Se você usar o Microsoft Azure, um Appliance Virtual (VPX) Citrix SD-WAN implantado no Azure VNET fornece otimizações avançadas de conectividade. Essas otimizações incluem failover de link integrado e corridas de pacotes de áudio.
- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud Direct. Este serviço fornece entrega confiável e segura para todo o tráfego direcionado à Internet.

Se a qualidade da conexão com a Internet da filial não for uma preocupação, pode ser suficiente para minimizar a latência. Desvie o tráfego do Microsoft Teams diretamente do dispositivo de filial Citrix SD-WAN para a porta da frente do Microsoft 365 mais próxima para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo com várias janelas

Você pode usar várias janelas de reuniões ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings no site do Microsoft 365.

> **Nota:**
>
> Esse recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303 e VDA 2112.

Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 suporta desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas ajudando a conversa a manter o foco na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas em conferência ou P2P.

> **Nota:**
>
> Esse recurso está integrado à interface do usuário/botões do Microsoft Teams. O suporte a MultiWindow é um pré-requisito que requer uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte Reuniões e bate-papo com várias janelas.

Os controles de interface do usuário do Microsoft Teams de desfoque e efeitos de fundo exigem as seguintes versões mínimas:

- Aplicativo Citrix Workspace para Windows 2207
- Aplicativo Citrix Workspace para Mac 2301
- Aplicativo Citrix Workspace para Linux 2212
- Aplicativo Citrix Workspace para ChromeOS 2303

Limitações:

- O cliente deve estar conectado à Internet durante a substituição da imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição da imagem de fundo definida pelo administrador e pelo usuário não é compatível com a interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser definidas usando parâmetros de configuração no cliente, se a imagem também estiver armazenada no cliente.

Configurar uma imagem de fundo personalizada

As chaves de registro a seguir só são necessárias se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso ou se um administrador quiser substituir os comportamentos padrão. Por exemplo, desativar o desfoque da tela de fundo porque o ponto de extremidade não é poderoso o suficiente.

No Windows Para definir uma imagem de fundo personalizada, os administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou ponto de extremidade:

Localização: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição da imagem de fundo)

O valor definido como 1 desfoca o fundo. Esse valor pode ser definido pelo usuário final ou pelo administrador.

O valor definido como 2 também requer que a chave **VideoBackgroundImage** esteja presente também. Somente o administrador pode definir esse valor. A seguinte chave é necessária somente se você quiser substituir a imagem de fundo, não para desfocar:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: my_image_name.jpeg

A imagem de fundo do vídeo deve estar presente no diretório `C:\Program Files (x86)\Citrix\ICA Client`.

Essa configuração do registro também pode ser usada para habilitar o desfoque em segundo plano ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de interface do usuário do Microsoft Teams. Em outras palavras, se o seu ambiente ou VDA não suportar várias janelas, você ainda poderá aplicar a solução alternativa do registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações da chave do Registro só entram em vigor quando a sessão HDX se conecta.

No Mac Localização da imagem baixada pelo usuário: */Users/username/Downloads/any_image.png*

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

No Linux Localização da imagem baixada pelo usuário: */home/username/Downloads/any_image.jpg*

Crie o arquivo */var/.config/citrix/hdx_rtc_engine/config.json* e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }
```

Em HTML5

1. Navegue até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }
```



```
 8
 9   }
10
11  <!--NeedCopy-->
```

3. Salve as alterações.

Considerações sobre o consumo de CPU cliente

Embora o recurso de desfoque seja econômico em termos de uso de CPU, você pode esperar um aumento no consumo. Por exemplo, em um cliente fino com um chip Intel® Pentium® Silver de 4 núcleos e 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

Exibição de galeria e alto-falantes ativos no Microsoft Teams

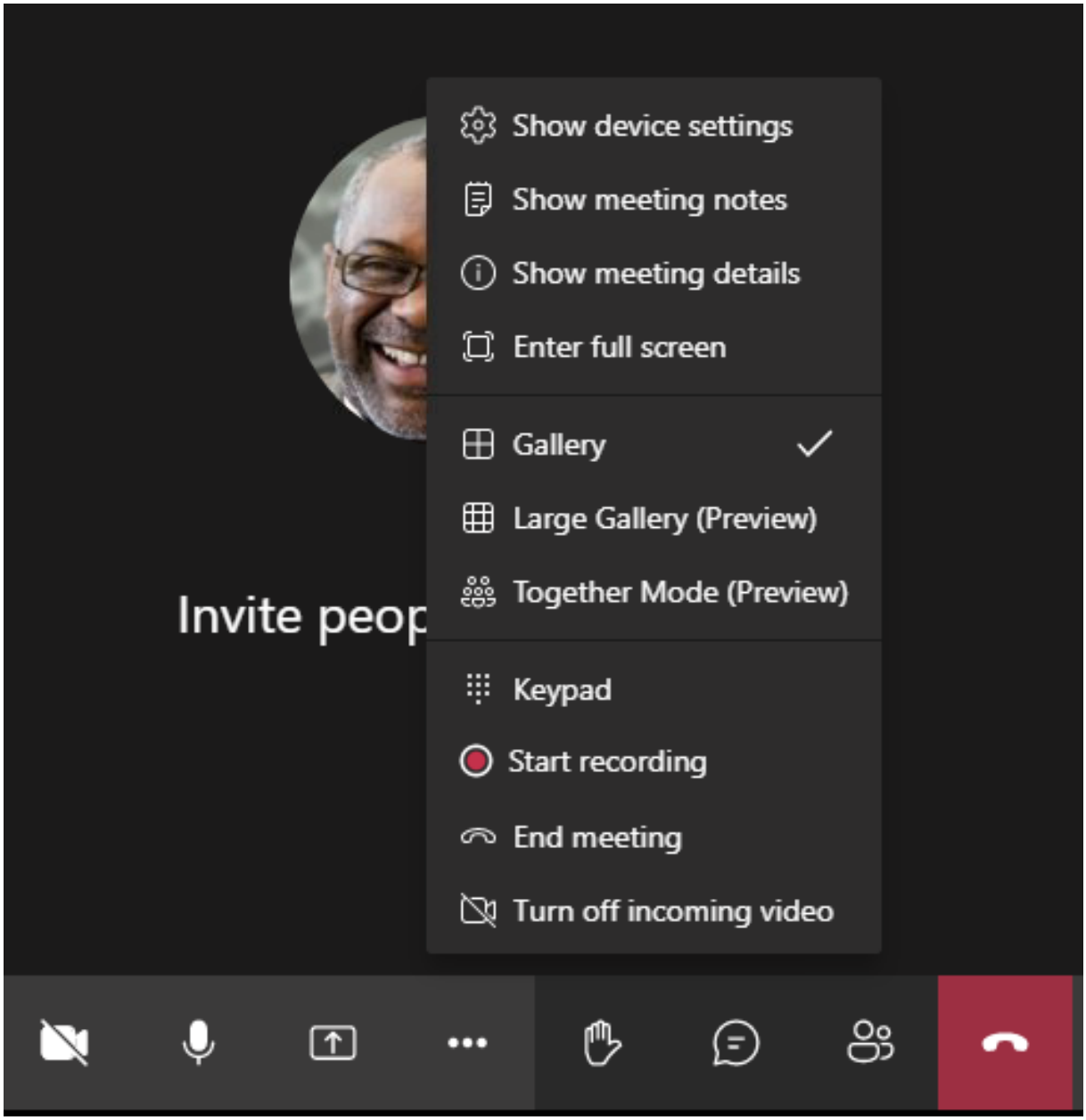
O Microsoft Teams oferece suporte a layouts de **Gallery**, **Large gallery** e **Together mode**.

O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecidos como **Gallery**). Nesse caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham vídeo, apenas os últimos quatro alto-falantes mais ativos aparecem na tela.

O Microsoft Teams também fornece a grande visualização da galeria com uma grade de até 7x7. Como resultado, o servidor de conferência Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Esse feed único, em estilo de matriz, também pode incluir o vídeo de pré-visualização automática dos usuários.

Por fim, o Microsoft Teams suporta o **Together mode**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para colocar digitalmente os participantes em um histórico compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada em conferência selecionando layouts de **Gallery**, **Large gallery** ou **Together mode** no menu de reticências.



Suporte para restrições de proporção de vídeo (CWA para Windows 2102, CWA para Linux 2106, CWA para MAC 2106 ou posterior):

- A opção **Preencher a moldura** está disponível em Gallery/Large Gallery View. Essa opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts Gallery e Large Gallery:

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Layout/Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro últimos palestrantes mais ativos aparecem na tela e os outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.
Técnica mista	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central combina e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Esta ação introduz um pouco de latência adicional.
Alto-falante ativo	O novo alto-falante ativo substitui o alto-falante menos ativo na grade.	Exibe todos os participantes, independentemente de estarem ativos ou inativos.
Codificação no ponto de extremidade	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no ponto de extremidade	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no ponto de extremidade pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo de áudio e vídeo. Isso reduz o consumo de CPU no ponto de extremidade.

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo poderá ser maior.	720p para o layout composto ou misto. Não há necessidade de um stream de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente reduz a resolução ou a taxa de bits de upload.
Problema de "usuário lento"	O remetente modifica a qualidade de cada modalidade (áudio/vídeo/compartilhamento de tela) para a menor qualidade de rede comum entre os participantes. Esse fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com más condições de rede afeta a qualidade de todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência fornece qualidades diferentes com base nas condições de rede de participantes individuais.
Autovisualização	Mostra você em uma pequena miniatura em tempo real.	Mostra você em uma miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout do vídeo principal com algum atraso adicional.

Compartilhamento de tela no Microsoft Teams

O Microsoft Teams conta com o compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho que está sendo compartilhada com codecs de vídeo como o H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do aplicativo Citrix Workspace 2109 ou superior, para Windows, Linux e Mac, e do aplicativo Citrix Workspace 2303, para ChromeOS, os usuários podem compartilhar suas telas e câmeras de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera é pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O par deve então retomar manualmente o compartilhamento da câmera.

> **Nota sobre o PowerPoint Live**
>
> Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros colegas ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para ver outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar uma apresentação de slides do PowerPoint Live, clique no botão da "Bandeja de compartilhamento"e selecione um dos slides sugeridos do PowerPoint, ou clique em "Procurar"e localize um arquivo do PowerPoint no seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Aplicativos locais sobrepostos ao Desktop Viewer não são capturados.

> **Nota**
>
> Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

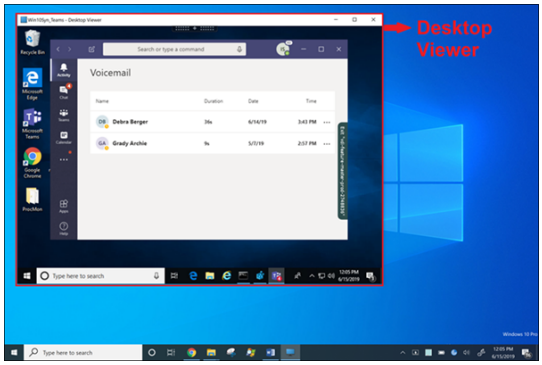
Multimonitor

Se o Desktop Viewer (CDViewer.exe) estiver no modo de tela cheia e abrangendo configurações de vários monitores, o aplicativo Citrix Workspace 2106 ou posterior (Windows/Linux/Mac) permite que o seletor de tela selecione o monitor que deve ser compartilhado.

Limitação conhecida:

- Se o Desktop Viewer estiver desativado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desativado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela com vários monitores.
- Nas versões do aplicativo Workspace anteriores à 2106, somente o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor primário para que o outro par na chamada possa vê-lo.

- O compartilhamento de tela com vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout do monitor virtual (partição lógica de um único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.
- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento só é possível se o aplicativo local tiver sido sobreposto no Desktop Viewer. Esse comportamento foi removido na versão 2009.6 ou posterior, e 1912 CU5 ou posterior.
- Durante o compartilhamento de tela, se você mudar do modo de janela para tela cheia, o compartilhamento de tela é interrompido. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.



Compartilhamento de tela a partir de um aplicativo integrado:

Se você estiver publicando o Microsoft Teams como um aplicativo integrado independente, o compartilhamento de tela capturará a área de trabalho local do seu ponto de extremidade físico. É necessário o aplicativo Citrix Workspace versão mínima 1909.

Compartilhamento de aplicativos

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

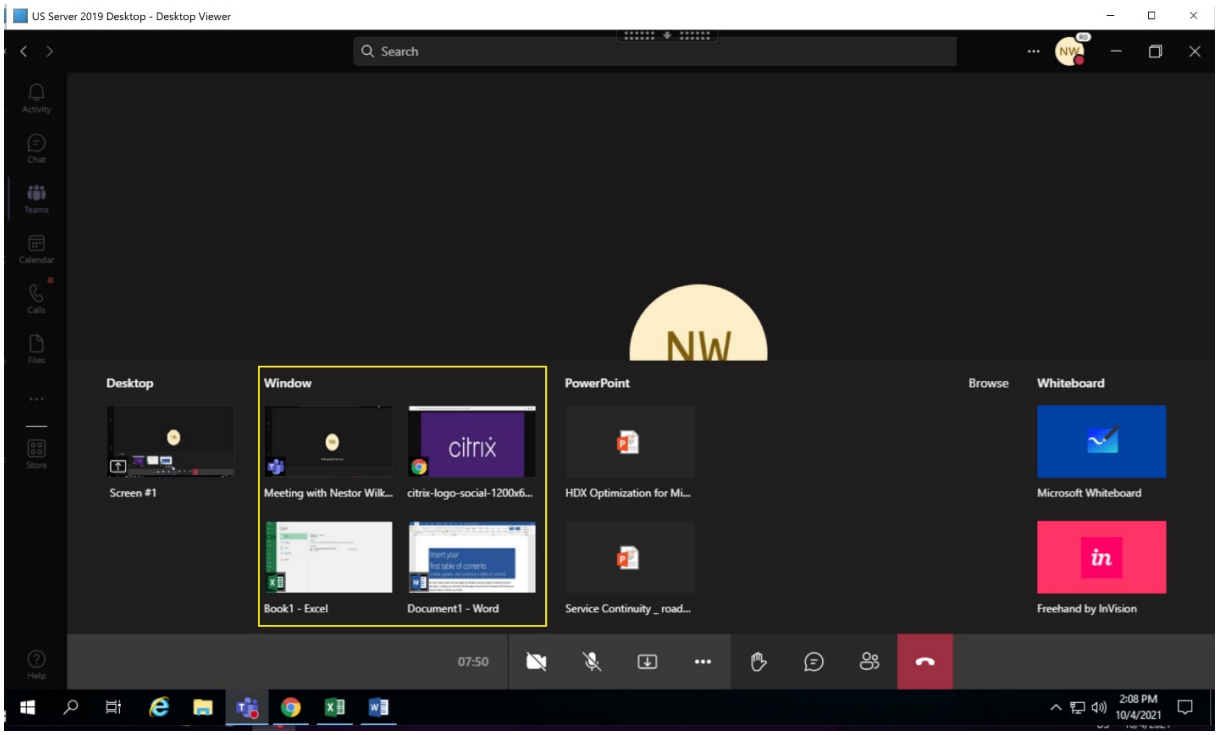
Começando com o aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Para compartilhar um aplicativo específico:

1. Navegue até o aplicativo Microsoft Teams em sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo que você selecionou e os colegas na chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desativar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`:
Nome: `UseWsProvider`
Tipo: `DWORD`
Valor: 0

> **Nota:**
>
> - Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
> - O compartilhamento de tela depende da captura do lado do VDA da janela. O conteúdo é retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para os colegas ou servidor de conferência.



Limitações conhecidas com o compartilhamento de tela de um aplicativo específico:

- O ponteiro do mouse não fica visível quando você está compartilhando a tela de um aplicativo.
- Se você minimizar um aplicativo ao compartilhá-lo, somente o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até você maximizar o aplicativo.
- Os aplicativos LAA (acesso a aplicativos locais) mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de desktop no Microsoft Teams otimizado no VDA. No entanto, quando você seleciona o aplicativo na lista, o resultado pode não ser o esperado.

Compatibilidade com a proteção de aplicativos
O compartilhamento de tela de um aplicativo específico é compatível com o recurso de proteção de aplicativos no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico, se tiver iniciado o aplicativo ou a área de trabalho a partir de um grupo de entrega que tenha a proteção de aplicativo ativada.

Quando você clica em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Área de trabalho**. Você só pode selecionar a opção **Janela** para compartilhar um aplicativo aberto.

> **Nota:**
>
> Quando você inicia aplicativos ou áreas de trabalho de um grupo de entrega com a proteção de aplicativos ativada, não é possível ver o vídeo recebido ou o compartilhamento de tela se estiver usando o aplicativo Citrix Workspace para Windows 2202 ou anterior.

Conceder e solicitar controle no Microsoft Teams Este recurso é suportado nas seguintes versões do aplicativo Citrix Workspace (não há dependência da versão do VDA ou do sistema operacional, sessão única ou multissessão):

- Aplicativo Citrix Workspace para Windows versão 2112.1 ou posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 ou posterior
- Aplicativo Citrix Workspace para Linux versão 2203 ou posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2303 ou posteriores

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de obter o controle, você pode fazer seleções, edições ou outras atividades usando o teclado e mouse na tela compartilhada.

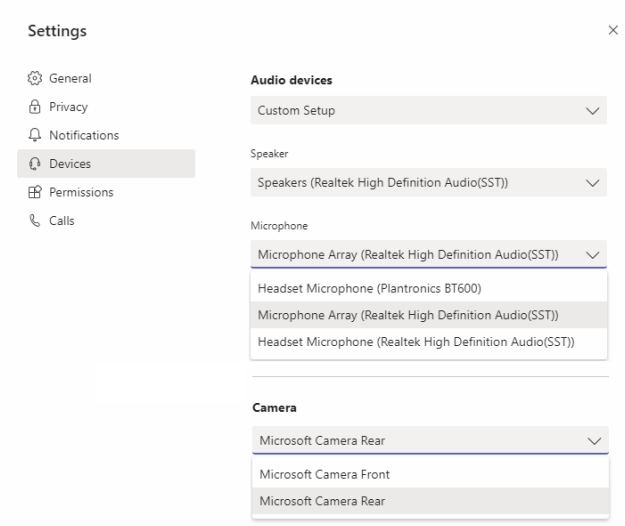
Para assumir o controle quando uma tela está sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar a sua solicitação.

Enquanto você tem controle, você pode fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar o teclado e o mouse. Quando terminar, clique em **Solicitar controle**.

> **Limitações:**
>
> - Conceder e solicitar controle não estarão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como compartilhamento de aplicativo). A área de trabalho ou o monitor completo devem ser compartilhados.
> - O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização do Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fone de ouvidos, microfones, câmeras, alto-falantes e assim por diante). Em seguida, os periféricos são listados devidamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele usa o mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão a partir do mesmo ponto de extremidade.

Recomendações:

- Headsets certificados pelo Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde microfone e alto-falantes estão em dispositivos separados, pode haver um eco. Um exemplo disso é uma webcam com um microfone embutido e um monitor com alto-falantes. Ao usar alto-falantes externos, coloque-os o mais longe possível do microfone. Além disso, coloque-os longe de qualquer superfície que possa refratar o som para o microfone. Para obter mais informações, acesse www.microsoft.com e pesquise fones de ouvido certificados pelo Microsoft Teams.
- Câmeras certificadas pelo Microsoft Teams, embora os periféricos certificados pelo Skype for Business sejam compatíveis com o Microsoft Teams. Para obter mais informações, acesse www.microsoft.com e pesquise câmeras certificadas pelo Microsoft Teams e periféricos certifi-

cados pelo Skype for Business.
- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento de CPU com webcams que executam codificação H.264 integrada - UVC 1.1 e 1.5.

> **Nota:**
>
> O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio com 24 bits ou com frequências acima de 96 kHz.
>
> O HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou mais antigo) suporta apenas esses formatos de dispositivo de áudio específicos (canais, profundidade de bits e taxa de amostragem):
>
> - Dispositivos de reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
> - Dispositivos de gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz
>
> Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.
>
> **Webrpc** apresenta logs em **HdxTeams.exe** que mostram este tipo de informação:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> Como solução alternativa, desative o dispositivo específico ou:
>
> 1. Abra o **Painel de controle de som** (mmsys.cpl).
> 2. Selecione o dispositivo de reprodução ou gravação.
> 3. Vá para **Propriedades > Avançado** e altere as configurações para um modo suportado.

Modo de fallback

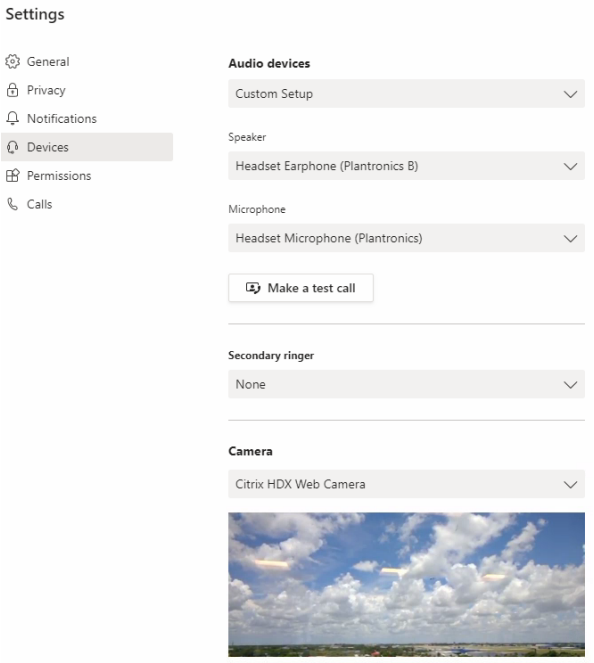
Se o Microsoft Teams não carregar no modo VDI otimizado (“Citrix HDX não conectado”em Teams/About/Version), o VDA retornará às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento da webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando um sistema operacional de versão/plataforma do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não serão aplicadas. No modo de reserva, os periféricos são traçados ao VDA. Os periféricos aparecem no aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro

no VDA. Para obter informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados pelo registro.

Esse recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior.

Para determinar se você está no modo otimizado ou não otimizado ao observar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX herdadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX** como mostrado no gráfico a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) quando comparados com o modo otimizado.



Quando são usadas as tecnologias HDX herdadas, o Microsoft Teams não descarrega o processamento de compartilhamento de áudio, vídeo e tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do ponto de extremidade. Em vez disso, as tecnologias HDX usam renderização no lado do servidor. Espere alto consumo de CPU no VDA quando você liga o vídeo. O desempenho de áudio em tempo real pode não ser otimizado.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e terminar chamada não têm suporte. Aumentar e diminuir volume têm suporte.

- As configurações de QoS no Admin Center for Microsoft Teams não se aplicam a usuários de VDI.
- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.

Limitação no VDA:

- Quando você define a configuração de DPI alto do aplicativo Citrix Workspace como **Sim**, a janela de vídeo redirecionado aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume no computador cliente, não no VDA.

Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams em Windows e Mac. Para Linux, consulte seu fornecedor de cliente fino.
Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes terminais são aprimoradas com a adaptação à resolução adequada para a melhor experiência de chamada para todos os chamadores.

Com essa experiência aprimorada, cada usuário pode enviar vários fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p e assim por diante), dependendo de vários fatores, incluindo capacidade do ponto de extremidade, condições da rede e outros. Depois, o ponto de extremidade receptor solicita a resolução de qualidade máxima que pode suportar, proporcionando a todos os usuários a melhor experiência de vídeo.

> **Nota:**
>
> Esse recurso está disponível somente após o lançamento da atualização do Microsoft Teams. Para obter informações sobre o ETA, acesse https://www.microsoft.com/ e pesquise o roadmap do Microsoft 365. Quando a atualização for lançada pela Microsoft, você poderá verificar o CTX253754 para obter a atualização da documentação e o anúncio.

Limitação da Microsoft

- Uma visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams —entre em contato com a Microsoft para saber para quando esperar a grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.

- A resolução máxima de fluxo de vídeo de entrada e saída é de 720p.
- O toque de retorno de chamada PSTN não é suportado
- O desvio de mídia para roteamento direto não tem suporte.
- As funções de produtor e apresentador de eventos de transmissão e ao vivo não têm suporte. A função de participante tem suporte, mas não é otimizada (renderiza no VDA).
- A função de aumentar zoom e diminuir zoom no Microsoft Teams não é suportada.
- Não há suporte para roteamento baseado na localização e bypass de mídia.
- A integridade da chamada não está disponível.
- As salas simultâneas são suportadas para participantes por VDI. O Microsoft Teams não dá suporte a salas simultâneas se o organizador for um usuário de VDI.
- A mesclagem de chamadas não é suportada (opção não exibida na interface do usuário).

Limitação da Citrix e Microsoft

- Ao fazer o compartilhamento de tela, a opção **include system audio** não está disponível.
- A **Campainha secundária** (**Teams** > **Settings** > **Devices**) não tem suporte.
- O Simulcast não é compatível com o ChromeOS.

Informações adicionais

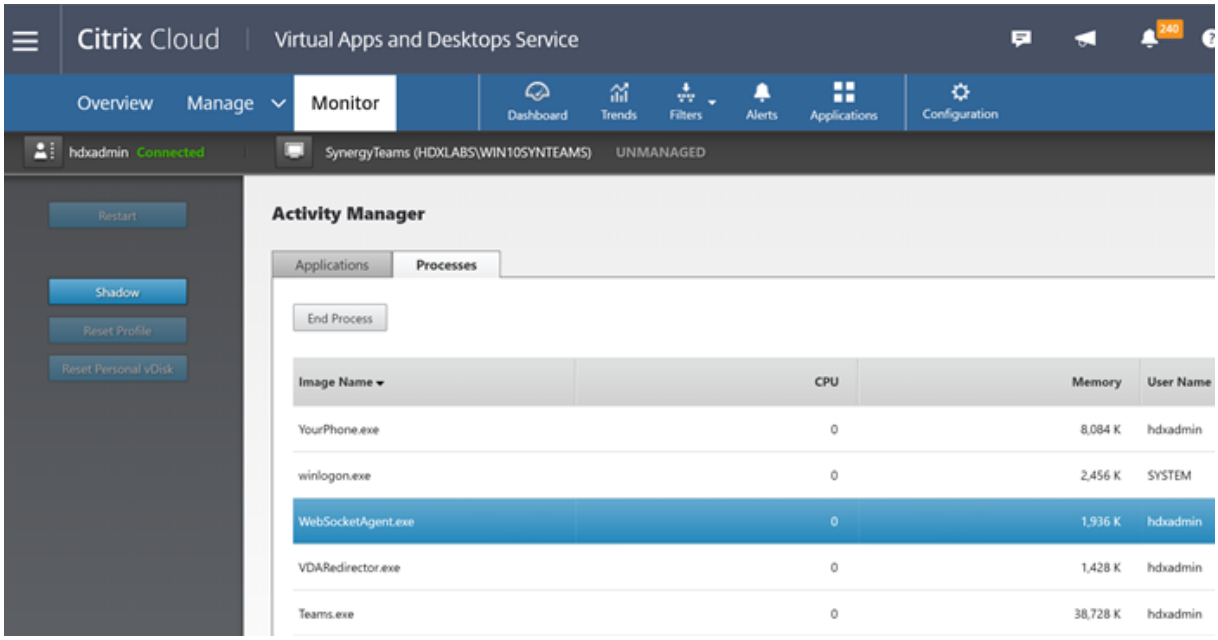
- Monitoramento, resolução de problemas e suporte ao Microsoft Teams
- Implantar o Microsoft Teams da área de trabalho na VM
- Instalar o Microsoft Teams usando o MSI (seção Instalação da VDI)
- Clientes finos
- ferramenta de avaliação de rede do Skype for Business
- Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.

Monitoramento, resolução de problemas e suporte ao Microsoft Teams

June 28, 2023

Monitorar o Teams

Esta seção fornece informações básicas para monitorar a otimização do Microsoft Teams com HDX. Se você estiver no modo otimizado e `HdxRtcEngine.exe` estiver sendo executado na máquina cliente, um processo do VDA chamado `WebSocketAgent.exe` está em execução na sessão. Use o **Activity Manager** no Director para ver o aplicativo.



Com o VDA versão mínima 1912, você pode monitorar chamadas ativas do Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o mais recente `hdxmonitor.msi` na pasta `layout\image-full\Support\HDX Monitor`.

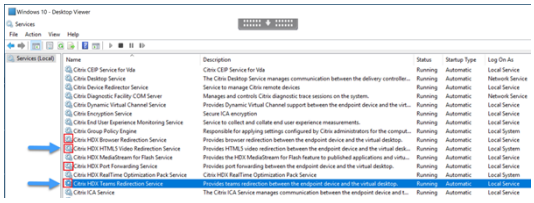
Para obter mais informações, consulte *Monitoring* no artigo do Knowledge Center CTX253754.

Solução de problemas

Esta seção fornece dicas de solução de problemas para problemas que você pode encontrar ao usar a otimização para o Microsoft Teams. Para obter mais informações, consulte CTX253754.

No Virtual Delivery Agent

Existem quatro serviços instalados pelo BCR_x64.msi. Apenas dois são responsáveis pelo redirecionamento do Microsoft Teams no VDA.

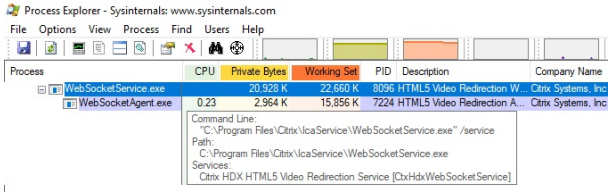


- O **Citrix HDX Teams Redirection Service** estabelece o canal virtual usado no Microsoft Teams. O serviço utiliza o CtxSvcHost.exe.
- O **Citrix HDX HTML5 Video Redirection Service** é executado como WebSocketService.exe escutando em 127.0.0.1:9002 TCP. WebSocketService.exe executa duas funções principais:

i. A **terminação do TLS para WebSockets seguros** recebe uma conexão segura do WebSocket do vdiCitrixPeerConnection.js, que é um componente dentro do aplicativo Microsoft Teams. Você pode rastreá-lo com o Monitor de processos. Para obter mais informações sobre certificados, consulte a seção "Redirecionamento de vídeo TLS e HTML5 e redirecionamento de conteúdo do navegador"em Comunicação entre o controlador e o VDA.

Alguns antivírus e software de segurança de desktop interfere com o bom funcionamento `WebSocketService.exe` e seus certificados. Embora o serviço Citrix HDX HTML5 Video Redirection possa estar em execução no console `services.msc`, o soquete TCP do localhost `127.0.0.1:9002` nunca está no modo de escuta, como visto no netstat. Tentar reiniciar o serviço faz com que ele trave ("Parando..."). Tenha o cuidado de aplicar as exclusões adequadas para o processo `WebSocketService.exe`.

ii. **Mapeamento de sessão do usuário.** Quando o aplicativo Microsoft Teams é iniciado, o WebSocketService.exe inicia o processo WebSocketAgent.exe na sessão do usuário no VDA. O WebSocketService.exe é executado na Sessão 0 como uma conta LocalSystem.



Você pode usar o `netstat` para verificar se o serviço WebSocketService.exe está em um estado de escuta ativa no VDA.

Execute o `netstat -anob -p tcp` a partir de uma janela de prompt de comando elevada:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

Em uma conexão bem-sucedida, o estado muda para ESTABELECIDA:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Importante:**
>
> o WebSocketService.exe escuta em dois soquetes TCP, 127.0.0.1:9001 e 127.0.0.1:9002. A porta 9001 é usada para redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5. A porta 9002 é usada para o redirecionamento do Microsoft Teams. Verifique se você

> não tem nenhuma configuração de proxy no sistema operacional Windows do VDA que possa impedir uma comunicação direta entre Teams.exe e WebSocketService.exe. Às vezes, quando você configura um proxy explícito no Internet Explorer 11 (**Opções da Internet > Conexões > Configurações de LAN > Servidor Proxy**), as conexões podem fluir através de um servidor proxy atribuído. Verifique se a opção **Não usar servidor proxy para endereços locais** está assinalada ao usar uma configuração manual e explícita de proxy.

Locais e descrições dos serviços

Serviço	Caminho para executável no sistema operacional Windows Server	Logon como	Descrição
Serviço de redirecionamento de vídeo Citrix HTML5	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	Conta do sistema local	Fornece vários serviços HDX Multimedia com a estrutura inicial necessária para executar o redirecionamento de mídia entre a área de trabalho virtual e o dispositivo de ponto de extremidade.
Serviço de redirecionamento de navegador Citrix HDX	"C:\Arquivos de programa (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	Esta conta (serviço local)	Fornece conteúdo de redirecionamento do navegador entre o dispositivo de ponto de extremidade e a área de trabalho virtual.

Serviço	Caminho para executável no sistema operacional Windows Server	Logon como	Descrição
Serviço de encaminhamento de portas Citrix	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	Esta conta (serviço local)	Fornece encaminhamento de porta entre o dispositivo de ponto de extremidade e a área de trabalho virtual para redirecionamento de conteúdo do navegador.
Serviço de redirecionamento do Citrix HDX Teams	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Conta do sistema local	Fornece o redirecionamento do Microsoft Teams entre o dispositivo de ponto de extremidade e a área de trabalho virtual.

Aplicativo Citrix Workspace

No ponto de extremidade 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 chamar ou acessar periféricos em autovisualização. Se você não vir este serviço, verifique o seguinte:

1. Certifique-se de que você instalou no mínimo o aplicativo Workspace versão 1905 para Windows. Você está vendo HdxTeams.exe ou HdxRtcEngine.exe e os binários webrpc.dll no caminho de instalação do aplicativo Workspace?
2. Se você validou o passo 1, faça o seguinte para verificar se HdxTeams.exe ou HdxRtcEngine.exe está sendo iniciado.

    a) Saia do Microsoft Teams no VDA.
    b) Inicie o 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 Citrix HDX HTML5.
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 ponto de extremidade do cliente.

Suporte

A Citrix e a Microsoft oferecem suporte ao fornecimento de Microsoft Teams do Citrix Virtual Apps and Desktops por meio de otimização para o Microsoft Teams. Este apoio conjunto é o resultado de uma estreita colaboração entre as duas empresas. Se você tiver contratos de suporte válidos e tiver um problema com essa solução, abra um ticket de suporte com o fornecedor cujo código você suspeita estar causando o problema. Ou seja, Microsoft for Teams ou Citrix para os componentes de otimização.
A Citrix ou a Microsoft recebem o ticket, faz a triagem do problema e escalona conforme apropriado. Não há necessidade de você entrar em contato com a equipe de suporte de cada empresa.

Quando você tiver um problema, recomendamos que você clique em **Help > Report a Problem** na interface do usuário do Teams. Os logs do lado do VDA são compartilhados automaticamente entre a Citrix e a Microsoft para resolver problemas técnicos mais rapidamente.

Coleta de logs

Os logs do mecanismo de mídia HDX podem ser encontrados no computador do usuário (não no VDA). Em caso de problemas, certifique-se de anexar logs ao seu caso de suporte.

Logs do Windows:

Você pode localizar logs do Windows em%TEMP% dentro da pasta **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Procure um arquivo.txt chamado webrpc_Day_Month_timestamp_Year.txt. Se você estiver usando versões mais recentes do aplicativo Citrix Workspace, por exemplo, Citrix Workspace app 2009.5 ou posterior, armazene os logs em AppData\Local\Temp\HdxRtcEngine.

Cada sessão cria uma pasta separada para logs.

Logs no Mac:

1. VDWEBRTC log - registra a execução do canal virtual.

   Localização: /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine log - registra a execução dos processos no HdxRtcEngine.

   Localização: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   O log HdxRtcEngine é ativado por padrão.

3. Logs do Webrpc –são os logs mais importantes que registram a execução na conclusão da biblioteca webrtc.

   Localização: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

Logs do Linux:

Você pode localizar logs do Linux nas pastas /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Log do 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 exigidas:

- Recolha de candidatos
- Troca de candidatos
- Verificações de conectividade (solicitações de associação STUN)
- Promoção do candidato

Nos logs HdxRtcEngine.exe, as entradas a seguir são as entradas relevantes do ICE (Interactive Connectivity Establishment). Essas entradas devem estar presentes para que a configuração de uma chamada seja bem-sucedida. Veja o seguinte trecho de amostra para o estágio 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
```



```
13
14 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
       Gathering
15
16 [...]
17 >>> begin:sdp
18 candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
       generation 0 ufrag oVk6 network-id 1
19 <<< end:sdp
20 [...]
21 >>> begin:sdp
22 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
23 <<< end:sdp
24 [...]
25 >>> begin:sdp
26 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
27 <<< end:sdp
28 [...]
29
30 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
       Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
31 >>> begin:sdp
32 [...]
33
34 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
       HaveRemotelOffer
35
36 <!--NeedCopy-->
```

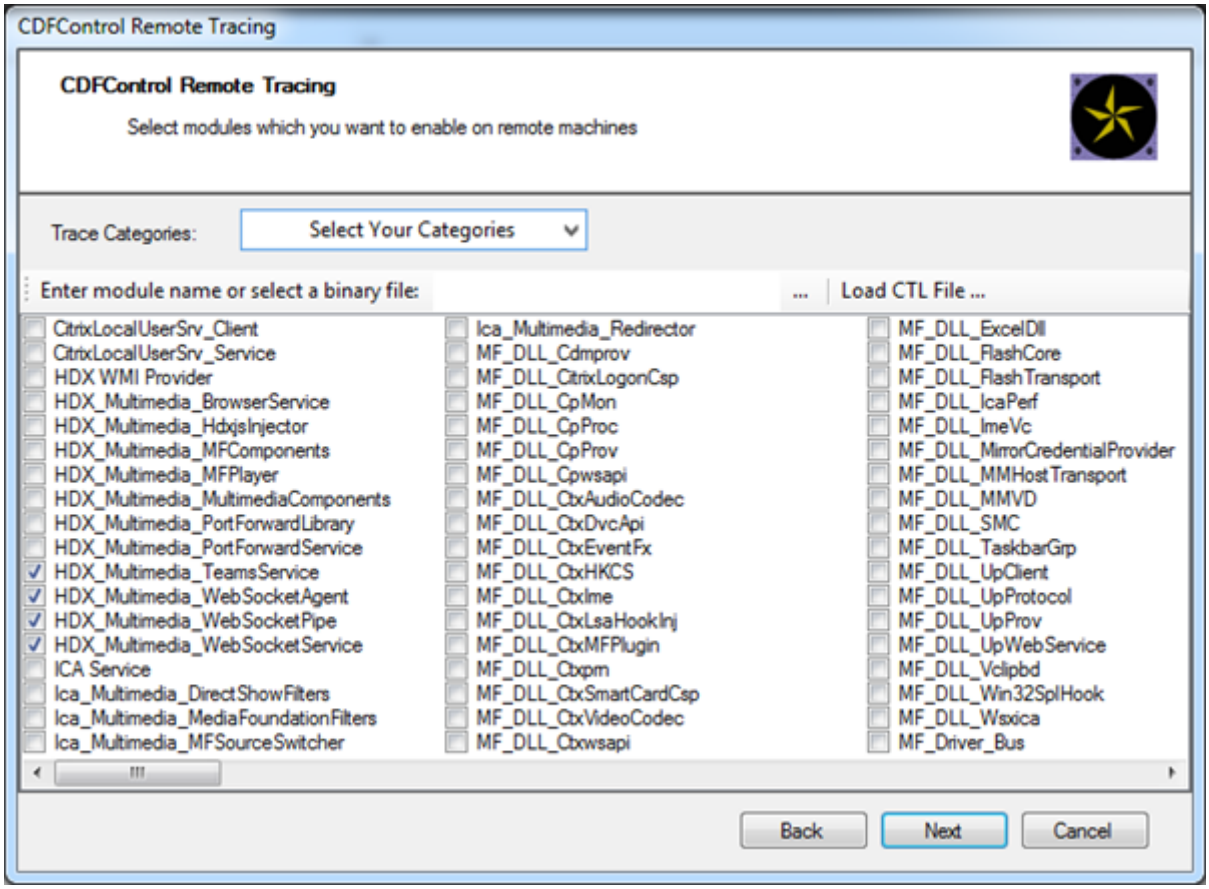
Se houver vários candidatos ICE, a ordem de preferência é:

1. host
2. peer reflexivo
3. servidor reflexivo
4. retransmissão de transporte

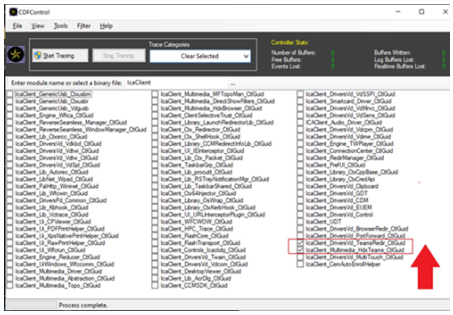
Se você encontrar um problema e puder reproduzi-lo de forma constante, recomendamos clicar em **Help > Report a problem** no Teams. Os logs são compartilhados entre a Citrix e a Microsoft para resolver problemas técnicos se você tiver aberto um caso com a Microsoft.
Capturar rastreamentos de CDF antes de entrar em contato com o Suporte Citrix também é útil. Para obter mais informações, consulte o artigo do Knowledge Center CDFcontrol.

Para obter recomendações sobre coleta de rastreamentos de CDF, consulte o artigo do Centro de conhecimento Recommendations for Collecting the CDF Traces.

Rastreamentos de CDF do lado VDA - Ative os seguintes provedores de rastreamento de CDF:



Rastreamentos de CDF do lado do aplicativo Workspace - Ative os seguintes provedores de rastreamento de CDF:



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requer o aplicativo Citrix Workspace 2012 ou posterior)

Redirecionamento do Windows Media

June 28, 2023

O redirecionamento do Windows Media controla e otimiza a maneira como os servidores fornecem streaming de áudio e vídeo aos usuários. Com a reprodução dos arquivos de tempo de execução de mídia no dispositivo cliente em vez do servidor, o redirecionamento do Windows Media reduz os requisitos de largura de banda para reproduzir arquivos multimídia. O redirecionamento do Windows Media melhora o desempenho do Windows Media Player e players compatíveis em execução em áreas de trabalho virtuais do Windows.

Se os requisitos para a busca de conteúdo do lado do cliente do Windows Media não forem atendidos, o fornecimento de mídia usará automaticamente a obtenção no lado do servidor. Este método é transparente para os usuários. Você pode usar o Citrix Scout para executar um rastreamento de Citrix Diagnosis Facility (CDF) a partir de HostMMTransport.dll para determinar o método usado. Para obter mais informações, consulte Citrix Scout.

O redirecionamento do Windows Media intercepta o pipeline de mídia no servidor host, captura os dados de mídia em seu formato comprimido nativo e redireciona o conteúdo para o dispositivo cliente. Em seguida, o dispositivo cliente recria o pipeline de mídia para descompactar e renderizar os dados de mídia recebidos do servidor host. O redirecionamento do Windows Media funciona bem em dispositivos clientes que têm um sistema operacional Windows. Esses dispositivos têm a estrutura multimídia necessária para reconstruir o pipeline de mídia como ele existia no servidor host. Os clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento do Windows Media** controla esse recurso e é **Permitido** por padrão. Normalmente, essa configuração aumenta a qualidade de áudio e vídeo renderizada do servidor para um nível comparável ao conteúdo reproduzido localmente em um dispositivo cliente. Em casos raros, a reprodução de mídia usando o redirecionamento do Windows Media parece pior do que a mídia renderizada usando compactação básica ICA e áudio normal. Você pode desativar esse recurso adicionando a configuração de **Redirecionamento de Mídia do Windows** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações da política, consulte Configurações de política multimídia.

Limitação:

Quando você estiver utilizando o Windows Media Player e as Extensões Remotas de Áudio e Vídeo (RAVE) ativadas dentro de uma sessão, poderá aparecer uma tela preta. Esta tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Em Execução no início**.

Redirecionamento geral de conteúdo

June 28, 2023

O redirecionamento de conteúdo permite controlar se os usuários acessam informações usando aplicativos publicados em servidores ou usando aplicativos executados localmente no dispositivo dos usuários.

Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a maneira como os arquivos do lado do cliente são acessíveis na sessão do lado do host.

- Quando você ativa somente o mapeamento da unidade do cliente no servidor, os volumes completos do lado do cliente são mapeados automaticamente para as sessões como links UNC (Convenção de nomenclatura universal).
- Quando você ativa o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo desktop do Windows, a parte do volume local especificado pelo usuário é redirecionada.

Redirecionamento de host para cliente

Considere usar o redirecionamento do host para o cliente para casos específicos de uso incomum. Normalmente, outras formas de redirecionamento de conteúdo podem ser melhores. Damos suporte a esse tipo de redirecionamento somente em VDAs de SO multissessão e não em VDAs de SO de sessão única.

Acesso a aplicativo local e redirecionamento de URL

O Acesso a Aplicativo Local integra aplicativos do Windows instalados localmente em um ambiente de desktop hospedado. Ele faz isso sem mudar de um computador para outro.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não têm suporte otimizado ou quando este é inadequado.

Redirecionamento de pasta do cliente

June 28, 2023

O redirecionamento de pasta do cliente altera a maneira como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Se você ativar somente o mapeamento da unidade do cliente no servidor, os volumes completos do lado do cliente são mapeados automaticamente para as sessões como links da Convenção de Nomenclatura Universal (UNC). Quando você ativa o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo desktop do Windows, a parte do volume local especificado pelo usuário é redirecionada.

Somente as pastas especificadas pelo usuário aparecem como links UNC dentro das sessões. Ou seja, em vez do sistema de arquivos completo no dispositivo do usuário. Se você desabilitar links UNC

através do registro, as pastas do cliente aparecerão como unidades mapeadas dentro da sessão.

O redirecionamento da pasta do cliente é suportado apenas em máquinas do sistema operacional Windows de sessão única.

O redirecionamento da pasta do cliente para uma unidade USB externa não é salvo ao desanexar e reconectar o dispositivo.

Ativar o redirecionamento da pasta do cliente no servidor. Em seguida, no dispositivo cliente, especifique quais pastas devem ser redirecionadas. O aplicativo usado para especificar as opções de pasta do cliente está incluído no aplicativo Citrix Workspace fornecido com esta versão.

Requisitos:

Para servidores:

- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter
- Windows Server 2012 R2, edições Standard e Datacenter

Para clientes:

- Windows 10, edições de 32 bits e 64 bits (versão mínima 1607)
- Windows 8.1, edições de 32 bits e 64 bits (incluindo edição Embedded)
- Windows 7, edições de 32 bits e 64 bits (incluindo edição Embedded)

Para habilitar o redirecionamento de pasta de cliente no servidor, consulte Redirecionamento de pasta do cliente na lista de recursos gerenciados através do registro.

No dispositivo do usuário, especifique quais pastas redirecionar:

1. Verifique se a versão mais recente do aplicativo Citrix Workspace está instalada.
2. No diretório de instalação do aplicativo Citrix Workspace, inicie o CtxCFRUI.exe.
3. Escolha o botão de opção **Custom** e adicione, edite ou remova pastas.
4. Desconecte e reconecte suas sessões para que a configuração tenha efeito.

Redirecionamento de host para cliente

June 28, 2023

O redirecionamento de host para cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix, sejam abertas usando o aplicativo correspondente no dispositivo de ponto de extremidade do usuário. Alguns casos de uso comuns para redirecionamento de host para cliente incluem:

- Redirecionamento de sites nos casos em que o servidor Citrix não tem acesso da Internet ou da rede à fonte.
- Redirecionamento de sites quando executar um navegador da Web dentro da sessão Citrix não é desejado por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos nos casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento de host para cliente não se destina a URLs que você acessa em uma página da Web ou digita na barra de endereços do navegador da Web em execução na sessão Citrix. Para redirecionar URLs em navegadores da Web, consulte Redirecionamento de URL bidirecional ou Redirecionamento de conteúdo do navegador.

Requisitos do sistema

- VDA para SO multissessão
- Clientes compatíveis:
  - Aplicativo Citrix Workspace para Windows
  - Aplicativo Citrix Workspace para Mac
  - Aplicativo Citrix Workspace para Linux
  - Aplicativo Citrix Workspace para HTML5
  - Aplicativo Citrix Workspace para Chrome

O dispositivo cliente deve ter um aplicativo instalado e configurado para lidar com o redirecionamento dos tipos de URL.

Configuração

Use a política Citrix Host to client redirection para ativar essa funcionalidade. **Host to client redirection** é desativada por padrão. Depois de ativar a política Host to client redirection, o aplicativo Citrix Launcher se registra no servidor Windows para garantir que ele possa interceptar URLs e enviá-las para o dispositivo cliente.

Em seguida, você deve configurar a política de grupo do Windows para usar o Citrix Launcher como o aplicativo padrão para os tipos de URL necessários. No VDA do servidor Citrix, crie o arquivo ServerFTAdefaultPolicy.xml e insira o seguinte código XML.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2
3 <DefaultAssociations>
4
5 <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
     ServerFTA" />
```



```
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

No console de gerenciamento de política de grupo, vá para **Configuração do computador > Modelos Administrativos > Componentes do Windows > Explorador de Arquivos > Definir um arquivo de configuração de associações padrão** e salve o seu arquivo ServerFTAdefaultPolicy.xml.

> **Nota:**
>
> Se um servidor Citrix não tiver as configurações da política de grupo, o Windows solicitará que os usuários selecionem um aplicativo para abrir URLs.

Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Para incluir tipos de URL padrão ou personalizados adicionais na lista para redirecionamento, crie uma nova linha **Association Identifier** no arquivo ServerFTAdefaultPolicy.xml referenciado anteriormente. Por exemplo:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```

```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

Adicionar tipos de URL à lista também requer a configuração do cliente. Crie a seguinte chave de registro e os valores no cliente Windows.

> **Nota:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto

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

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome do valor: ExtraURLProtocols
- Tipo de valor: REG_SZ
- Dados de valor: especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade do URL. Por exemplo:
  `ftp://;mailto:;customtype1:///;custometype2://`

Você pode adicionar tipos de URL somente para clientes Windows. Os clientes que não têm as configurações de registro acima rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para lidar com os tipos de URL especificados.

Para remover os tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e os valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD
- Dados de valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados de valor: especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

```
http
https
rtsp
```

Para habilitar o redirecionamento de host para cliente para um conjunto específico de sites, crie uma chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: ValidSites
- Tipo de valor: REG_MULTI_SZ
- Dados de valor: especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNS). Digite vários FQDNS em linhas separadas. Inclua somente o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este caractere curinga combina um único nível de domínio, que é consistente com as regras no RFC 6125. Por exemplo:

`www.exmaple.com`

`*.example.com`

> **Nota:**
>
> Você não pode usar a chave **ValidSites** em combinação com as chaves **DisableServerFTA** e **NoRedirectClasses**.

Configuração do navegador padrão de VDA do servidor

Ativar o redirecionamento de host para cliente, conforme mencionado nesta seção, substitui qualquer configuração padrão anterior do navegador no VDA do servidor. Se um URL da Web não for redirecionado, o Citrix Launcher passa a URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente. Para obter mais informações, consulte Configuração do navegador padrão de VDA do servidor na lista de recursos gerenciados através registro.

Redirecionamento de conteúdo bidirecional

June 28, 2023

O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS presentes em navegadores da Web, ou incorporados em aplicativos, sejam encaminhados entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Um URL inserido em um navegador em execução na sessão Citrix pode ser aberto por meio do navegador padrão do cliente. Por outro lado, um URL inserido em um navegador em execução no cliente pode ser aberto em uma sessão Citrix, tanto com um aplicativo publicado quanto uma área de trabalho. Alguns casos de uso comuns para redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da Web nos casos em que o navegador inicial não tem acesso de rede à fonte.
- Redirecionamento de URLs da web por motivos de segurança e compatibilidade do navegador.
- Não é desejável o redirecionamento de URLs da Web incorporados em aplicativos durante a execução de um navegador da Web na sessão Citrix ou no cliente.

Requisitos do sistema

- VDAs de SO de sessão única ou multissessão
- Aplicativo Citrix Workspace para Windows

Navegadores:

- Internet Explorer 11
- Extensão de redirecionamento do Google Chrome com Citrix Browser (disponível na Google Chrome Web Store)
- Microsoft Edge (Chromium) com extensão de redirecionamento de navegador Citrix (disponível na Google Chrome Web Store)

Configuração

O redirecionamento de conteúdo bidirecional deve ser ativado usando a política da Citrix no VDA e no cliente para que o redirecionamento funcione. O redirecionamento de conteúdo bidirecional está desativado por padrão.

Quanto à configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações de política do ICA.

Quanto à configuração do cliente, consulte Redirecionamento de conteúdo bidirecional na documentação do aplicativo Citrix Workspace para Windows.

As extensões do navegador devem ser registradas por meio dos comandos mostrados. Execute os comandos conforme necessário no VDA e no cliente com base no navegador em uso.

Para registrar as extensões do navegador no VDA, abra um prompt de comando. Em seguida, execute o `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` com a opção de navegador necessária, conforme mostrado nos exemplos seguintes:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Para registrar a extensão em todos os navegadores disponíveis, execute:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Para cancelar o registro de uma extensão do navegador, use a opção `/unreg<browser>`, como no exemplo mostrado:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Para registrar as extensões do navegador no cliente, abra um prompt de comando e execute o `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` com as mesmas opções dos exemplos mostrados.

> **Nota:**
>
> O comando de registro faz com que os navegadores Chrome e Edge solicitem aos usuários que habilitem a Extensão de Redirecionamento de Navegador Citrix durante a primeira inicialização. A extensão do navegador também pode ser instalada manualmente por meio da Google Chrome Web Store.

Redirecionamento com curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de caracteres curinga para definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Web Studio, defina a URL curinga em **Allowed URLs to be redirected to Client**. O asterisco (*) é o caractere curinga.

> **NOTA:**
>
> - Não defina **Allowed URLs to be redirected to VDA** na política do cliente. Certifique-se de que os sites tenham definido **Allowed URLs to be redirected to VDA** para evitar loops de redirecionamento infinitos.
> - Domínios de nível superior não são suportados. Por exemplo, `https://www.citrix.*` ou `http://www.citrix.co*` não são redirecionados.

Redirecionamento de protocolo personalizado do VDA para o cliente

O redirecionamento de conteúdo bidirecional suporta o redirecionamento de protocolos personalizados do Citrix VDA para o cliente. Protocolos diferentes de HTTP ou HTTPS são suportados. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Web Studio, defina o protocolo personalizado em **Allowed URLs to be redirected to Client**.

> **NOTA:**
>
> - O cliente deve ter um aplicativo registrado para lidar com o protocolo. Caso contrário, a URL será redirecionada para o cliente e não será iniciada.
> - URLs de protocolos personalizados que você insere ou inicia nos navegadores Chrome e Edge não são compatíveis e não são redirecionados.
> - Os seguintes protocolos não são suportados: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

Outras considerações

- Os requisitos e configurações do navegador são aplicáveis apenas ao navegador que inicia o redirecionamento. O navegador de destino, onde o URL é aberto após um redirecionamento bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, apenas no VDA é necessária uma configuração de navegador com suporte. Por outro lado, ao redirecionar URLs do cliente para um VDA, apenas no cliente é necessária uma configuração de navegador com suporte. Os URLs redirecionados são transferidos para o navegador padrão configurado na máquina de destino, o cliente ou o VDA, dependendo da direção. Não é necessário usar o mesmo tipo de navegador no VDA e no cliente.
- Verifique se as regras de redirecionamento não resultam em uma configuração em loop. Por exemplo, uma política de VDA é definida para redirecionar o `https://www.citrix.com` e a política de cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Somente URLs do protocolo HTTP/HTTPS têm suporte. Não há suporte para encurtadores de URL.
- O redirecionamento de cliente para VDA requer que o cliente Windows seja instalado com direitos de administrador.
- Se o navegador de destino já estiver aberto, o URL redirecionado será aberto em uma nova guia. Caso contrário, o URL será aberto em uma nova janela do navegador.
- O redirecionamento de conteúdo bidirecional não funciona quando o LAA (Local App Access) está ativado.

Acesso a aplicativo local e redirecionamento de URL

June 28, 2023

Introdução

O Local App Access integra perfeitamente os aplicativos do Windows instalados localmente em um ambiente de trabalho hospedado sem mudar de uma área de trabalho para outra. Com o acesso ao aplicativo local, você pode:

- Acessar aplicativos instalados localmente em um laptop, PC ou outro dispositivo físico diretamente da área de trabalho virtual.
- Fornecer uma solução flexível de entrega de aplicativos. Se os usuários tiverem aplicativos locais que você não pode virtualizar ou que a TI não mantém, esses aplicativos ainda se comportam como se estivessem instalados em uma área de trabalho virtual.

- Elimine a latência de salto duplo quando os aplicativos são hospedados separadamente da área de trabalho virtual. Faça isso colocando um atalho para o aplicativo publicado no dispositivo Windows do usuário.
- Use aplicativos como:
  - Software de videoconferência, como o GoToMeeting.
  - Aplicações especializadas ou de nicho que ainda não estão virtualizadas.
  - Aplicativos e periféricos que, de outra forma, transfeririam grandes quantidades de dados de um dispositivo de usuário para um servidor e de volta para o dispositivo do usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops, as sessões de desktop hospedadas usam o redirecionamento de URL para iniciar aplicativos de acesso ao aplicativo local. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de bloqueios de URL do navegador) selecionando links incorporados dentro de um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueios, o URL será aberto novamente na sessão da área de trabalho.

O redirecionamento de URL funciona apenas para sessões de área de trabalho, não para sessões de aplicativos. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo do host para o cliente, que é um tipo de redirecionamento FTA (File Type Association) do servidor. Este FTA reorienta determinados protocolos para o cliente, como HTTP, HTTPS, RTSP ou MMS. Por exemplo, se você abrir apenas links incorporados com HTTP, os links serão abertos diretamente com o aplicativo cliente. Não há lista de bloqueio de URL ou suporte de lista de permissão.

Quando o acesso ao aplicativo local estiver habilitado, as URLs que são exibidas aos usuários como links de aplicativos em execução localmente, de aplicativos hospedados pelo usuário ou como atalhos na área de trabalho são redirecionados de uma das seguintes maneiras:

- Do computador do usuário para a área de trabalho hospedada
- Do servidor Citrix Virtual Apps and Desktops ao computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento do conteúdo de sites específicos, configure a lista de permissões de URL e a lista de bloqueios de URL no Virtual Delivery Agent. Essas listas contêm chaves de registro de várias cadeias de caracteres que especificam as configurações de política de redirecionamento de URL. Para obter mais informações, consulte as Configurações da política de acesso ao aplicativo local.

Os URLs podem ser renderizados no VDA com as seguintes exceções:

- Informações sobre geografia/localidade —Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na área geográ-

fica). Por exemplo, se o VDA for provisionado a partir de um data center no Reino Unido e o cliente estiver se conectando da Índia, o usuário espera ver in.msn.com. Em vez disso, o usuário vê uk.msn.com.
- Conteúdo multimídia —Os sites que contêm conteúdo de mídia avançada, quando renderizados no dispositivo cliente, proporcionam aos usuários finais uma experiência nativa e também economizam largura de banda mesmo em redes de alta latência. Esse recurso redireciona sites com outros tipos de mídia, como o Silverlight. Este processo está em um ambiente seguro. Ou seja, os URLs que o administrador aprova são executados no cliente quando o resto dos URLs for reorientado ao VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento de FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, o aplicativo local deve ter acesso ao arquivo para abri-lo. Portanto, você só pode abrir arquivos que residem em compartilhamentos de rede ou em unidades de cliente (usando o mapeamento de drive do cliente) usando aplicativos locais. Por exemplo, ao abrir um arquivo PDF, se um leitor de PDF for um aplicativo local, o arquivo será aberto usando esse leitor de PDF. Como o aplicativo local pode acessar o arquivo diretamente, não há transferência de rede do arquivo através do ICA para abrir o arquivo.

Requisitos, considerações e limitações

Damos suporte a acesso ao aplicativo local nos sistemas operacionais válidos para VDAs para SO Windows multi-sessões e para VDAs para SO Windows de sessão única. O acesso ao aplicativo local requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são compatíveis:

- Edge, versão mais recente
- Firefox, versão mais recente e versão com suporte estendido
- Chrome, versão mais recente

Leia as seguintes considerações e limitações ao usar o acesso a aplicativos locais e o redirecionamento de URL.

- O acesso ao aplicativo local foi concebido para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o acesso ao aplicativo local com uma área de trabalho virtual executada no modo janela ou que não cobre todos os monitores.
  - Vários monitores —Quando um monitor é maximizado, ele se torna a área de trabalho padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo se os aplicativos subsequentes tipicamente começarem em outro monitor.
  - O recurso suporta um VDA. Não há integração com vários VDAs simultâneos.

- Alguns aplicativos podem se comportar inesperadamente, afetando os usuários:
  - As letras da unidade podem confundir usuários, como a unidade C: local em vez de área de trabalho virtual C:.
  - As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
  - Os aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados pelo cliente.
  - Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).
  - Os aplicativos locais aparecem com o tema Windows da máquina local.
  - Os aplicativos de tela cheia não têm suporte. Esses aplicativos incluem aplicativos que se abrem para uma tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem toda a área de trabalho.
  - O acesso ao aplicativo local copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
  - Os aplicativos que personalizam como a ordem de janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
  - Os atalhos não têm suporte, incluindo Meu computador, Lixeira, Painel de controle, atalhos da unidade de rede e atalhos de pasta.
  - Os seguintes arquivos e tipos de arquivo não têm suporte: tipos de arquivos personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
  - O agrupamento da barra de tarefas não tem suporte o para aplicativos mistos de 32 bits e 64 bits hospedados no cliente ou VDA. Ou seja, agrupando aplicativos locais de 32 bits com aplicativos VDA de 64 bits.
  - Os aplicativos não podem ser iniciados por meio de COM. Por exemplo, se você clicar em um documento do Office incorporado dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local será malsucedida.
- Cenários de salto duplo, em que um usuário está iniciando uma área de trabalho virtual a partir de outra sessão de desktop virtual, não têm suporte.
- O redirecionamento de URL suporta apenas URLs explícitas (isto é, URLs que aparecem na barra de endereços do navegador ou encontrados usando a navegação no navegador, dependendo do navegador).
- O redirecionamento de URL funciona apenas com sessões de área de trabalho, não com sessões de aplicativos.
- A pasta local da área de trabalho em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução local se comportam de acordo com as configurações da barra de tarefas estabelecidas para a área de trabalho virtual. No entanto, os

atalhos para aplicativos em execução local não são agrupados com instâncias em execução desses aplicativos. Eles também não são agrupados com instâncias em execução de aplicativos hospedados ou atalhos fixados para aplicativos hospedados. Os usuários podem fechar apenas janelas de aplicativos em execução localmente a partir da Barra de Tarefas. Embora os usuários possam fixar janelas de aplicativos locais na barra de tarefas e no menu Iniciar da área de trabalho, os aplicativos podem não ser iniciados de forma uniforme por meio desses atalhos.

- Se você definir a definição de política **Allow Local App Access** como **Enabled**, o redirecionamento de conteúdo do navegador não tem suporte. Por padrão, o acesso a aplicativos locais é proibido.

Interação com o Windows

A interação acesso ao aplicativo local com o Windows inclui os seguintes comportamentos.

- Comportamento de atalho do Windows 8 e Windows Server 2012
  - Os aplicativos da Windows Store instalados no cliente não são enumerados como parte dos atalhos de acesso ao aplicativo local.
  - Os arquivos de imagem e vídeo são abertos por padrão por meio do aplicativos da loja do Windows. No entanto, o acesso ao aplicativo local enumera os aplicativos de armazenamento do Windows e abre atalhos com aplicativos de desktop.
- Programas Locais
  - No Windows 7, a pasta está disponível no menu Iniciar.
  - No Windows 8, os Programas Locais só estão disponíveis quando o usuário escolhe **All Apps** como uma categoria na tela Iniciar. Nem todas as subpastas são exibidas em Programas Locais.
- Recursos gráficos do Windows 8 para aplicativos
  - Os aplicativos de desktop estão restritos à área de trabalho e são cobertos pela tela inicial e pelos aplicativos de estilo do Windows 8.
  - Os aplicativos Local App Access não se comportam como aplicativos de desktop no modo multi-monitor. No modo multi-monitor, a tela Iniciar e a área de trabalho são exibidos em monitores diferentes.
- Windows 8 e redirecionamento de URL de acesso ao aplicativo local
  - Como o Windows 8 Internet Explorer não tem complementos habilitados, use o Internet Explorer para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desativa os complementos por padrão. Para implementar o redirecionamento de URL, desative a configuração aprimorada do Internet

Explorer. Em seguida, redefina as opções do Internet Explorer e reinicie para garantir que os complementos estejam habilitados para usuários padrão.

Configurar o acesso ao aplicativo local e o redirecionamento de URL

Para usar o acesso a aplicativos locais e o redirecionamento de URL com o aplicativo Citrix Workspace:

- Instale o aplicativo Citrix Workspace no computador cliente local. Você pode habilitar ambos os recursos durante a instalação do aplicativo Citrix Workspace ou habilitar o modelo Acesso a aplicativos locais usando o editor de política de grupo.
- Defina a configuração da política **Allow Local App Access** como **Enabled**. Você também pode configurar configurações de política de lista de permissão de URL e lista de bloqueios para redirecionamento de URL. Para obter mais informações, consulte as Configurações da política de acesso ao aplicativo local.

Habilitar o acesso a aplicativo local e redirecionamento de URL

Para habilitar o acesso ao aplicativo local para todos os aplicativos locais, siga estas etapas:

1. Faça logon no Web Studio e clique em **Policies** no painel esquerdo.
2. Na barra de ações, clique em **Create Policy**.
3. Na janela Criar política, digite "Allow Local App Access"na caixa de pesquisa e clique em **Select**.
4. Na janela Edit Setting, selecione **Allowed**. Por padrão, a política **Allow local app access** é proibida. Quando essa configuração é permitida, o VDA permite que o usuário final decida se os aplicativos publicados e os atalhos de Acesso a aplicativos locais devem estar ativados na sessão. (Quando essa configuração é proibida, tanto os aplicativos publicados quanto os atalhos de Acesso a aplicativos locais não funcionam para o VDA.) Essa configuração de política se aplica a todo o computador e à política de redirecionamento de URL.
5. Na janela Criar política, digite "URL redirection allow list"na caixa de pesquisa e clique em **Select**. A lista de permissões de redirecionamento de URL especifica as URLs que devem ser abertas no navegador padrão da sessão remota.
6. Na janela Edit setting, clique em **Add** para adicionar os URLs e clique em **OK**.
7. Na janela Create Policy, digite "URL redirection block list"na caixa de pesquisa e clique em **Select**. A lista de bloqueios de redirecionamento de URL especifica URLs que são redirecionados para o navegador padrão em execução no ponto de extremidade.
8. Na janela Edit setting, clique em **Add** para adicionar os URLs e clique em **OK**.
9. Na página Settings, clique em **Next**.
10. Na página Users and Machines, atribua a política aos grupos de entrega aplicáveis e clique em **Next**.

11. Na página Summary, revise as configurações e clique em **Finish**.

Para habilitar o redirecionamento de URL para todos os aplicativos locais durante a instalação do aplicativo Citrix Workspace, siga estas etapas:

1. Ative o redirecionamento de URL ao instalar o aplicativo Citrix Workspace para todos os usuários em um computador. Isso também registra os complementos do navegador necessários para o redirecionamento de URL.
2. No prompt de comando, execute o comando apropriado para instalar o aplicativo Citrix Workspace usando uma das seguintes opções:
    - Para CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
    - Para CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Habilitar o modelo Acesso ao aplicativo local usando o editor de política de grupo

> **Nota:**
>
> - Antes de ativar o modelo Acesso a aplicativos locais usando o editor de política de grupo, adicione os arquivos de modelo receiver.admx/adml ao GPO local.
> - Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Administrative Templates > Citrix Components > Citrix Workspace** somente quando você adiciona CitrixBase.admx/CitrixBase.adml à pasta %system-root%\policyDefinitions.

Para habilitar o modelo acesso ao aplicativo local usando o editor de política de grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá até **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Workspace > User Experience**.
3. Clique em **Local App Access settings**.
4. Selecione **Enabled** e depois selecione **Allow URL Redirection**. Para redirecionamento de URL, registre complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais abaixo neste artigo.

Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o PowerShell SDK.

Para o Editor do Registro, consulte O Local App Access para aplicativos publicados na lista de recursos gerenciados através do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina em que o Delivery Controller está sendo executado.
2. Digite o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEn "-value "true"`.

Para ter acesso a **Add Local App Access Application** em uma implantação de serviço de nuvem, use o Remote PowerShell SDK do Citrix DaaS. Para obter mais informações, consulte Remote PowerShell SDK 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. Digite o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEn "-value "true"`.

Depois de concluir as etapas anteriores aplicáveis, siga estas etapas para continuar.

1. Entre no Web Studio e selecione **Applications** no painel esquerdo.
2. No painel central superior, clique com o botão direito do mouse na área em branco e selecione **Add Local App Access Application** do menu de contexto. Você também pode clicar em **Add Local App Access Application** na barra de ações. Para exibir a opção Add Local App Access Application na barra de ações, clique em **Refresh**.
3. Publique o aplicativo Local App Access.

   - O assistente de Acesso a Aplicativos Locais é iniciado com uma página Introdução, que você pode remover de inicializações futuras do assistente.
   - O assistente orienta você pelas páginas Groups, Location, Identification, Delivery e Summary descritas abaixo. Quando terminar cada página, clique em **Next** até chegar à página Summary.
   - Na página Groups, selecione um ou mais grupos de entrega onde os novos aplicativos serão adicionados e clique em **Next**.
   - Na página Location, digite o caminho executável completo do aplicativo na máquina local do usuário e digite o caminho para a pasta onde o aplicativo está localizado. A Citrix recomenda que você use o caminho da variável de ambiente do sistema; por exemplo, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.

- Na página Identification, aceite os valores padrão ou digite as informações desejadas e clique em **Next**.
- Na página Delivery, configure como esse aplicativo é fornecido aos usuários e clique em **Next**. Você pode especificar o ícone para o aplicativo selecionado. Você também pode especificar se o atalho para o aplicativo local na área de trabalho virtual está visível no menu Iniciar, na área de trabalho ou em ambos.
- Na página Summary, revise as configurações e clique em **Finish** para sair do assistente Local Application Access.

Registrar complementos do navegador

> **Nota:**
>
> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente quando você instala o aplicativo Citrix Workspace a partir da linha de comando usando a opção /ALLOW_CLIENTHOSTEDAPPSURL =1.

Você pode usar os seguintes comandos para registrar e cancelar o registro de um ou todos os complementos:

- Para registrar complementos em um dispositivo cliente: <*client-installation-folder*>\redirector.exe /reg<*navegador*r>
- Para cancelar o registro de complementos em um dispositivo cliente: <*client-installation-folder*>\redirector.exe /unreg<*navegador*>
- Para registrar complementos em um VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*navegador*>
- Para cancelar o registro de complementos em um VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*navegador*>

Onde <*navegador*> é Internet Explorer, Firefox, Chrome ou All.

Por exemplo, o comando a seguir registra complementos do Internet Explorer em um dispositivo que executa o aplicativo Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

O comando a seguir registra todos os complementos em um VDA com SO multissessão Windows.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

Intercepção de URL entre navegadores

- Por padrão, o Internet Explorer redireciona a URL especificada. Se a URL não estiver na lista de bloqueios, mas o navegador ou site o redireciona para outro URL, o URL final não será redire-

cionado. Ele não é redirecionado mesmo se estiver na lista de bloqueios.

Para que o redirecionamento de URL funcione corretamente, ative o complemento quando solicitado pelo navegador. Se os complementos que estão usando as opções da Internet ou os complementos no prompt estiverem desativados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam os URLs.

Quando um complemento é instalado, o Firefox avisa para permitir ou impedir a instalação do complemento em uma nova página de guias. Permita que o complemento do recurso funcione.

- O complemento do Chrome sempre redireciona a URL final que é navegada e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desabilita a extensão, o recurso de redirecionamento de URL não funciona no Chrome. Se o redirecionamento de URL for necessário no modo de navegação anônima, permita que a extensão seja executada nesse modo nas configurações do navegador.

Configurar o comportamento do aplicativo local no logoff e na desconexão

> **Nota:**
>
> Se você não seguir estas etapas para configurar as configurações, por padrão, os aplicativos locais continuarão a ser executados quando um usuário fizer logoff ou se desconectar da área de trabalho virtual. Após a reconexão, os aplicativos locais serão reintegrados se estiverem disponíveis na área de trabalho virtual.

Para configurar o comportamento do aplicativo local no logoff e na desconexão, consulte Comportamento do aplicativo local no logoff e na desconexão na lista de recursos gerenciados através do registro.

Considerações genéricas de redirecionamento USB e unidade de cliente

June 28, 2023

A tecnologia HDX fornece **suporte otimizado** para a maioria dos dispositivos USB mais difundidos. O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes de alta latência ou sensíveis à segurança.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não têm suporte otimizado ou quando este é inadequado.

- O dispositivo USB tem recursos mais avançados que não fazem parte do suporte otimizado, como um mouse ou webcam com mais botões.
- Os usuários precisam de funções que não fazem parte do suporte otimizado.
- O dispositivo USB é um dispositivo especializado, como equipamentos de teste e medição ou um controlador industrial.
- Um aplicativo requer acesso direto ao dispositivo como um dispositivo USB.
- O dispositivo USB tem apenas um driver do Windows disponível. Por exemplo, um leitor de cartão inteligente pode não ter um driver disponível para o aplicativo Citrix Workspace para Android.
- A versão do aplicativo Citrix Workspace não fornece suporte otimizado para esse tipo de dispositivo USB.

Com redirecionamento USB genérico:

- Os usuários não precisam instalar drivers de dispositivo no dispositivo do usuário.
- Os drivers de cliente USB são instalados na máquina VDA.

> **Importante:**
>
> - O redirecionamento USB genérico pode ser usado em conjunto com suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as Configurações de política de dispositivos USB Citrix para o redirecionamento USB genérico e suporte otimizado.
> - A configuração de política Citrix nas Regras de otimização do dispositivo USB do cliente é uma configuração específica para o redirecionamento USB genérico, para um dispositivo USB específico. Não se aplica ao suporte otimizado conforme descrito aqui.

Considerações de desempenho para dispositivos USB

A latência e a largura de banda da rede podem afetar a experiência do usuário e a operação do dispositivo USB ao usar o redirecionamento USB genérico para alguns tipos de dispositivos USB. Por exemplo, dispositivos sensíveis ao tempo podem não funcionar corretamente com links de baixa largura de banda de alta latência. Use suporte otimizado sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para que possam ser usados, por exemplo, um mouse 3D (usado com aplicativos 3D que normalmente também exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você pode ser capaz de mitigar o problema ajustando o uso da largura de banda de outros componentes usando as configurações da política de largura de banda. Para obter mais informações, consulte as Configurações da política de largura de banda, para o redirecionamento de dispositivo USB do cliente, e Configurações de políticas de conexões multi-stream.

Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartões inteligentes, leitores de impressões digitais e mesas gráficas para assinatura. Outros dispositivos USB, como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser sensíveis.

Dispositivos USB são usados frequentemente para distribuir malware. A configuração do aplicativo Citrix Workspace e do Citrix Virtual Apps and Desktops pode reduzir, mas não eliminar, os riscos desses dispositivos USB. Esta situação se aplica se for usado o redirecionamento USB genérico ou suporte otimizado.

> **Importante:**
>
> Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX usando TLS ou IPsec.
>
> Ative apenas o suporte para os dispositivos USB de que você precisa. Configure o redirecionamento USB genérico e o suporte otimizado para atender a essa necessidade.
>
> Forneça orientação aos usuários para uso seguro de dispositivos USB:
>
> - Use apenas dispositivos USB obtidos a partir de uma fonte confiável.
> - Não deixe dispositivos USB desacompanhados em ambientes abertos - por exemplo, uma unidade flash em um internet café.
> - Explique os riscos de usar um dispositivo USB em mais de um computador.

Compatibilidade com redirecionamento USB genérico

O redirecionamento USB genérico é suportado para dispositivos USB 2.0 e anteriores. O redirecionamento USB genérico também é suportado para dispositivos USB 3.0 conectados a uma porta USB 2.0 ou USB 3.0. O redirecionamento USB genérico não suporta recursos USB introduzidos no USB 3.0, como super velocidade.

Esses aplicativos do Citrix Workspace oferecem suporte ao redirecionamento USB genérico:

- Aplicativo Citrix Workspace para Windows, consulte Configuração da entrega de aplicativos.
- Aplicativo Citrix Workspace para Mac, consulte Aplicativo Citrix Workspace para Mac.
- Aplicativo Citrix Workspace para Linux, consulte Otimizar.
- Aplicativo Citrix Workspace para Chrome OS, consulte Aplicativo Citrix Workspace para Chrome.

Para ver as versões do aplicativo Citrix Workspace, consulte a Matriz de recursos do aplicativo Citrix Workspace.

Se você estiver usando versões anteriores do aplicativo Citrix Workspace, consulte a documentação do aplicativo Citrix Workspace para confirmar que o redirecionamento USB genérico tem suporte.

Consulte a documentação do aplicativo Citrix Workspace para saber sobre as restrições aos tipos de dispositivos USB compatíveis.

O redirecionamento USB genérico é suportado para sessões de desktop do VDA para o sistema operacional de sessão única versão 7.6 até a atual.

O redirecionamento USB genérico tem suporte para sessões de desktop do VDA para a versão 7.6 do SO multissessão até a atual, com estas restrições:

- O VDA deve estar executando o Windows Server 2012 R2, o Windows Server 2016, o Windows Server 2019 ou o Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o RDSH (Remote Desktop Session Host) para o sistema operacional VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não têm suporte para redirecionamento USB genérico porque não seria útil redirecioná-los:

- Modems USB.
- Adaptadores de rede USB.
- Hubs USB Os dispositivos USB conectados a hubs USB são manipulados individualmente.
- Portas USB COM virtuais. Use o redirecionamento da porta COM em vez de redirecionamento USB genérico.

Para obter informações sobre dispositivos USB que foram testados com redirecionamento USB genérico, consulte Citrix Ready Marketplace. Alguns dispositivos USB não funcionam corretamente com o redirecionamento USB genérico.

Configurar o redirecionamento USB genérico

Você pode controlar e configurar separadamente quais tipos de dispositivos USB usam o redirecionamento USB genérico:

- No VDA, usando as configurações de política Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações da política de dispositivos USB na referência de configurações de políticas
- No aplicativo Citrix Workspace, usando mecanismos dependentes de aplicativos do Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações do registro que configuram o aplicativo Citrix Workspace para Windows. Por padrão, o redirecionamento USB é permitido para certas classes de dispositivos USB e negado para outros. Para obter mais informações, consulte Configure na documentação do aplicativo Citrix Workspace para Windows.

Esta configuração separada fornece flexibilidade. Por exemplo:

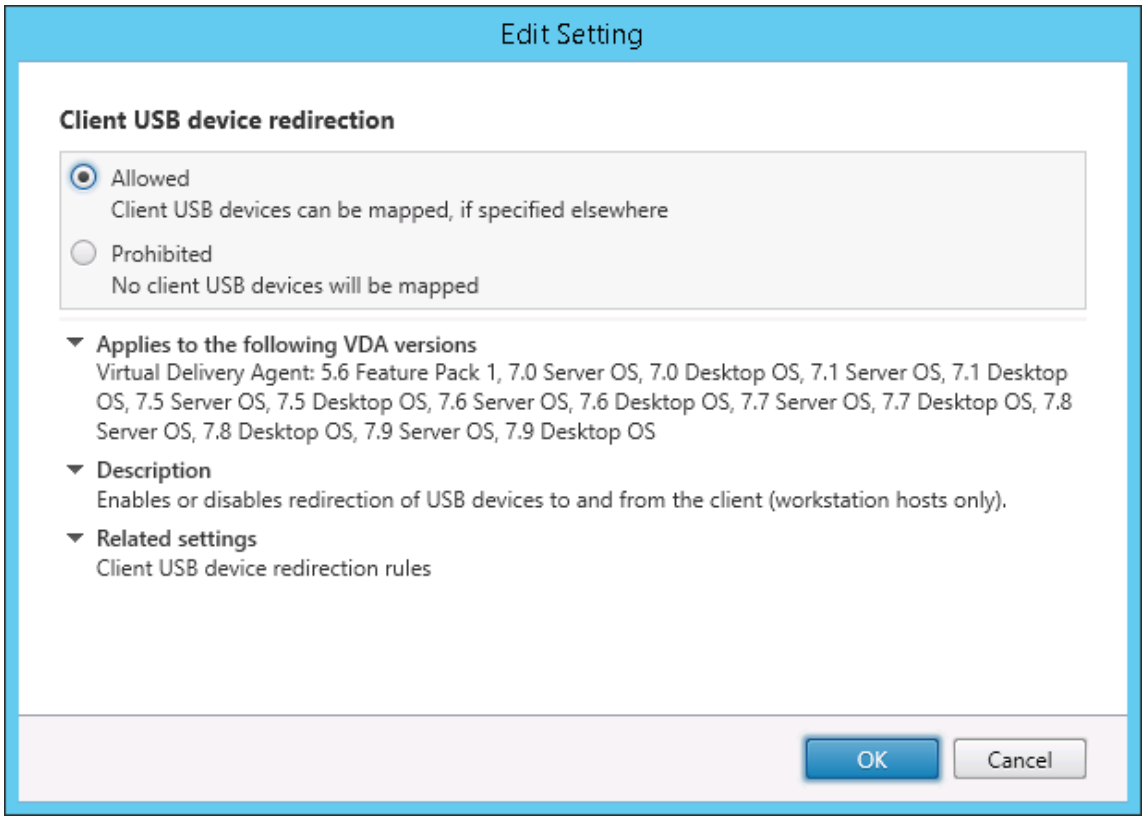
- Se duas organizações ou departamentos diferentes forem responsáveis pelo aplicativo Citrix Workspace e pelo VDA, elas poderão impor o controle separadamente. Essa configuração se aplica quando um usuário em uma organização acessa um aplicativo em outra organização.
- As configurações de política do Citrix podem controlar dispositivos USB permitidos apenas para determinados usuários ou para usuários que se conectam somente por uma LAN (em vez de usar o Citrix Gateway).

Enable generic USB redirection

Para habilitar o redirecionamento USB genérico e não exigir o redirecionamento manual pelo usuário, faça as configurações de política Citrix e as preferências de conexões do aplicativo Citrix Workspace.

Nas configurações da política Citrix:

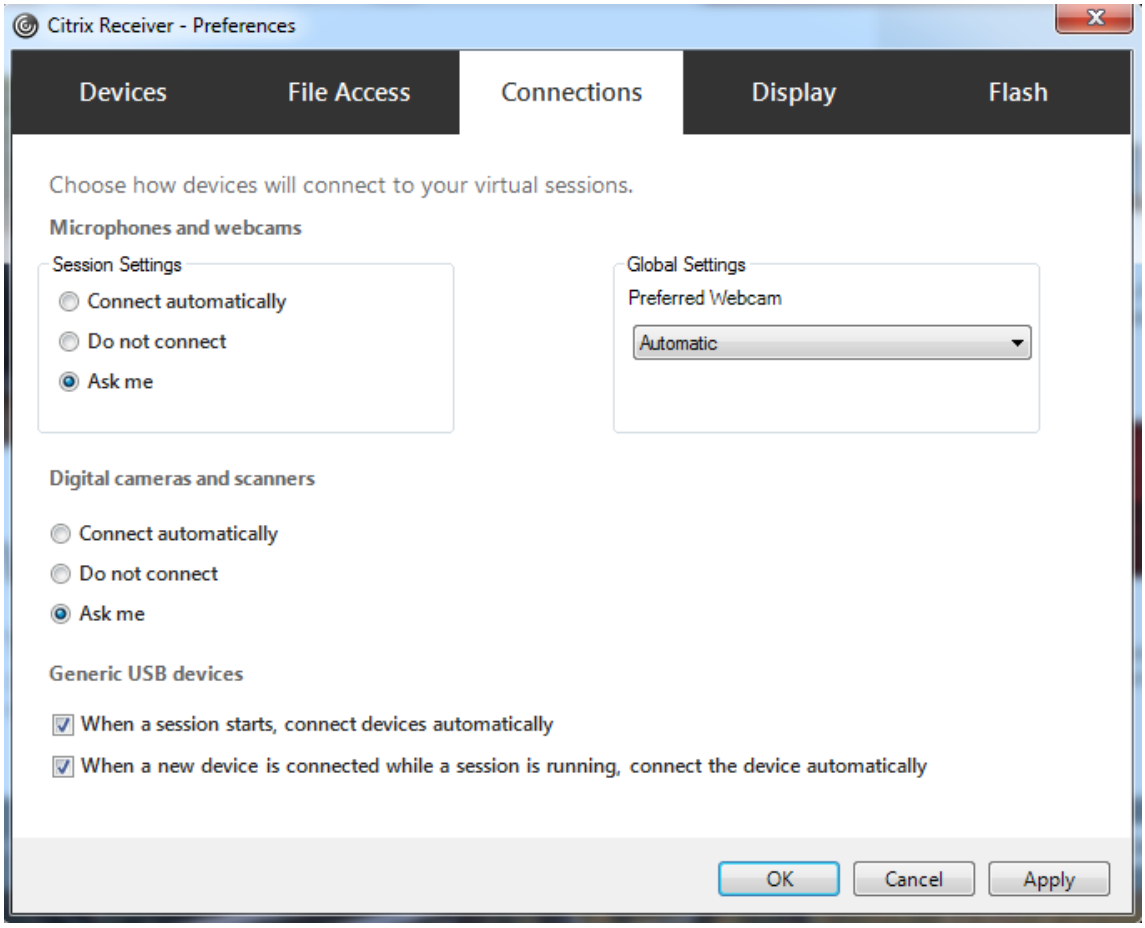
1. Adicione Client USB device redirection a uma política e defina seu valor como **Allowed**.



2. (Opcional) Para atualizar a lista de dispositivos USB disponíveis para redirecionamento, adicione a configuração Client USB device redirection rules a uma política e especifique as regras de política USB.

   Quando as configurações da política estiverem concluídas, no aplicativo Citrix Workspace:

3. Especifique se os dispositivos são conectados automaticamente sem redirecionamento manual. Você pode fazer isso usando um modelo administrativo ou no aplicativo Citrix Workspace para **Windows > Preferences > Connections**.



Se você especificou as regras de política USB para o VDA na etapa anterior, especifique as mesmas regras de política para o aplicativo Citrix Workspace.

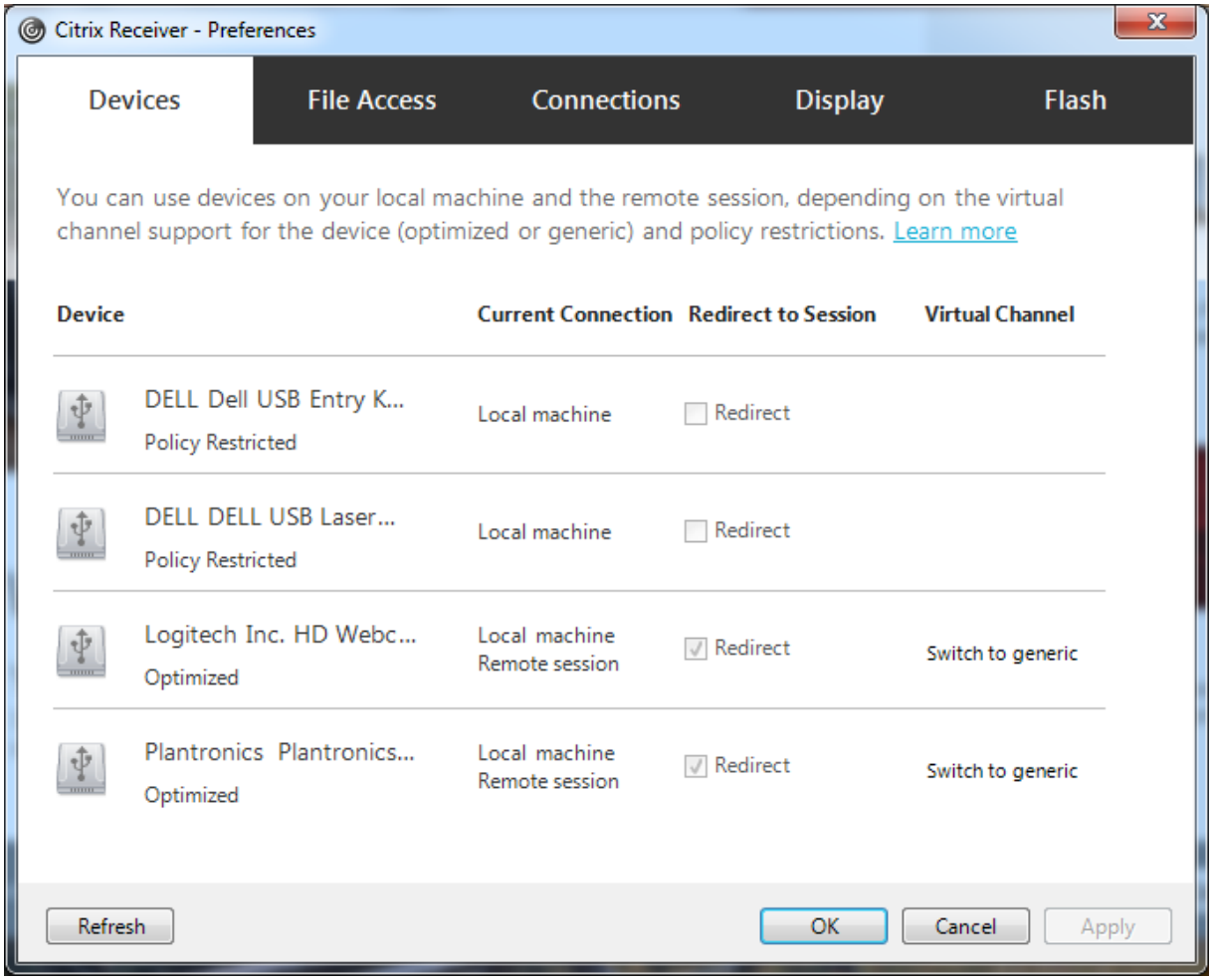
Para clientes finos, consulte o fabricante para obter detalhes sobre o suporte USB e a configuração necessária.

Configuração dos tipos de dispositivos USB disponíveis para redirecionamento USB genérico

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado e as configurações de preferência do usuário USB são definidas para conectar dispositivos USB automaticamente. Os dispositivos USB também são redirecionados automaticamente quando a barra de conexão não está presente.

Os usuários podem redirecionar explicitamente dispositivos que não são redirecionados automaticamente selecionando os dispositivos na lista de dispositivos USB. Para obter mais informações, con-

sulte o artigo da ajuda do usuário do aplicativo Citrix Workspace para Windows Exibir seus dispositivos no Desktop Viewer.



Para usar o redirecionamento USB genérico em vez de suporte otimizado, você pode:

- No aplicativo Citrix Workspace, selecione manualmente o dispositivo USB para usar o redirecionamento USB genérico, escolha **Switch to generic** na guia Devices da caixa de diálogo Preferences.
- Selecione automaticamente o dispositivo USB para usar o redirecionamento USB genérico, configurando o redirecionamento automático para o tipo de dispositivo USB (por exemplo, AutoRedirectStorage=1) e defina as configurações de preferência do usuário USB para conectar automaticamente dispositivos USB. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

> **Nota:**
>
> Apenas configure o redirecionamento USB genérico para uso com uma webcam se a webcam for considerada incompatível com o redirecionamento multimídia de HDX.

Para evitar que dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e para o VDA.

Para redirecionamento USB genérico, você precisa saber pelo menos a classe de dispositivo USB e a subclasse. Nem todos os dispositivos USB usam sua classe de dispositivo USB e subclasse óbvias. Por exemplo:

- As canetas usam a classe dispositivo mouse.
- Os leitores de cartões inteligentes podem usar a classe de dispositivo definido pelo fornecedor ou HID.

Para um controle mais preciso, você precisa saber o ID do fornecedor, o ID do produto e o ID da versão. Você pode obter essas informações do fornecedor do dispositivo.

> **Importante:**
>
> Dispositivos USB maliciosos podem apresentar características do dispositivo USB que não correspondem ao uso pretendido. As regras do dispositivo não se destinam a impedir esse comportamento.

Você controla os dispositivos USB disponíveis para redirecionamento USB genérico especificando regras de redirecionamento de dispositivos USB para substituir as regras de política USB padrão.

Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service):

- Na maioria dos casos, baixe Citrix Group Policy Management Console MSI (`CitrixGroupPolicyManagem.msi`) e instale-o em seu sistema Active Directory, e então gerencie as políticas de grupo do AD. (Não instale o MSI em um VDA.)
- Para o aplicativo Citrix Workspace para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário através da política de grupo do Active Directory:dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops local:

- Para o VDA, edite as regras de substituição do administrador para os computadores do SO multissessão por meio de regras de política de grupo. O console de gerenciamento de política de grupo está incluído na mídia de instalação:
  - x64: dvd root `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: dvd root `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Para o aplicativo Citrix Workspace para Windows, edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa

alterar o dispositivo do usuário através da política de grupo do Active Directory:dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

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

As regras padrão do produto são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB. Não edite estas regras padrão do produto. Em vez disso, use-os como um guia para criar regras de substituição de administrador, o que é explicado mais adiante neste artigo. As substituições de GPO são avaliadas antes das regras padrão do produto.

As regras de substituição do administrador são armazenadas em HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citri
As regras de política de GPO assumem o formato **{Allow:|Deny:}** seguido por um conjunto de expressões *tag=value* separadas por espaço em branco.

As seguintes marcas têm suporte:

Marca	Descrição
VID	ID do fornecedor do descritor de dispositivo
PID	ID do produto do descritor do dispositivo
REL	Liberar ID do descritor de dispositivo
Class	Classe do descritor de dispositivo ou de um descritor de interface; consulte o site USB em http://www.usb.org/ para códigos de classe USB disponíveis
SubClass	Subclasse do descritor de dispositivo ou de um descritor de interface
Prot	Protocolo do descritor de dispositivo ou de um descritor de interface

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas e minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por #. Não é obrigatório usa delimitador, e o comentário é ignorado para fins de correspondência.
- As linhas em branco ou puramente de comentários são ignoradas.

- O espaço em branco é usado como separador, mas não pode aparecer no meio de um número ou identificador. Por exemplo, Deny: Class = 08 SubClass=05 é uma regra válida, mas Deny: Class=0 Sub Class=05 não é.
- As marcas devem usar o operador correspondente =. Por exemplo, VID=1230.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.

> **Nota:**
>
> - A partir da versão 2212 do Citrix Virtual Apps and Desktops, o uso do recurso de redirecionamento USB genérico está desabilitado para alguns dispositivos USB. Você deve adicionar esses dispositivos explicitamente usando seus respectivos ID do fornecedor (VID) e ID do produto (PID).
> - Se você estiver usando o arquivo de modelo ADM, deverá criar regras em uma única linha, como uma lista separada por ponto e vírgula.

Exemplos:

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para identificadores de fornecedor e produto:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para uma classe, subclasse e protocolo definidos:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

Usar e remover dispositivos USB

Os usuários podem conectar um dispositivo USB antes ou depois de iniciar uma sessão virtual.

Ao usar o aplicativo Citrix Workspace para Windows, o seguinte se aplica:

- Os dispositivos conectados após o início de uma sessão aparecem imediatamente no menu USB do Desktop Viewer.
- Se um dispositivo USB não estiver redirecionando corretamente, você pode tentar resolver o problema aguardando para conectar o dispositivo até que a sessão virtual seja iniciada.
- Para evitar a perda de dados, use o ícone "Remover hardware com segurança"do Windows antes de remover o dispositivo USB.

Controles de segurança para dispositivos de armazenamento em massa USB

É fornecido suporte otimizado para dispositivos de armazenamento em massa USB. Esse suporte faz parte do mapeamento da unidade cliente Citrix Virtual Apps and Desktops. As unidades no dispositivo do usuário são mapeadas automaticamente para letras de unidades na área de trabalho virtual quando os usuários fazem logon. As unidades são exibidas como pastas compartilhadas que têm letras de unidade mapeadas. Para configurar o mapeamento da unidade cliente, use a configuração **Client removable drives**. Essa configuração está na seção Configurações da política de redirecionamento de arquivos das configurações de política ICA.

Com dispositivos USB de armazenamento em massa, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados pelas políticas da Citrix. Controle-os usando as políticas Citrix. As principais diferenças são:

Recurso	Client drive mapping	Redirecionamento USB genérico
Ativado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes de o dispositivo ser acessado	Sim
Dispositivos BitLocker To Go	Não	Não
Exclusão segura do dispositivo durante uma sessão	Não	Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura

Se o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estiverem ativados e um dispositivo de armazenamento em massa for inserido antes ou depois que uma sessão seja iniciada, ele será redirecionado por meio do mapeamento da unidade cliente. Quando o redirecionamento USB genérico e as políticas de mapeamento da unidade cliente estão ativadas e um dispositivo é configurado para redirecionamento automático e um dispositivo de armazenamento em massa é inserido antes ou depois que uma sessão seja iniciada, ele é redirecionado por meio do redirecionamento USB genérico. Para obter mais informações, consulte o artigo do Knowledge Center CTX123015.

> **Nota:**
>
> O redirecionamento USB tem suporte em conexões de largura de banda mais baixa, por exemplo,

> 50 Kbps. No entanto, copiar arquivos grandes não funciona.

Controle o acesso a arquivos com mapeamento da unidade do cliente

Você pode controlar se os usuários podem copiar arquivos de seus ambientes virtuais para seus dispositivos de usuário. Por padrão, os arquivos e pastas em unidades de cliente mapeadas estão disponíveis no modo de leitura/gravação a partir da sessão.

Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, ative a configuração de política **Read-only client drive access**. Ao adicionar essa configuração a uma política, verifique se a configuração de redirecionamento da unidade cliente está definida como **Allowed** e também adicionada à política.

Impressão

June 28, 2023

Gerenciar impressoras em seu ambiente é um processo de vários estágios:

1. Familiarize-se com os conceitos de impressão, se não estiver ainda.
2. Planeje sua arquitetura de impressão. Isso inclui analisar suas necessidades de negócios, sua infraestrutura de impressão existente, como seus usuários e aplicativos interagem com a impressão hoje e qual modelo de gerenciamento de impressão se aplica melhor ao seu ambiente.
3. Configure seu ambiente de impressão selecionando um método de provisionamento de impressora e criando políticas para implantar seu design de impressão. Atualize políticas quando novos funcionários ou servidores forem adicionados.
4. Teste uma configuração de impressão piloto antes de implantá-la para os usuários.
5. Faça a manutenção do seu ambiente de impressão Citrix gerenciando drivers de impressora e otimizando o desempenho de impressão.
6. Solucione os problemas que possam surgir.

Conceitos de impressão

Antes de começar a planejar sua implantação, certifique-se de que você entende estes conceitos principais de impressão:

- Os tipos disponíveis de provisionamento de impressora
- Como os trabalhos de impressão são roteados
- Noções básicas de gerenciamento de drivers de impressora

Conceitos de impressão são compilados nos conceitos de impressão do Windows. Para configurar e gerenciar a impressão em seu ambiente com êxito, você deve entender como funciona a impressão em rede e cliente do Windows e como isso se traduz em comportamento de impressão nesse ambiente.

Processo de impressão

Neste ambiente, toda a impressão é iniciada (pelo usuário) em computadores que hospedam aplicativos. Os trabalhos de impressão são redirecionados através do servidor de impressão de rede ou dispositivo do usuário para o dispositivo de impressão.

Não há espaço de trabalho persistente para usuários de áreas de trabalho e aplicativos virtuais. Quando uma sessão termina, o espaço de trabalho do usuário é excluído, portanto, todas as configurações precisam ser recompiladas no início de cada sessão. Como resultado, toda vez que um usuário inicia uma nova sessão, o sistema deve recompilar o espaço de trabalho do usuário.

Quando um usuário imprime:

- Determina quais impressoras oferecer ao usuário. Isso é conhecido como provisionamento de impressoras.
- Restaura as preferências de impressão do usuário.
- Determina qual impressora é o padrão para a sessão.

Você pode personalizar como executar essas tarefas configurando opções para provisionamento de impressoras, roteamento de tarefas de impressão, retenção de propriedades da impressora e gerenciamento de drivers. Certifique-se de avaliar como as diferentes configurações da opção podem alterar o desempenho da impressão em seu ambiente e a experiência do usuário.

Provisionamento da impressora

O processo que torna as impressoras disponíveis em uma sessão é conhecido como provisionamento. O provisionamento da impressora geralmente é 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 compilada durante o logon e a reconexão. Como resultado, as impressoras podem mudar de acordo com a política, a localização do usuário e as alterações de rede, desde que sejam refletidas nas políticas. Assim, os usuários que fazem roaming para um local diferente podem ver alterações em seu espaço de trabalho.

O sistema também monitora as impressoras do lado do cliente e ajusta dinamicamente as impressoras criadas automaticamente na sessão com base em adições, exclusões e alterações às impressoras do lado do cliente. Essa descoberta dinâmica da impressora beneficia os usuários móveis à medida que se conectam de diferentes dispositivos.

Os métodos mais comuns de provisionamento de impressoras são:

- **Universal Print Server** - O Citrix Universal Print Server oferece suporte a impressão universal para impressoras de rede. O servidor de impressão universal usa o driver de impressão Universal. Essa solução permite que você use um único driver em um computador com SO multissessão para permitir a impressão de rede a partir de qualquer dispositivo.

A Citrix recomenda o Citrix Universal Print Server para os cenários de servidor de impressão remota. O servidor de impressão universal 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.

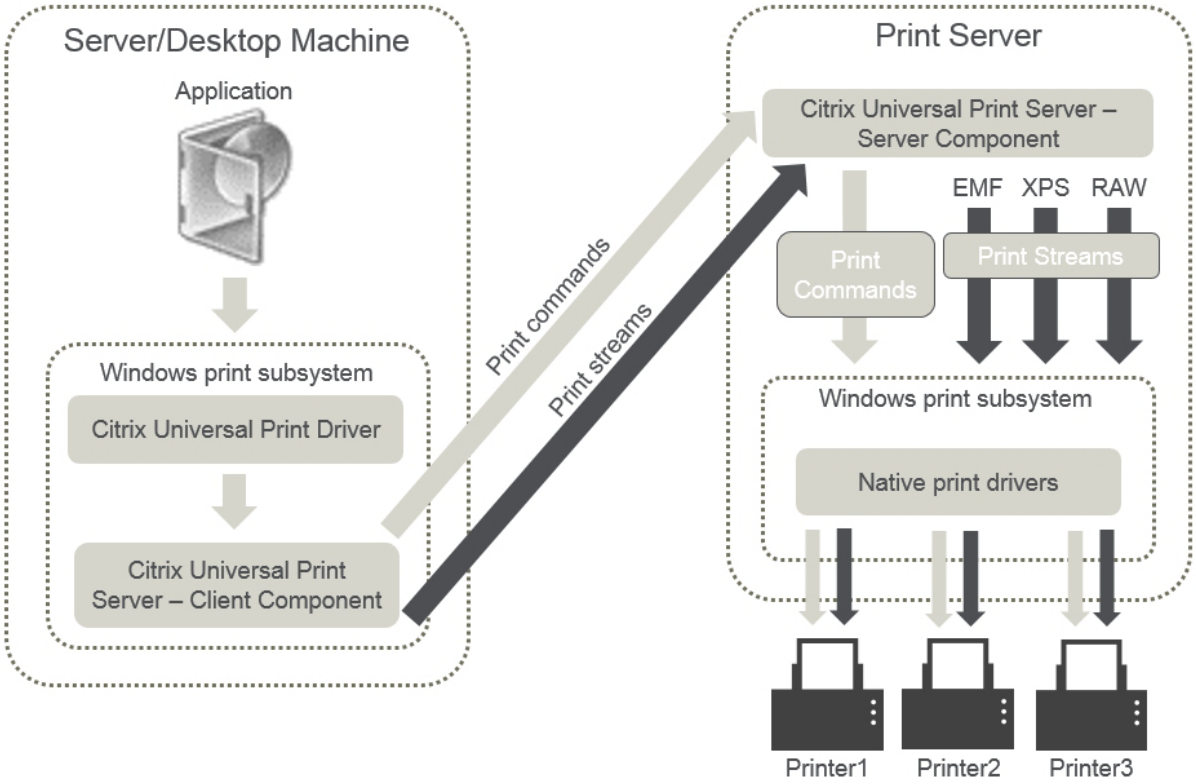
O recurso de servidor de impressão universal compreende:

Um componente de cliente, **UPClient** - Habilite o UPClient em cada computador com SO multissessão 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 da sessão serem provisionadas centralmente).

Para obter os requisitos do servidor de impressão universal e os detalhes de configuração, consulte os artigos requisitos do sistema e instalação.

A ilustração a seguir mostra o fluxo de trabalho típico de uma impressora baseada em rede em um ambiente que usa o servidor de impressão universal.



Quando você ativa 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 criar automaticamente apenas a impressora cliente padrão para ambientes com um grande número de impressoras por usuário. A criação automática de um número menor de impressoras usa menos sobrecarga (memória e CPU) em computadores com SO multissessão. Minimizar as impressoras criadas automaticamente também pode reduzir os tempos de logon do usuário.

  As impressoras criadas automaticamente são baseadas em:

  - Impressoras instaladas no dispositivo do usuário.
  - Quaisquer políticas que se aplicam à sessão.

    As configurações da política de criação automática permitem limitar o número ou o tipo das impressoras criadas automaticamente. Por padrão, as impressoras estão disponíveis nas sessões ao configurar todas as impressoras no dispositivo do usuário automaticamente, incluindo impressoras de rede e conectadas localmente.

  Depois que o usuário encerra a sessão, as impressoras dessa sessão são excluídas.

A criação automática de impressora cliente e de rede tem manutenção associada. Por exemplo, adicionar uma impressora requer que você:

- Atualize a configuração de política de impressoras da sessão.
- Adicione o driver a todas as máquinas com SO multissessão usando a configuração de política Printer driver mapping and compatibility.

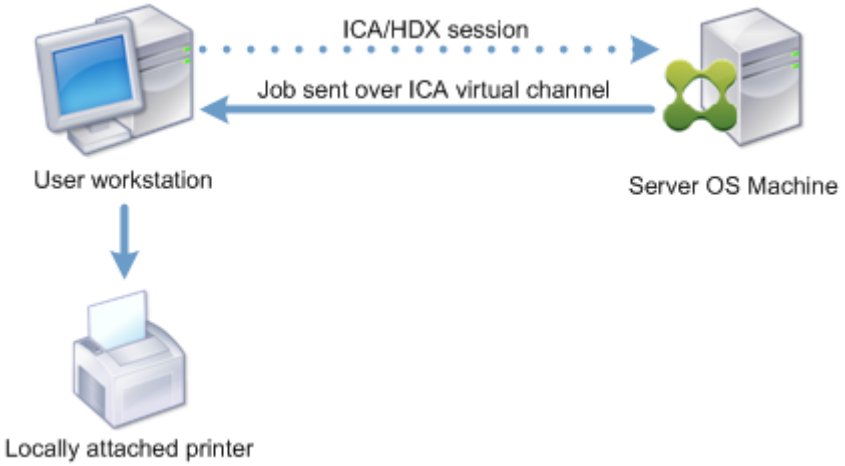
Roteamento de trabalho de impressão

O caminho de impressão do termo abrange tanto o caminho pelo qual os trabalhos de impressão são roteados quanto o local onde é feito o spool dos trabalhos de impressão. Ambos os aspectos desse conceito são importantes. O roteamento afeta o tráfego de rede. O spool 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 referidos como o caminho de impressão cliente e o caminho de impressão de rede. Qual caminho é escolhido por padrão depende do tipo de impressora usada.

Impressoras conectadas localmente

O sistema encaminha trabalhos para impressoras conectadas localmente a partir do computador com SO multissessão, seguindo através do cliente e então para o dispositivo de impressão. O protocolo ICA otimiza e comprime 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.



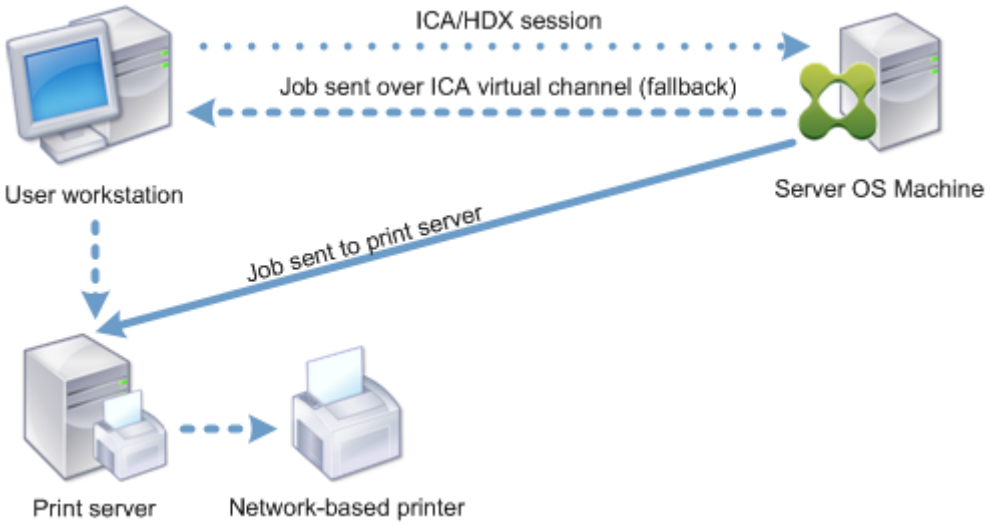
Impressoras baseadas em rede

Por padrão, todos os trabalhos de impressão destinados a impressoras de rede são roteados a partir do computador com SO multissessão, pela rede e diretamente para o servidor de impressão. No entanto, os trabalhos de impressão são roteados automaticamente pela conexão ICA nas seguintes situações:

- Se a área de trabalho ou aplicativo virtual não conseguir contatar o servidor de impressão.
- Se o driver de impressora nativo não estiver disponível no computador com SO multissessão.

Se o servidor de impressão universal não estiver ativado, configurar o caminho de impressão do cliente para impressão em rede é útil para conexões de baixa largura de banda, como redes de longa distância, que podem se beneficiar da otimização e compressão de tráfego resultante 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 os trabalhos de impressão. Se o roteamento de trabalhos pelo dispositivo do usuário não for possível, como para thin clients sem recursos de impressão, a qualidade do 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 driver da impressora universal Citrix (UPD) é um driver de impressão independente de dispositivo e 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 Citrix Virtual Apps and Desktops VDA. O VDA instala os seguintes drivers com o Citrix UPD: “Impressora Universal Citrix” (driver EMF) e “Impressora Universal Citrix XPS”(driver XPS).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

Os instaladores de VDA não mais oferecem opções para controlar a instalação do driver de impressora PDF do servidor de impressão universal. Agora, o driver de impressora PDF é sempre instalado automaticamente. Quando você atualiza para o 7.17 VDA (ou uma versão mais recente suportada), qualquer driver de impressora Citrix PDF 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 o envia, sem qualquer modificação no dispositivo de ponto final.

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.

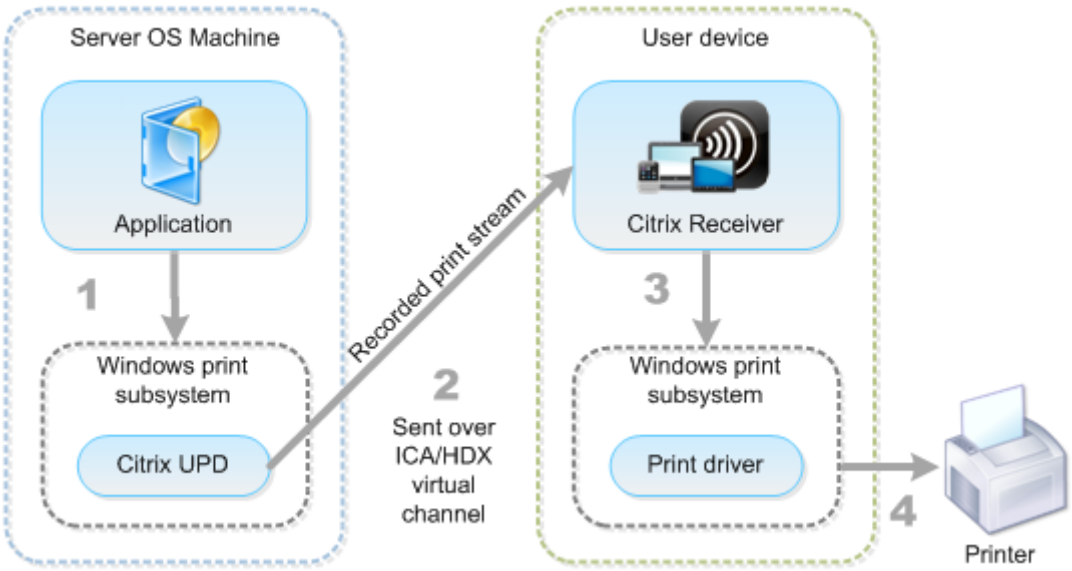
O Citrix UPD suporta os seguintes formatos de impressão:

- 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 no Windows.
- XML Paper Specification (**XPS**). O driver XPS usa XML para criar um "papel eletrônico"independente de plataforma semelhante ao formato Adobe PDF.
- Linguagem de Comando da 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 básico e gráficos e é amplamente suportado na HP LaserJet e periféricos multifuncionais.
- PostScript (**PS**). PostScript é uma linguagem de computador que pode ser usada para imprimir texto e gráficos vetoriais. O driver é amplamente utilizado em impressoras de baixo custo e periféricos multifuncionais.

Os drivers PCL e PS são mais adequados quando se usa dispositivos não baseados em Windows, como um cliente Mac ou UNIX. A ordem na qual o Citrix UPD tenta usar os drivers pode ser alterada usando a configuração da política Universal driver preference.

O Citrix UPD (drivers EMF e XPS) suporta recursos avançados de impressão, como grampeamento e seleção da origem do papel. Esses recursos estarão 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 palavras-chave não padronizadas forem usadas, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

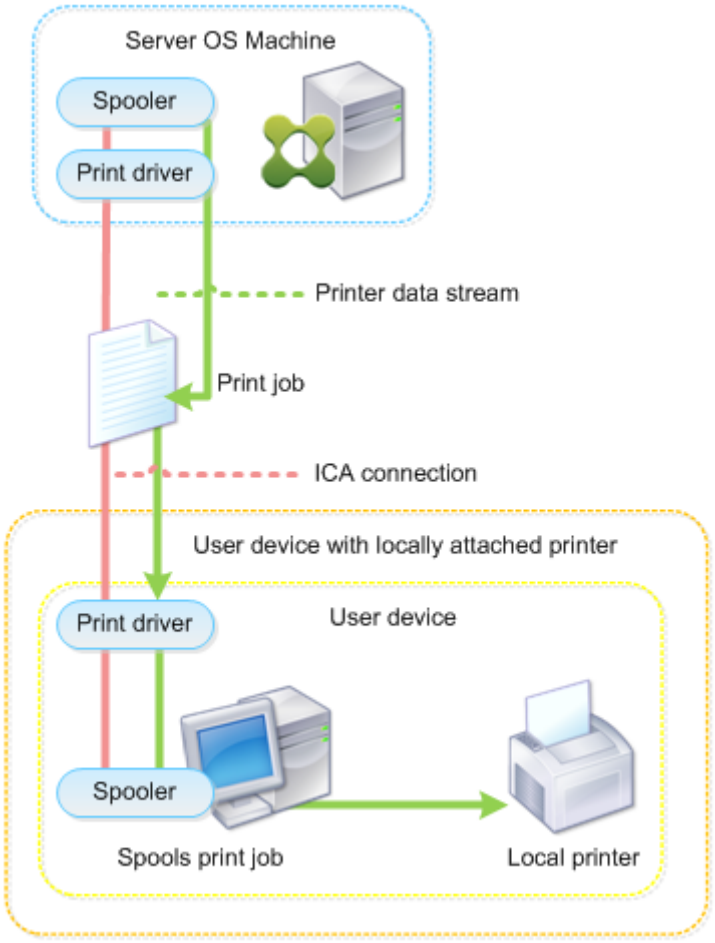
A ilustração a seguir mostra os componentes do driver de impressão universal e um fluxo de trabalho típico de uma impressora conectada localmente a um dispositivo.



Ao planejar sua estratégia de gerenciamento de drivers, determine se você suportará o driver de impressão universal, drivers específicos do dispositivo ou ambos. Se você aceitar drivers padrão, deve determinar:

Durante a criação automática da impressora, se o sistema detectar uma nova impressora local conectada a um dispositivo de usuário, ele verificará o computador com SO multissessão quanto ao 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 no computador com SO multissessão 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 para suportar.
- Se os drivers de impressora devem ser instalados automaticamente quando estão ausentes computadores com SO multissessão.
- Se deseja criar listas de compatibilidade de drivers.

Conteúdo relacionado

- Exemplo de configuração de impressão
- Práticas recomendadas, considerações de segurança e operações padrão
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

Exemplo de configuração de impressão

June 28, 2023

Escolher as opções de configuração de impressão mais adequadas para suas necessidades e ambiente pode simplificar a administração. Embora a configuração de impressão padrão permita que os usuários imprimam na maioria dos ambientes, os padrões podem não proporcionar a experiência do usuário esperada ou o uso de rede ideal e sobrecarga de gerenciamento para seu ambiente.

Sua configuração de impressão depende de:

- Suas necessidades comerciais e sua infraestrutura de impressão existente.

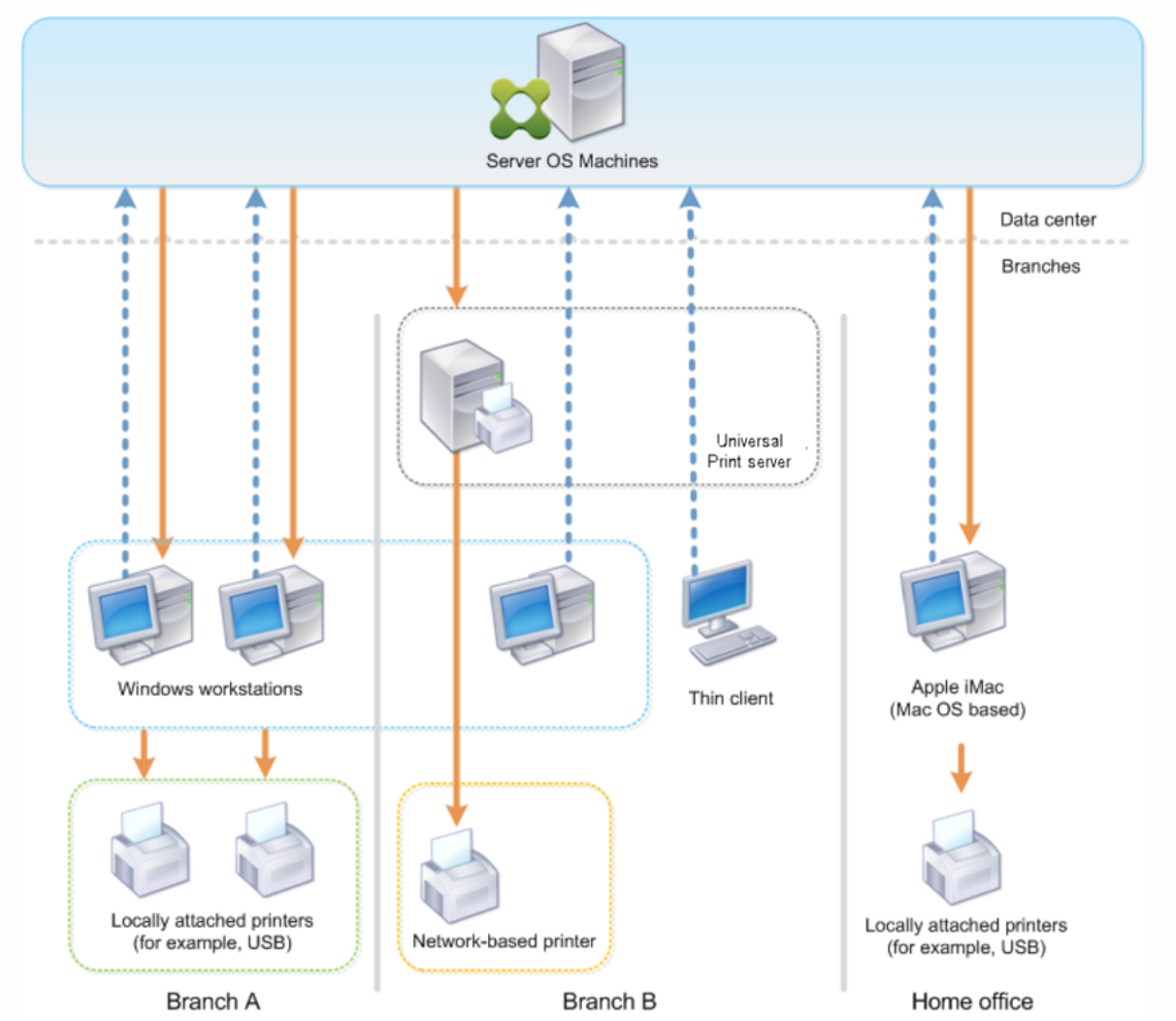
  Projete sua configuração de impressão de acordo com as necessidades de sua organização. Sua implementação de impressão existente (se os usuários podem adicionar impressoras, quais usuários têm acesso a quais impressoras e assim por diante) pode ser um guia útil ao definir sua configuração de impressão.
- Se a sua organização tem 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 deslocam entre estações de trabalho ou viajam a negócios.

Ao projetar sua configuração de impressão, tente oferecer aos usuários em uma sessão a mesma experiência que eles têm ao imprimir de dispositivos de usuário locais.

Exemplo de implantação de impressão

A ilustração a seguir mostra a implantação de impressão para esses casos de uso:

- **Filial A** –uma pequena filial no exterior com algumas estações de trabalho Windows. Cada estação de trabalho do usuário tem uma impressora privada conectada localmente.
- **Filial B** –uma filial grande com clientes finos e estações de trabalho baseadas no Windows. Para maior eficiência, os usuários dessa filial compartilham impressoras baseadas em rede (uma por andar). Os servidores de impressão baseados no Windows localizados na filial gerenciam as filas de impressão.
- **Home office** –Um escritório doméstico com um dispositivo de usuário baseado em Mac OS que acessa a infraestrutura Citrix da empresa. O dispositivo do 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 universal Citrix

Na filial A, todos os usuários trabalham em estações de trabalho baseadas no Windows, portanto, impressoras cliente criadas automaticamente e o driver de impressora universal são usados. Essas tecnologias oferecem esses benefícios:

- Desempenho –os trabalhos de impressão são entregues pelo canal de impressão ICA, portanto, os dados de impressão podem ser compactados para economizar largura de banda.

  Para garantir que um único usuário que imprime um documento grande não possa degradar 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 universal Citrix garante que todas as impressoras conectadas a um cliente também possam ser usadas a partir de uma sessão de aplicativo ou área de trabalho virtual sem integrar um novo driver de impressora no data center.

Citrix Universal Print Server

Na filial B, todas as impressoras são baseadas em rede e suas filas são gerenciadas em um servidor de impressão Windows, portanto, o Citrix Universal Print Server 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 na sessão do aplicativo ou área de trabalho virtual funciona da seguinte forma:

- Para estações de trabalho baseadas no Windows –a equipe de TI local ajuda os usuários a conectarem a impressora baseada em rede apropriada às suas estações de trabalho do Windows. Isso permite que os usuários imprimam a partir de aplicativos instalados localmente.

  Durante uma sessão de aplicativo ou área de trabalho virtual, as impressoras configuradas localmente são enumeradas por meio da autocriação. A área de trabalho ou aplicativo virtual se conecta ao servidor de impressão como uma conexão de rede direta, se possível.

  Os componentes do Citrix Universal Print Server são instalados e ativados, portanto, drivers de impressora nativos não são necessários. Se um driver for atualizado ou uma fila de impressora for modificada, nenhuma configuração adicional é necessária no data center.

- Para clientes finos –para usuários cliente fino, as impressoras devem estar conectadas na sessão de aplicativo ou área de trabalho virtual. Para oferecer aos usuários a experiência de impressão mais simples, os administradores configuram uma única política Citrix Session Printer 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 percorram os andares, as políticas são filtradas com base na sub-rede ou no nome do cliente fino. Essa configuração, conhecida como impressão por proximidade, permite a manutenção do driver da impressora local (de acordo com o modelo de administração delegada).

  Se uma fila de impressora precisar ser modificada ou adicionada, os administradores da Citrix deverão modificar a respectiva política Session printer dentro do ambiente.

Como o tráfego de impressão em rede será enviado para fora do canal virtual do ICA, a QoS é implementada. O tráfego de rede de entrada e saída nas portas usadas pelo tráfego ICA/HDX é priorizado

em relação a todos os outros tráfegos de rede. Essa configuração garante que as sessões do usuário não sejam afetadas por grandes trabalhos de impressão.

Impressoras cliente criadas automaticamente e driver de impressora universal Citrix

Para escritórios domésticos em que os usuários trabalham em estações de trabalho não padrão e usam dispositivos de impressão não gerenciados, a abordagem mais simples é usar impressoras cliente criadas automaticamente e o driver de impressora universal.

Resumo de implantação

Em resumo, a implantação de amostra é configurada da seguinte forma:

- Nenhum driver de impressora é instalado em máquinas com SO multissessão. Somente o driver de impressora universal Citrix é usado. O fallback para impressão nativa e a instalação automática de drivers de impressora são desativados.
- Uma política é configurada para criar automaticamente todas as impressoras cliente para todos os usuários. Por padrão, as máquinas com SO multissessão se conectarão diretamente aos servidores de impressão. A única configuração necessária é ativar 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 clientes finos do respectivo andar.
- A QoS é implementada para a filia B para garantir uma excelente experiência do usuário.

Práticas recomendadas, considerações de segurança e operações padrão

June 28, 2023

Práticas recomendadas

Muitos fatores determinam a melhor solução de impressão para um ambiente específico. Algumas dessas práticas podem não se aplicar ao seu site.

- Use o Citrix Universal Print Server.
- Use o driver de impressora universal ou os drivers nativos do Windows.
- Minimize o número de drivers de impressora instalados em máquinas com SO multissessão.

- 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 que possível, desinstale um driver, reinicie o servidor de impressão e, em seguida, instale o driver de substituição.
- Desinstale drivers não utilizados ou use a política Printer driver mapping and compatibility para evitar que impressoras sejam criadas com o driver.
- Tente evitar o uso de drivers no modo kernel versão 2.
- Para determinar se um modelo de impressora é compatível, entre em contato com o fabricante ou consulte o guia do produto Citrix Ready em www.citrix.com/ready.

  Em geral, todos os drivers de impressora fornecidos pela Microsoft são testados com os Serviços de Terminal e é garantido que funcionarão com a 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 Serviços de Terminal pelo programa Windows Hardware Quality Labs (WHQL). A Citrix não certifica drivers de impressora.

Considerações de segurança

As soluções de impressão Citrix são seguras por design.

- O 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 representando o usuário da sessão real.
- A impressão Citrix atribui a cada impressora um espaço de nome 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 estejam inacessíveis aos usuários em execução em outras sessões. Por padrão, os usuários administrativos não podem imprimir acidentalmente na impressora cliente de outra sessão, mesmo que possam ver e ajustar manualmente as permissões de qualquer impressora cliente.

Operações de impressão padrão

Por padrão, se você não configurar nenhuma regra de política, o comportamento de impressão é o seguinte:

- O Universal Print Server é desativado.
- Todas as impressoras configuradas no dispositivo do usuário são criadas automaticamente no início de cada sessão.

Esse comportamento equivale a definir a configuração da política Citrix de criação automática de impressoras cliente com a opção de criar automaticamente todas as impressoras cliente.

- O sistema roteia todos os trabalhos de impressão na fila para impressoras conectadas localmente aos dispositivos do usuário como trabalhos de impressão cliente (ou seja, pelo canal ICA e pelo dispositivo do usuário).
- O sistema encaminha todos os trabalhos de impressão na fila para impressoras de rede diretamente de máquinas com SO multissessão. Se o sistema não puder rotear os trabalhos pela rede, ele os roteará pelo dispositivo do usuário como um trabalho de impressão cliente redirecionado.

  Esse comportamento equivale a desabilitar a configuração da política Citrix de conexão direta com os servidores de impressão.
- O sistema tenta armazenar as propriedades de impressão, uma combinação das preferências de impressão do usuário com configurações específicas do dispositivo de impressão, no dispositivo do usuário. Se o cliente não suportar essa operação, o sistema armazena propriedades de impressão em perfis de usuário na máquina com SO multissessão.

  Esse comportamento equivale à configuração da política Citrix de retenção de propriedades da impressora com a opção Held in profile only if not saved on client.
- Nos VDAs versão 7.16 e posterior, a configuração de política Citrix "Automatic installation of inbox printer drivers"não tem nenhum efeito nas versões de sistemas operacionais Windows 8 e posteriores do Windows, pois os drivers de impressora V3 in-box não estão incluídos no sistema operacional.
- Em VDAs anteriores à 7.16, o sistema usa a versão Windows do driver da impressora se estiver disponível na máquina com sistema operacional multissessão. Se o driver da impressora não estiver disponível, o sistema tentará instalar o driver a partir do sistema operacional Windows. Se o driver não estiver disponível no Windows, ele usará um driver de impressão Citrix Universal.

  Esse comportamento equivale a habilitar a configuração de política Citrix "Automatic installation of in-box printer drivers"e definir a configuração de impressão Universal com a opção "Use universal printing only if requested driver is unavailable".

  Habilitar "Automatic installation of in-box printer drivers"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 Ativado. A opção que aparece é a padrão.

Log Always-On

Um recurso de log Always-On 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 fazer upload automático de logs para o Citrix Insight Services, use o cmdlet do PowerShell **Start-TelemetryUpload**.

Políticas e preferências de impressão

June 28, 2023

Quando os usuários acessam impressoras a partir de aplicativos publicados, você pode configurar políticas Citrix para especificar:

- Como as impressoras são provisionadas (ou adicionadas às sessões)
- Como os trabalhos de impressão são roteados
- Como os drivers de impressora são gerenciados

Você pode ter configurações de impressão diferentes 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 da política Citrix Printing. 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 de impressora na sessão, antes de procurar configurações e preferências em outros locais.

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 com SO multissessão. Quando um usuário altera as propriedades da impressora durante uma sessão, essas alterações são atualizadas no perfil do usuário na máquina. Na próxima vez em que o usuário fizer logon ou se reconectar, o dispositivo do usuário herdará essas configurações retidas. Ou seja, as alterações na propriedade da impressora no dispositivo do usuário não afetam a sessão atual até que o usuário faça logoff e logon novamente.

Locais de preferência de impressão

Em ambientes de impressão do Windows, as alterações feitas nas preferências de impressão podem ser armazenadas no computador local ou em um documento. Nesse ambiente, quando os usuários

modificam as configurações de impressão, as configurações são armazenadas nestes locais:

- **No próprio dispositivo do usuário** –os usuários 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 estiver selecionada como orientação de página, a paisagem será salva como a preferência de orientação de página padrão para essa impressora.
- **Dentro de um documento** –em programas de processamento de texto e publicação desktop, as configurações do documento, como orientação de página, geralmente são armazenadas dentro dos documentos. Por exemplo, quando você colocar um documento para impressão na fila, o Microsoft Word geralmente armazena as preferências de impressão especificadas, como orientação da página e nome da impressora, dentro do documento. Essas configurações aparecem por padrão na próxima vez que você imprimir esse documento.
- **A partir 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 tiver sido feita no Painel de controle na sessão, ou seja, na máquina com SO multissessão.
- **Na máquina com SO multissessão** –estas são as configurações padrão associadas a um driver de impressora específico na máquina.

As configurações preservadas em qualquer ambiente baseado no Windows variam de acordo com o local onde o usuário fez as alterações. Isso também significa que as configurações de impressão que aparecem em um lugar, como em um programa de planilhas, podem ser diferentes daquelas em outros lugares, como em um programa de documentos. Como resultado, as configurações de impressão aplicadas a uma impressora específica podem mudar ao longo de uma sessão.

Hierarquia das 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 observar que as configurações do dispositivo são tratadas de modo distinto das configurações do documento e geralmente têm precedência sobre elas.

Por padrão, o sistema sempre aplica todas as configurações de impressão que um usuário modificou durante uma sessão (ou seja, as configurações retidas) antes de considerar outras configurações. Quando o usuário imprime, o sistema mescla e aplica as configurações padrão da impressora armazenadas na máquina com SO multissessão com as configurações de impressora cliente ou retidas.

Salvar preferências de impressão do usuário

A Citrix recomenda que você não altere o local 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 faz o fallback automaticamente para o perfil do usuário na máquina com SO multissessão.

Revise a configuração da política de retenção de propriedades da impressora se esses cenários se aplicarem:

- Se você usa plug-ins herdados que não permitem que os usuários armazenem propriedades da impressora em um dispositivo de usuário.
- Se você usa perfis obrigatórios na sua rede Windows e quer manter as propriedades da impressora do usuário.

Provisionar impressoras

September 13, 2023

Citrix Universal Print Server

Ao determinar a melhor solução de impressão para o seu ambiente, considere o seguinte:

- O Universal Print Server oferece recursos não disponíveis para o Windows Print Provider: armazenamento em cache de imagens e fontes, compressão avançada, otimização e suporte a QoS.
- O driver de impressão universal suporta as configurações públicas independentemente dos dispositivos que são definidas pela Microsoft. Se os usuários precisarem acessar as configurações do 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. Um ponto a se considerar é que os drivers nativos do Windows requerem manutenção.
- O Citrix Universal Print Server oferece suporte a impressão universal para impressoras de rede. O Universal Print Server usa o driver de impressão universal, um único driver na máquina com SO multissessão que permite a impressão local ou em rede a partir de qualquer dispositivo, incluindo clientes finos e tablets.

Para usar o Universal Print Server com um driver nativo do Windows, ative o Universal Print Server. Por padrão, se o driver nativo do Windows estiver disponível, ele será usado. Caso contrário, o driver de impressão universal será usado. Para especificar alterações nesse comportamento, como usar somente o driver nativo do Windows ou somente o driver de impressão universal, atualize a configuração de política de uso do driver de impressão universal.

Instale o Universal Print Server

Para usar o Universal Print Server, instale o componente UpsServer em seus servidores de impressão, conforme descrito nos documentos de instalação, e configure-o. Para obter mais informações, consulte Instalar componentes principais e Instalar usando a linha de comando.

Para ambientes em que você deseja implantar o componente UPClient separadamente, por exemplo, com o **XenApp 6.5**:

1. Baixe o pacote autônomo Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) para o sistema operacional de sessão única Windows ou sistema operacional multissessão Windows.
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 somente 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. Localize o componente UPClient em \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
6. Instale o componente UPClient extraindo e iniciando o MSI do componente.
7. É necessária uma reinicialização após a instalação do componente UPClient.

Desativar o CEIP para o Universal Print Server

Você é automaticamente registrado no Programa de Aperfeiçoamento da Experiência do Usuário (CEIP) da Citrix ao instalar o Universal Print Server. O primeiro upload de dados ocorre após sete dias a partir da data e hora da instalação.

Para desativar o CEIP, edite a chave do registro **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** e defina o valor **DWORD** como **0**.

Para reativar, defina o valor DWORD como 1.

Cuidado: editar o registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

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.

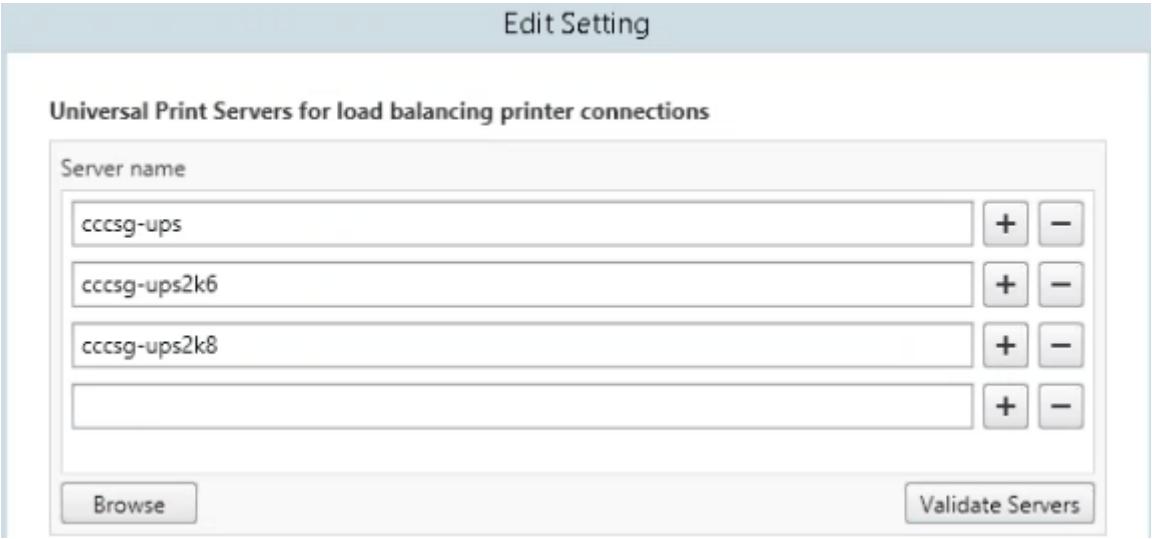
- **Universal Print Server enable**. O Universal Print Server está desativado por padrão. Ao ativar o Universal Print Server, você escolhe se deseja usar o Windows Print Provider se o Universal Print Server não estiver disponível. Depois de ativar o Universal Print Server, um usuário pode adicionar e enumerar impressoras de rede por meio das interfaces do Windows Print Provider e Citrix Provider.
- **Universal Print Server print data stream (CGP) port**. Especifica o número da porta TCP usado pelo ouvinte CGP (Common Gateway Protocol) de stream de dados de impressão do Universal Print Server. O padrão é **7229**.
- **Universal Print Server web service (HTTP/SOAP) port**. Especifica o número da porta TCP usada pelo ouvinte do Universal Print Server para solicitações HTTP/SOAP recebidas. O padrão é **8080**.

Para alterar a porta padrão do HTTP 8080 para comunicação do Universal Print Server com os VDAs do Citrix Virtual Apps and Desktops, o registro a seguir 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:\<númerodaporta\>

Esse número de porta deve corresponder à porta do serviço Web do Universal Print Server (HTTP/-SOAP), da política HDX, no Studio.

- **Universal Print Server print stream input bandwidth limit (kbps)**. Especifica o limite superior (em kilobits por segundo) da 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 for load balancing**. Essa configuração lista os Universal Print Servers que devem ser usados para balancear as conexões de impressora de balanceamento de carga estabelecidas na inicialização da sessão, depois de avaliar outras configurações de política de impressão 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.



- **Universal Print Servers out-of-service threshold**. Especifica por quanto tempo o balanceador de carga deve aguardar a recuperação de um servidor de impressão indisponível antes de determinar que o servidor está permanentemente offline e redistribua sua carga para outros servidores de impressão disponíveis. O padrão é 180 (segundos).

Depois que as políticas de impressão forem modificadas no Delivery Controller, pode levar alguns minutos para que as alterações da política sejam aplicadas aos VDAs.

Interactions with other policy settings —o Universal Print Server segue as outras configurações de política de impressão Citrix e interage com elas conforme observado na tabela a seguir. As informações fornecidas pressupõem que a configuração da política Universal Print Server está ativada, os componentes do Universal Print Server estão instalados e as configurações de política estão aplicadas.

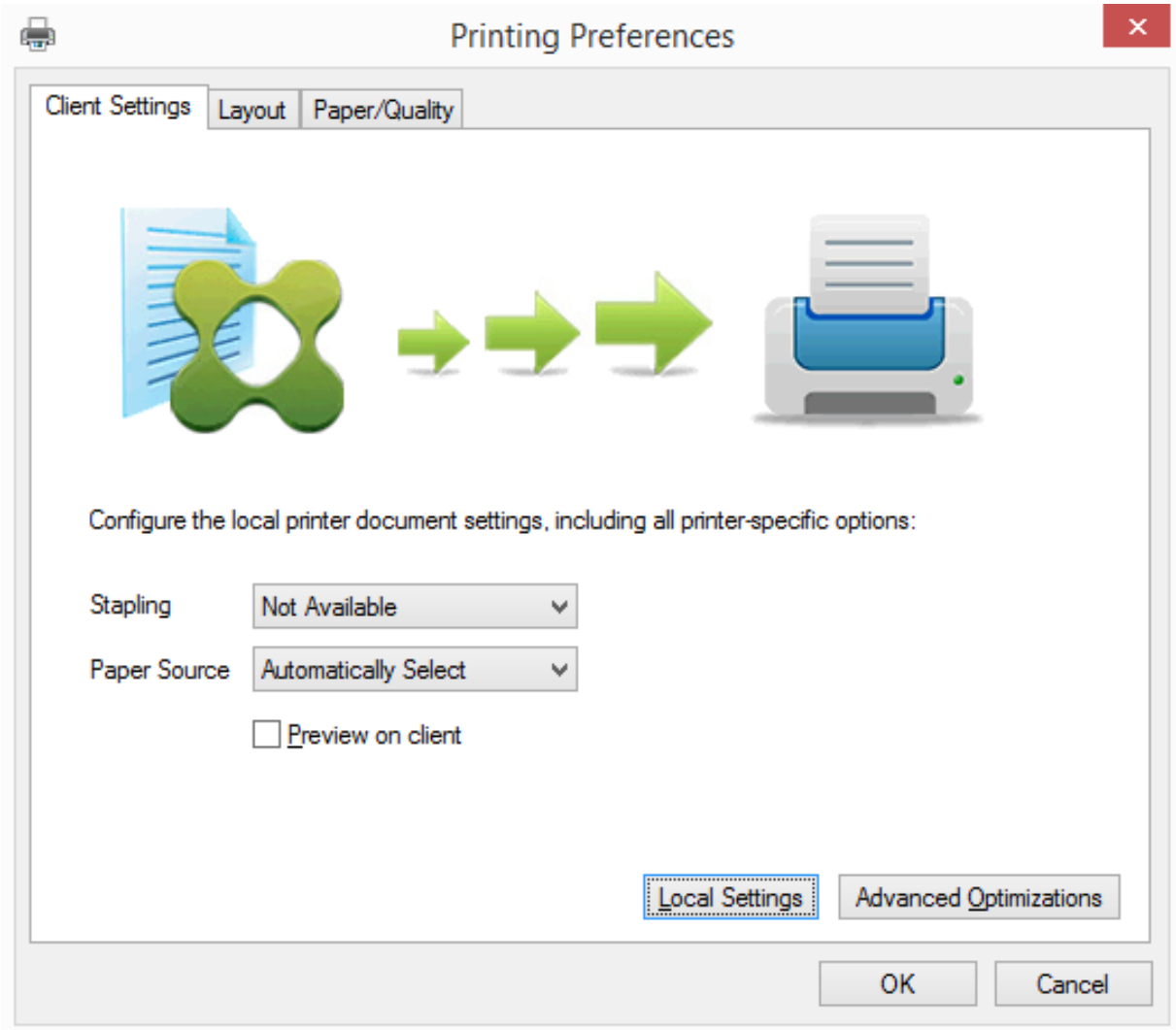
Configuração da política	Interação
Client printer redirection, Auto-create client printers	Depois que o Universal Print Server é ativado, as impressoras de rede cliente são criadas usando o driver de impressão universal em vez dos drivers nativos. Os usuários veem o mesmo nome da impressora de antes.
Session printers	Quando você usa a solução Citrix Universal Print Server, as configurações da política do driver de impressão universal são seguidas.

Direct connections to print server	Quando o Universal Print Server está ativado e a configuração de política de uso do driver de impressão universal está configurada para usar apenas impressão universal, uma conexão direta da impressora de rede com o servidor de impressão pode ser criada usando o driver de impressão universal.
UPD preference	Suporta drivers EMF e XPS.

Efeitos nas interfaces do usuário —o driver de impressão Citrix Universal usado pelo Universal Print Server desativa os seguintes controles da interface do usuário:

- Na caixa de diálogo Printer Properties, o botão Local Printer Settings
- Na caixa de diálogo Document Properties, os botões Local Printer Settings e Preview on client

O driver de impressão Citrix Universal (drivers EMF e XPS) suporta recursos avançados de impressão, como grampeamento e origem do papel. O usuário pode selecionar as opções de grampeamento ou origem de papel na caixa de diálogo de impressão UPD personalizada se as impressoras cliente ou de rede mapeadas para o UPD na sessão aceitarem esses recursos.



Para definir configurações de impressora não padrão, como grampeamento e PIN seguro, selecione **Local Settings** na caixa de diálogo de impressão UPD do cliente em qualquer impressora cliente mapeada que usa os drivers Citrix UPD EMF ou XPS. A caixa de diálogo **Printing Preferences** da impressora mapeada é exibida fora da sessão no cliente, permitindo que o usuário altere qualquer opção de impressora, e as configurações modificadas da impressora são usadas na sessão ativa ao imprimir o documento.

Esses recursos estarão 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 palavras-chave não padronizadas forem usadas, os recursos avançados de impressão não estarão disponíveis usando o driver de impressão universal Citrix.

Ao usar o Universal Print Server, o Add Printer Wizard do Citrix Print Provider é o mesmo que o Add Printer Wizard do Windows Print Provider, com as seguintes exceções:

- Ao adicionar uma impressora por nome ou endereço, você pode fornecer um número de porta

HTTP/SOAP para o servidor de impressão. Esse número de porta se torna parte do nome da impressora e aparece em monitores.
- Se a configuração de política de uso do driver de impressão Citrix Universal especificar que a impressão universal deve ser usada, o nome do driver de impressão Universal aparece ao selecionar uma impressora. O Windows Print Provider não pode usar o driver de impressão Universal.

O Citrix Print Provider não oferece suporte à renderização no lado do cliente.

Para obter mais informações sobre o Universal Print Server, consulte CTX200328.

Impressoras cliente criadas automaticamente

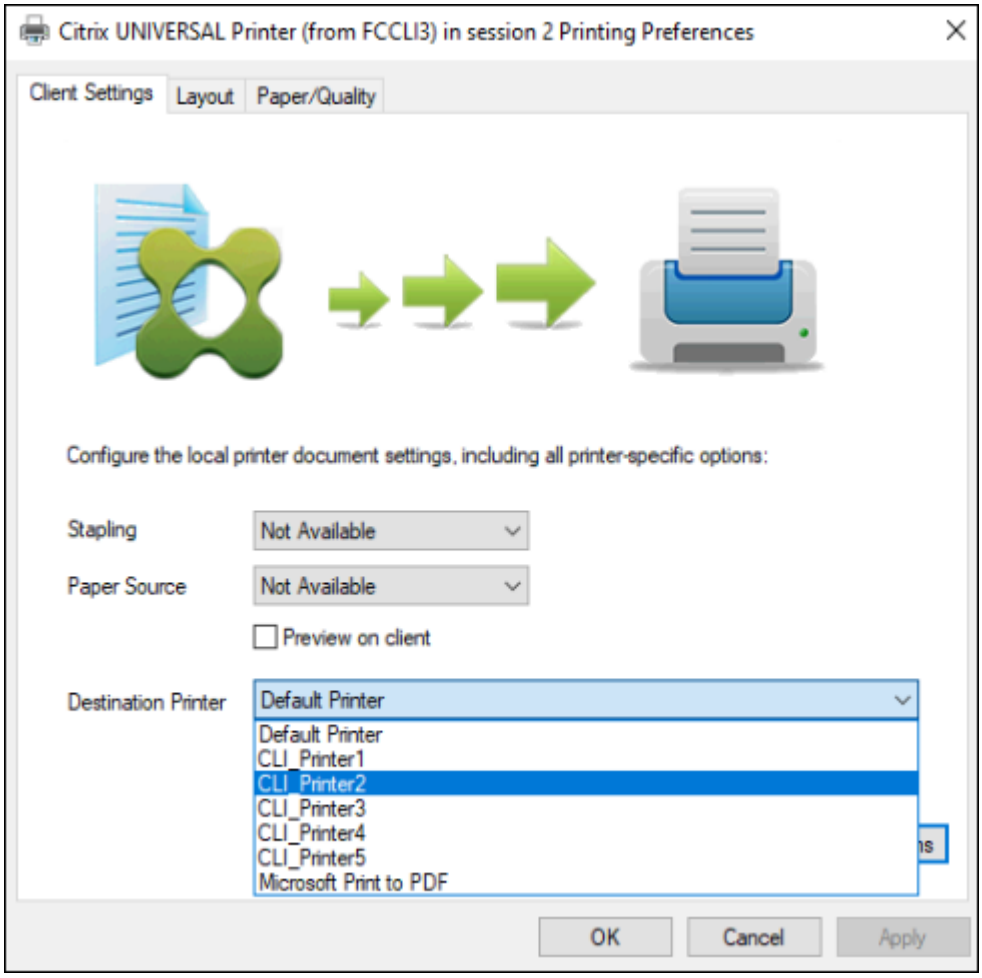
Essas soluções de impressão universal são fornecidas para impressoras cliente:

- **Impressora universal Citrix** —uma impressora genérica criada no início das sessões que não está vinculada a um dispositivo de impressão. Quando você cria automaticamente e usa somente a impressora universal Citrix, você pode notar um uso reduzido de recursos e tempos de login 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 que são transmitidos para o cliente. Considere usar impressoras cliente criadas automaticamente e o driver de impressão Universal nesses ambientes.

  Para usar uma solução de impressão universal para aplicativos Citrix Workspace que não são Windows, use um dos outros drivers de impressão universal baseados em PostScript ou PCL.

  A impressora universal Citrix permite que você selecione a impressora padrão do cliente ou uma impressora cliente específica como o destino da impressão. Para escolher uma impressora específica para um trabalho de impressão, abra a caixa de diálogo **Preferências de impressão**. Selecione o menu suspenso **Impressora de destino**. A opção **Impressora padrão** envia trabalhos de impressão para a impressora padrão do cliente. Todas as impressoras redirecionadas pelo cliente conectadas ao ponto de extremidade que executa a sessão também são listadas. A impressora selecionada é salva como a impressora de destino para qualquer trabalho de impressão futuro.



- **Drivers de impressão universal Citrix** –um driver de impressora independente do dispositivo. Se você configurar um driver de impressão universal Citrix, o sistema usa o driver de impressão universal baseado em EMF por padrão.

  O driver de impressão universal Citrix cria trabalhos de impressão menores do que os drivers de impressora mais antigos ou menos avançados. No entanto, um driver específico ao dispositivo pode ser necessário para otimizar os 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.

- Universal print driver usage. Especifica quando usar a impressão universal.
- Auto-create generic universal printer. Ativa ou desativa a criação automática do objeto genérico Citrix Universal Printer para sessões quando um dispositivo de usuário compatível com Universal Printing estiver em uso. Por padrão, o objeto Universal Printer genérico não é criado automaticamente.

- Universal driver preference. Especifica a ordem em que o sistema tenta usar drivers de impressão universal, começando com a primeira entrada na lista. Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.
- Universal printing preview preference. Especifica se a função de visualização de impressão deve ser usada para impressoras universais genéricas ou criadas automaticamente.
- Universal printing EMF processing mode. Controla o método de processamento do arquivo de spool EMF no dispositivo do usuário Windows. Por padrão, os registros EMF são postos em spool diretamente para a impressora. Colocar em spool diretamente na impressora permite que o spooler processe os registros mais rapidamente e use menos recursos da CPU.

Para obter mais políticas, consulte Otimizar o desempenho de impressão. Para alterar os padrões de configurações como tamanho do papel, qualidade de impressão, cor, frente e verso e número de cópias, consulte CTX113148.

Auto-create printers from the user device –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 são provisionados aos usuários e impedir a autocriação.

Use a configuração de política Citrix
Auto-create client printers to control autocreation. Você pode especificar que:

- Todas as impressoras visíveis para o dispositivo do usuário, incluindo em rede e impressoras conectadas localmente, são criadas automaticamente no início de cada sessão (padrão)
- Todas as impressoras locais fisicamente conectadas ao dispositivo do usuário são criadas automaticamente
- Somente a impressora padrão para o dispositivo do usuário é criada automaticamente
- A autocriação está desativada para todas as impressoras cliente

A configuração Auto-create client printers requer que a configuração Client printer redirection seja Allowed (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 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 as políticas da impressora de sessão por endereço IP para fornecer impressão por proximidade. A impressão por proximidade permite que os usuários dentro de um intervalo de endereços IP especificado acessem automaticamente os dispositivos de impressão de rede que existem dentro desse 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 os endereços IP para os usuários.
- Todos os departamentos dentro da empresa têm intervalos de endereços IP exclusivos designados.
- As impressoras de rede estão presentes dentro do intervalo de endereços IP de cada departamento.

Quando a impressão por proximidade é configurada e um funcionário muda de um departamento para outro, nenhuma configuração adicional do dispositivo de impressão é necessária. Depois 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.

Configure specific printers to be redirected in sessions –para criar impressoras atribuídas pelo administrador, defina a configuração de política 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 \\nomedoservidor\nomedaimpressora.
- Navegue até um local de impressora na rede.
- Procure impressoras em um servidor específico. Digite o nome do servidor usando o formato \\nomedoservidor e clique em Browse.

Importante: o servidor mescla todas as configurações de impressora de sessão ativadas 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 prioridade mais alta no qual a 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 objetos, como as sub-redes.

Specify a default network printer for a session –por padrão, a impressora principal do usuário é usada como a impressora padrão para a sessão. Use a configuração de política Citrix Default printer para alterar a forma como a impressora padrão no dispositivo do usuário é estabelecida em uma sessão.

1. Na página de configurações Default printer, selecione uma configuração para Choose client's default printer:
    - Network printer name. As impressoras adicionadas com a configuração de política Session printers aparecem neste menu. Selecione a impressora de rede a ser usada como padrão para essa política.
    - Do not adjust the user's default printer. Usa a configuração atual do perfil de usuário do Windows ou Serviços de Terminal 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.

Configure proximity printing –a impressão por proximidade também é fornecida pelo Citrix Universal Print Server, a qual não requer a configuração descrita aqui.

1. Crie uma política separada para cada sub-rede (ou para corresponder à localização da impressora).
2. Em cada política, adicione as impressoras na localização geográfica da sub-rede à configuração Session printers.
3. Defina a configuração Default printer como Do not adjust the user's default printer.
4. Filtre as políticas por endereço IP cliente. Certifique-se de atualizar essas políticas para refletir as alterações aos intervalos de endereços IP DHCP.

Manter o ambiente de impressão

June 28, 2023

A manutenção do ambiente de impressão inclui:

- Gerenciamento de drivers de impressora
- Otimização do desempenho de impressão
- Exibição da impressora e gerenciamento de filas de impressão

Gerenciar drivers de impressora

Para minimizar a sobrecarga administrativa e o potencial de problemas do driver de impressão, a Citrix recomenda o uso do driver de impressão universal Citrix.

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 faz o fallback para o driver de impressão universal. Para obter mais informações sobre padrões de driver de impressora, consulte Práticas recomendadas, considerações de segurança e operações padrão.

Se o driver de impressão universal Citrix não for uma opção para todos os cenários, mapeie os drivers da impressora para minimizar a quantidade de drivers instalados em máquinas com SO multissessão Além disso, o mapeamento de drivers de impressora permite que você:

- Permita que impressoras especificadas usem somente o driver de impressão universal Citrix
- Permita ou impeça que impressoras sejam criadas com um driver especificado
- Substitua bons drivers de impressora por drivers desatualizados ou corrompidos
- Substitua um driver que está disponível no servidor Windows por um nome de driver cliente

Impedir a instalação automática de drivers de impressora –a instalação automática de drivers de impressão deve ser desativada para garantir a consistência em máquinas com sistema operacional multissessão. Isso pode ser alcançado por meio de políticas da Citrix, políticas da Microsoft ou das duas. Para evitar a instalação automática de drivers de impressora nativos do Windows, desative a configuração de política Citrix Automatic installation of in-box printer drivers.

Mapear drivers de impressora cliente –cada cliente fornece informações sobre impressoras do lado do cliente durante o logon, incluindo o nome do driver da impressora. Durante a autocriação automática da impressora cliente, os nomes dos drivers da impressora do servidor Windows são selecionados para corresponderem aos nomes dos modelos de impressoras fornecidos pelo cliente. O processo de criação automática usa os drivers de impressora identificados e disponíveis para construir filas de impressão cliente redirecionadas.

Eis aqui 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, defina a configuração da 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 para o driver da impressora cliente no menu Find printer driver. Você pode usar curingas nessa 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 drivers na lista.
4. Para editar as configurações de impressão dos drivers de impressora cliente mapeados, selecione o driver da impressora, clique em Settings e especifique as configurações, como qualidade de impressão, orientação e cor. Se você especificar uma opção de impressão que o driver da impressora não suporta, essa opção não terá efeito. Essa configuração substitui as configurações de impressora retidas que o usuário definiu durante uma sessão anterior.
5. A Citrix recomenda testar o comportamento das impressoras em detalhes após o mapeamento dos drivers, já que algumas funcionalidades de impressora só estão disponíveis com um driver específico.

Quando os usuários fazem logon, o sistema verifica a lista de compatibilidade de drivers da impressora cliente antes de configurar as impressoras cliente.

Otimizar o desempenho de impressão

Para otimizar o desempenho da impressão, use o Universal Print Server e o driver de impressão universal. As políticas a seguir controlam a otimização e a compactação de impressão:

- Universal printing optimization defaults. Especifica as configurações padrão da impressora universal quando ela é criada para uma sessão:
  - A qualidade de imagem desejada especifica o limite de compactação 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 compactação de qualidade padrão ou reduzida.
  - Ativar a compactação intensa ativa ou desativa a redução da largura de banda além do nível de compactação definido pela qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compactação intensa está desativada.
  - As configurações de cache de imagens e fontes especificam se as imagens e fontes que aparecem várias vezes no fluxo de impressão em cache, garantindo que cada imagem ou fonte exclusiva seja enviada para a impressora apenas uma vez. Por padrão, imagens incorporadas e fontes são armazenadas em cache.
  - Allow non-administrators to modify these settings 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.
- Universal printing image compression limit. Define a qualidade máxima e o nível mínimo de compactação disponíveis para imagens impressas com o driver de impressão universal. Por padrão, o limite de compactação de imagem é definido como Best quality (lossless compression).
- Universal printing print quality limit. Define o máximo de pontos por polegada (dpi) disponíveis 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 a partir do computador com SO multissessão, pela rede e diretamente para o servidor de impressão. Considere rotear os trabalhos de impressão pela conexão ICA se a rede tiver latência substancial ou largura de banda limitada. Para fazer isso, desative a configuração de política Citrix Direct connections para os servidores de impressão. Os dados enviados pela conexão ICA são compactados, portanto, é consumida menos largura de banda à medida que os dados viajam pela WAN.

Melhore o desempenho da sessão limitando a largura de banda de impressão –enquanto imprime arquivos de máquinas com SO multissessão para impressoras de usuários, outros canais virtuais (como vídeo) podem sentir um desempenho reduzido devido à concorrência pela 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, pressionamento de teclas e dados do mouse.

> **Importante:**
>
> O limite de largura de banda da impressora é sempre aplicado, mesmo quando nenhum outro canal está em uso.

Use as seguintes configurações de impressora de largura de banda da política Citrix para definir limites de sessão de largura de banda de impressão. Para definir os limites para o site, execute essa tarefa usando o Studio. Para definir os limites para servidores individuais, execute essa tarefa usando o Console de Gerenciamento de Política de Grupo no Windows localmente em cada máquina com SO multissessão.

- A configuração Printer redirection bandwidth limit especifica a largura de banda disponível para impressão em kilobits por segundo (kbps).
- A configuração Printer redirection bandwidth limit percent 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 Printer redirection bandwidth limit percent, ative também Overall session bandwidth limit.

  Se você inserir valores para as duas configurações, a configuração mais restritiva (o valor mais baixo) será aplicada.

Para obter informações em tempo real sobre largura de banda de impressão, use o Citrix Director.

Balancear a carga de servidores de impressão universal

A solução Universal Print Server pode ser dimensionada adicionando-se mais servidores de impressão à solução de balanceamento de carga. Não há um ponto de falha único, 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 for load balancing e Universal Print Servers out-of-service threshold para distribuir a carga de impressão a 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 redistribuirá automaticamente as conexões da impressora alocadas nos servidores de impressão com falha para os outros servidores de impressão disponíveis, de modo que todas as sessões existentes e recebidas funcionem normalmente sem afetar a experiência do usuário e sem exigir a intervenção imediata do administrador.

Os administradores podem monitorar a atividade dos servidores de impressão com carga balanceada usando um conjunto de contadores de desempenho para rastrear o seguinte no VDA:

- Lista de servidores de impressão com carga balanceada no VDA e seu estado (disponível, indisponível)
- Número de conexões de impressora aceitas por cada servidor de impressão
- Número de conexões de impressora com falha em cada servidor de impressão
- Número de conexões de impressora ativas em cada servidor de impressão
- Número de conexões de impressora pendentes em cada servidor de impressão

Exibir e gerenciar filas de impressão

A tabela a seguir resume onde você pode exibir impressoras e gerenciar filas de impressão em seu ambiente.

		Caminho de impressão
Impressoras cliente (impressoras conectadas ao dispositivo do usuário)	Caminho de impressão cliente	UAC Enabled On: snap-in Gerenciamento de Impressão localizado no Console de Gerenciamento Microsoft; UAC Enabled Off: Pré-Windows 8: Painel de Controle, Windows 8: snap-in Gerenciamento de Impressão
Impressoras de rede (impressoras em um servidor de impressão em rede)	Caminho de impressão em rede	UAC Enabled On: Servidor de Impressão > snap-in Gerenciamento de Impressão localizado no Console de Gerenciamento Microsoft; UAC Enabled Off: Servidor de Impressão > Painel de Controle
Impressoras de rede (impressoras em um servidor de impressão em rede)	Caminho de impressão cliente	UAC Enabled On: Servidor de Impressão > snap-in Gerenciamento de Impressão localizado no Console de Gerenciamento Microsoft; UAC Enabled Off: Pré-Windows 8: Painel de Controle, Windows 8: snap-in Gerenciamento de Impressão

		Caminho de impressão
Impressoras de servidor de rede local (impressoras de um servidor de impressão em rede que são adicionadas a uma máquina com SO multissessão)	Caminho de impressão em rede	UAC Enabled On: Servidor de Impressão > Painel de Controle; UAC Enabled Off: Servidor de Impressão > Painel de Controle

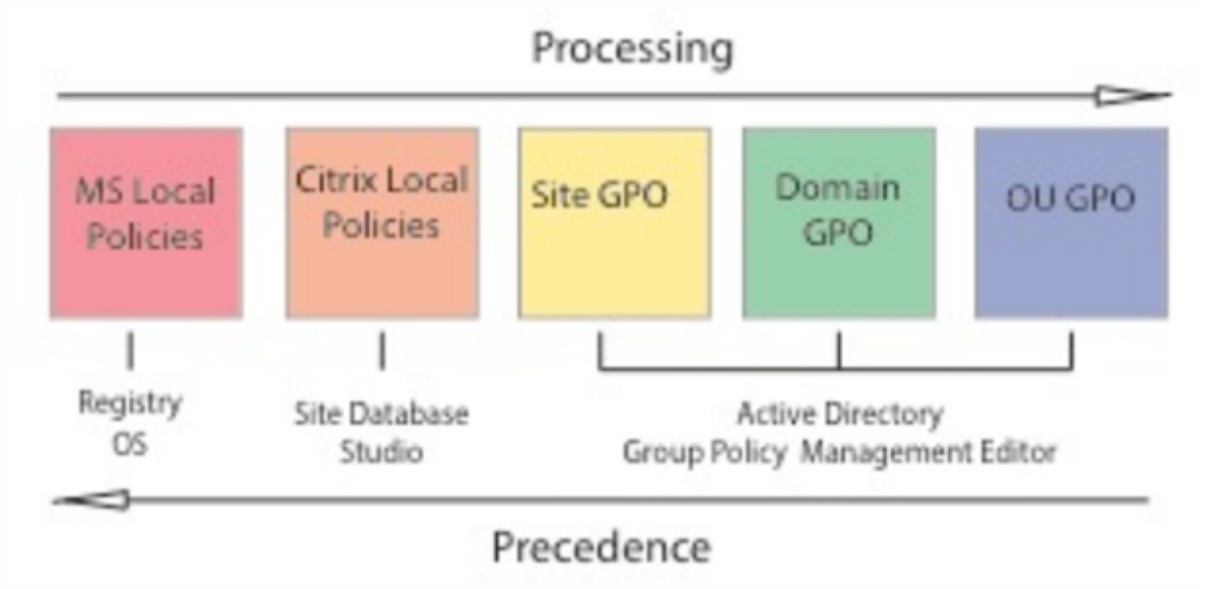
> **Nota:**
>
> As filas de impressão para impressoras de rede que usam o caminho de impressão em rede são privadas e não podem ser gerenciadas através do sistema.

Políticas

June 28, 2023

Políticas são uma coleção de configurações que definem como as sessões, a largura de banda e a segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.

Você pode aplicar configurações de política a máquinas físicas e virtuais ou a usuários. Você pode aplicar configurações a usuários individuais no nível local ou em grupos de segurança no Active Directory. As configurações definem regras e critérios específicos. Se você não atribuir especificamente as políticas, as configurações serão aplicadas a todas as conexões.



Você pode aplicar políticas em diferentes níveis da rede. As configurações da política colocadas no nível do GPO da Unidade Organizacional têm a maior precedência na rede. As políticas no nível do GPO do Domínio substituem as políticas no nível do Objeto de Política de Grupo do Site. O nível do Objeto da Política de Grupo do Site substitui todas as políticas conflitantes nos níveis de Políticas Locais da Microsoft e da Citrix.

Todas as políticas locais da Citrix são criadas e gerenciadas no console Web Studio e armazenadas no banco de dados do site. As políticas de grupo são criadas e gerenciadas usando o Console de Gerenciamento de Política de Grupo (GPMC) da Microsoft e armazenadas no Active Directory. As políticas locais da Microsoft são criadas no sistema operacional Windows e são armazenadas no registro.

O Studio usa um Assistente para Modelagem para ajudar os administradores a comparar os parâmetros de configuração em modelos e políticas para ajudar a eliminar configurações conflitantes e redundantes. Os administradores podem definir GPOs usando o GPMC para definir as configurações. Além disso, aplicá-los a um conjunto alvo de usuários em diferentes níveis da rede.

Esses GPOs são salvos no Active Directory. O acesso ao gerenciamento dessas configurações é restrito para a maior parte do pessoal de TI por questões de segurança.

As configurações são mescladas de acordo com a prioridade e sua condição. Qualquer configuração desativada substitui uma configuração ativada com classificação inferior. As configurações de política não definidas são ignoradas e não substituem as configurações de classificação inferior.

As políticas locais também podem ter conflitos com políticas de grupo no Active Directory, que podem se sobrepor dependendo da situação.

Todas as políticas são processadas na seguinte ordem:

1. O usuário final faz logon em uma máquina usando credenciais de domínio.
2. As credenciais são enviadas para o controlador de domínio.
3. O Active Directory aplica todas as políticas (usuário final, endpoint, unidade organizacional e domínio).
4. O usuário final faz logon no aplicativo Citrix Workspace e acessa um aplicativo ou área de trabalho.
5. As políticas da Citrix e da Microsoft são processadas para o usuário final e o computador que hospeda o recurso.
6. O Active Directory determina a precedência para as configurações da política. Depois elas são aplicadas aos registros do dispositivo endpoint e ao computador que hospeda o recurso.
7. O usuário final faz logoff do recurso. As políticas da Citrix para o usuário final e o dispositivo de endpoint não estão mais ativas.
8. O usuário final faz logoff do dispositivo do usuário, que libera as políticas de usuário do GPO.
9. O usuário final desliga o dispositivo, que libera as políticas do computador do GPO.

Ao criar políticas para grupos de usuários, dispositivos e computadores, alguns membros podem ter

requisitos diferentes, exigindo exceções a algumas configurações da 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 Windows e Citrix no mesmo GPO.

Trabalhar com políticas

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Configurar políticas Citrix para controlar o acesso do usuário e os ambientes de sessão. As políticas da Citrix são o método mais eficiente de controlar as configurações de conexão, segurança e largura de banda. Você pode criar políticas para grupos específicos de usuários, dispositivos ou tipos de conexão. Cada política pode conter várias configurações.

Ferramentas para trabalhar com políticas Citrix

Você pode usar as seguintes ferramentas com políticas Citrix.

- **Web Studio.** Se você for um administrador do Citrix sem permissão para gerenciar a política de grupo, use o Web Studio para criar políticas para o seu site. As políticas criadas usando o Web Studio são armazenadas no banco de dados do site, e as atualizações são enviadas para o VDA quando esse VDA se registra no agente ou quando um usuário se conecta a esse VDA.
- **Editor de política de grupo local** (snap-in do Console de Gerenciamento Microsoft). Se o ambiente de rede usar o Active Directory e você tiver permissão para gerenciar a política de grupo, você poderá usar o editor de política de grupo local para criar políticas para o seu site. As configurações definidas afetam os objetos de política de grupo (GPOs) que você especificar no console de gerenciamento de política de grupo.

> **Importante:**
>
> Recomendamos usar o Editor de Política de Grupo Local para definir algumas configurações de política. Os exemplos incluem configurações relacionadas ao registro de VDAs em um contro-

> lador e configurações relacionadas aos servidores Microsoft App-V.

Ordem e precedência de processamento de políticas

As configurações de política de grupo são processadas na seguinte ordem:

1. GPO local
2. GPO do site do Virtual Apps and Desktops (armazenado no banco de dados do site)
3. GPOs 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 substituirão as configurações processadas anteriormente. A ordem de precedência das configurações de política é a seguinte:

1. Unidades organizacionais
2. GPOs de nível de domínio
3. GPOs no nível do site
4. GPO do site do Virtual Apps and Desktops (armazenado no banco de dados do site)
5. GPO local

Por exemplo, um administrador do Citrix usa o Web Studio para criar uma política (Política A) que permite 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 desativa o redirecionamento do arquivo do cliente para funcionários de vendas. Quando os funcionários de vendas fazem logon nas áreas de trabalho virtuais, a Política B é aplicada e a Política A é ignorada. O motivo é que a Política B foi processada no nível do domínio e a Política A foi processada no nível do GPO do site do Citrix Virtual Apps and Desktops.

No entanto, quando um usuário inicia uma sessão ICA ou RDP (Remote Desktop Protocol), as configurações da sessão Citrix substituem as mesmas configurações configuradas em uma política do Active Directory ou por meio da configuração do host de sessão de área de trabalho remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão do cliente RDP. Os exemplos das configurações de conexão de cliente RDP são papel de parede da área de trabalho, animação do menu e conteúdo da janela de exibição enquanto arrasta.

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. Defina as configurações de política.
3. Atribua a política aos objetos da máquina e do usuário.
4. Priorize a política.
5. Verifique a política efetiva executando o assistente de modelagem de políticas de grupo Citrix.

> **Nota:**
>
> Abra o assistente de Modelagem de Política de Grupo Citrix navegando até a guia **Policies > Modeling** e clicando em **Launch Modeling Wizard** na barra de ações. A guia **Modeling** está disponível no Web Studio por solicitação do cliente.

Navegue pelas políticas e configurações da 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 da Citrix. Consulte a documentação da Microsoft para obter detalhes sobre como navegar e usar este snap-in.

No Web Studio, as configurações de política são classificadas em categorias com base na funcionalidade ou recurso que afetam. Por exemplo, a seção **Profile Management** inclui configurações de política para o Profile Management.

- As configurações do computador (configurações de política aplicáveis a máquinas) definem o comportamento das áreas de trabalho virtuais e são aplicadas quando uma área de trabalho virtual é iniciada. Essas configurações se aplicam mesmo quando não há sessões de usuário ativas na área de trabalho virtual. As configurações do usuário definem a experiência do usuário ao conectar usando o ICA. As políticas de usuário são aplicadas quando um usuário se conecta ou se reconecta usando o ICA. As políticas de usuário não são aplicadas se um usuário se conectar usando o RDP ou fizer logon diretamente ao console.

  Para acessar políticas, configurações ou modelos, selecione **Policies** no painel esquerdo do Web Studio.

  - A guia **Policies** lista todas as políticas. Quando você seleciona uma política, as guias na parte inferior exibem:
    - Overview –lista nome, prioridade, status ativado/desativado e descrição
    - Settings –lista todos de parâmetros configurados

    * Assigned to –lista objetos do usuário e do computador aos quais a política está atribuída.
      Para obter mais informações, consulte Criar políticas.
  - A guia **Templates** lista os modelos personalizados e fornecidos pela Citrix que você criou. Quando você seleciona um modelo, as guias na parte inferior exibem:
    * Description (motivo para você querer usar o modelo)
    * Settings (lista de parâmetros configurados). Para obter mais informações, consulte Modelos de políticas.
  - A guia **Comparison** permite comparar as configurações em uma política ou modelo com as configurações de outras políticas ou modelos. Por exemplo, você pode verificar a definição de valores para garantir a conformidade com as práticas recomendadas. Para obter mais informações, consulte Comparar, priorizar, modelar e solucionar problemas de políticas.

  Para pesquisar uma configuração em uma política ou modelo:

  1. Selecione a política ou o modelo.
  2. Selecione **Edit policy** ou **Edit Template** na barra de ações.
  3. Na página **Settings**, digite o nome da configuração no campo **search**:

     Você pode refinar sua pesquisa selecionando:

     - Uma versão específica do produto
     - Uma categoria (por exemplo, Bandwidth)
     - Palavras-chave no nome da configuração
     - A caixa de seleção **View selected only**
     - Para pesquisar somente as configurações que foram adicionadas à política selecionada.

  Para uma pesquisa não filtrada, selecione **All Settings**.

- Para pesquisar uma configuração dentro de uma política:

  1. Selecione a política.
  2. Selecione a guia **Settings** e digite o nome da configuração.

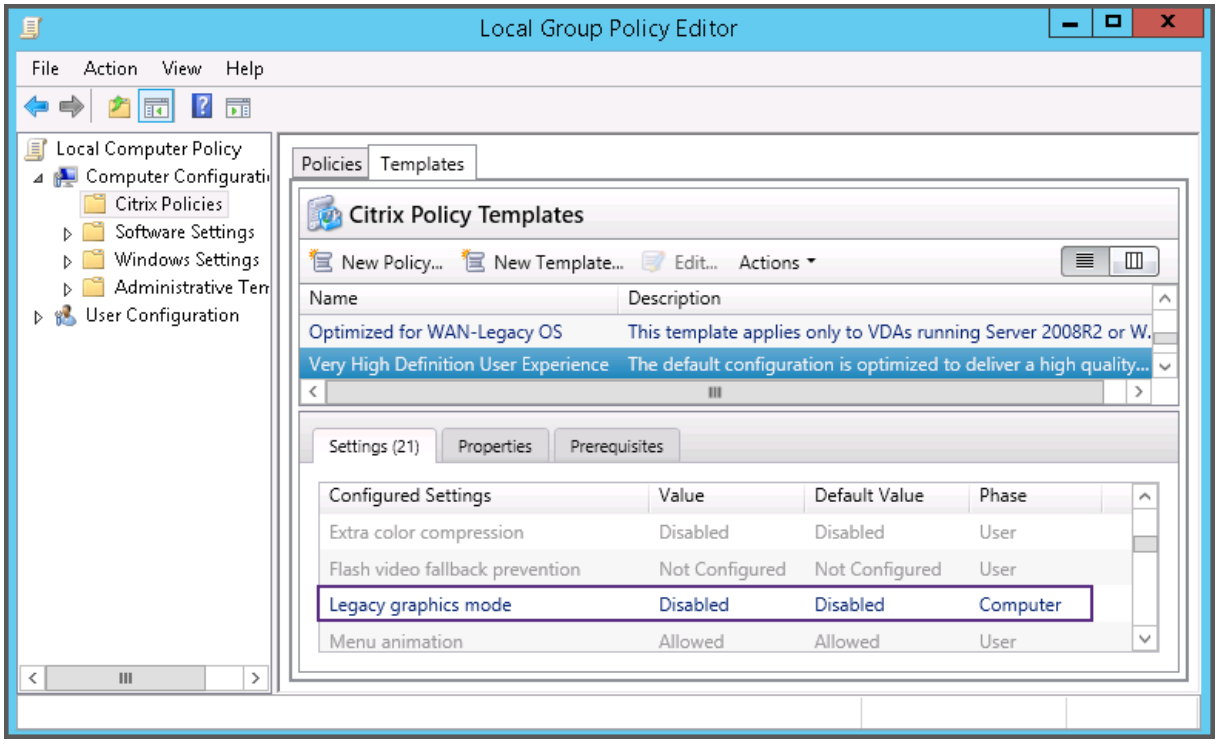
Você pode refinar sua pesquisa selecionando uma versão específica do produto ou selecionando uma categoria. Para uma pesquisa não filtrada, selecione **All Settings**.

Uma política, uma vez criada, é independente do modelo usado. Você pode usar o campo **Description** em uma nova política para rastrear o modelo de origem usado.

No Group Policy Editor, as configurações do computador e do usuário devem ser aplicadas separadamente, mesmo se criadas a partir de um modelo que inclua ambos os tipos de configurações. Neste

exemplo escolhendo usar a experiência do usuário da definição muito alta na configuração do computador:

- O modo gráfico legado é uma configuração de computador que é usada em uma política criada a partir deste modelo.
- As configurações do usuário, em cinza, não são usadas em uma política criada a partir deste modelo.



Modelos de política

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Os modelos são uma fonte para criar políticas a partir de um ponto de partida predefinido. Os modelos Citrix integrados, otimizados para ambientes específicos ou condições de rede, podem ser usados como:

- Uma fonte para criar suas próprias políticas e modelos para compartilhar entre sites.
- Uma referência para facilitar a comparação dos resultados entre implantações, pois você pode citar os resultados, por exemplo, "…ao usar o modelo Citrix x ou y…".
- Um método para comunicar políticas com o suporte da Citrix ou terceiros confiáveis importando ou exportando modelos.

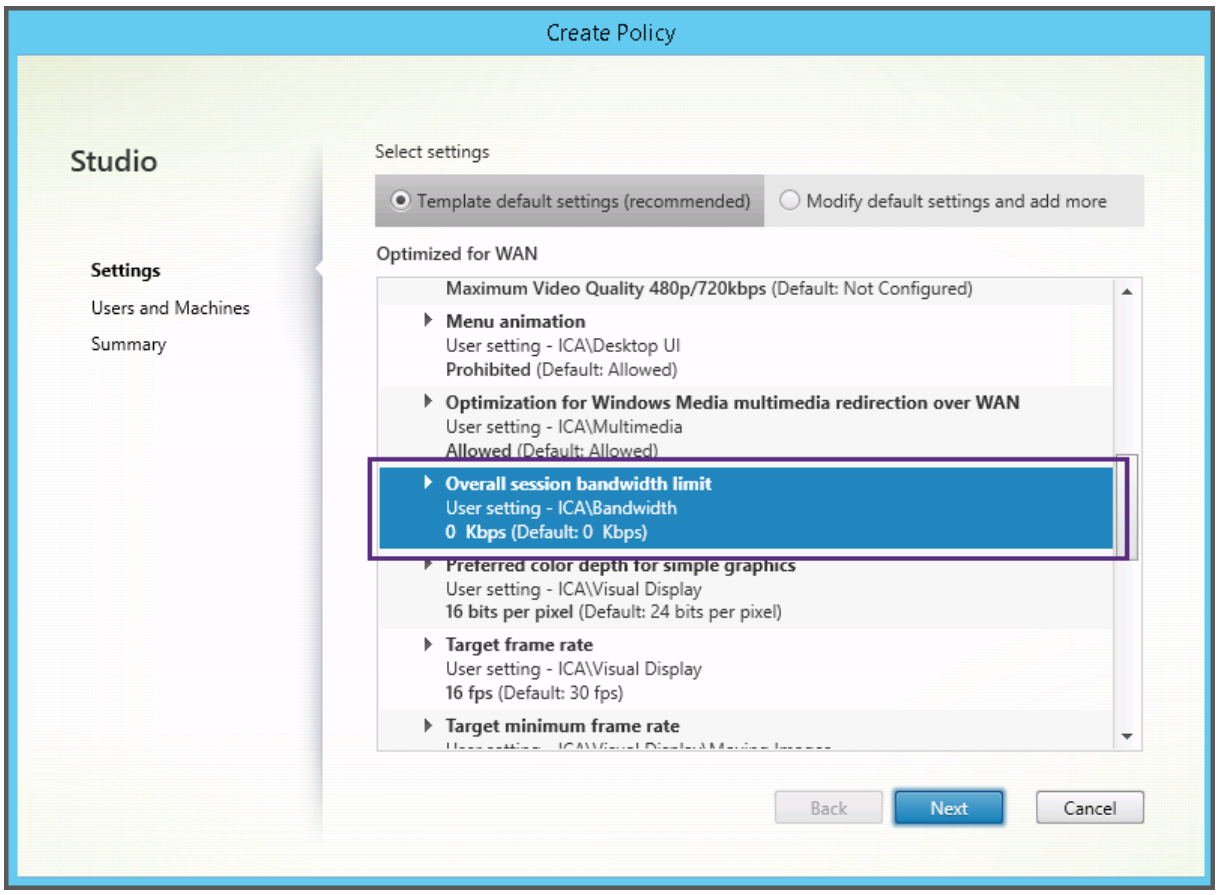
Os modelos de política podem ser importados e exportados.

Modelos Citrix incorporados

Os seguintes modelos de política estão disponíveis:

- **Very High Definition User Experience**. Este modelo impõe as configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde as políticas múltiplas são processadas por ordem de precedência.
- **High Server Scalability**. Aplique este modelo para economizar nos recursos do servidor. Este modelo equilibra a experiência do usuário e a escalabilidade do servidor. Ele oferece uma boa experiência de usuário, aumentando o número de usuários que você pode hospedar em um único servidor. Este modelo não usa um codec de vídeo para compressão de gráficos e impede a renderização multimídia do lado do servidor.
- **High Server Scalability-Legacy OS**. Este modelo de alta escalabilidade do servidor aplica-se apenas aos VDAs com Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo se baseia no modo gráfico legado, que é mais eficiente para os sistemas operacionais.
- **Optimized for NetScaler SD-WAN.** Aplique este modelo para usuários que trabalham em filiais com o NetScaler SD-WAN para otimizar a entrega do Citrix Virtual Desktops. (NetScaler SD-WAN é o novo nome de CloudBridge).
- **Optimized for WAN**. Este modelo destina-se a trabalhadores de tarefas em filiais usando uma conexão WAN compartilhada ou locais remotos com conexões de baixa largura de banda que acessam aplicativos com interfaces de usuário graficamente simples e pouco conteúdo multimídia. Este modelo negocia a experiência de reprodução de vídeo e alguma escalabilidade do servidor para eficiência otimizada da largura de banda.
- **Optimized for WAN-Legacy OS**. Este modelo *Optimized for WAN* aplica-se apenas a VDAs com Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo se baseia no modo gráfico legado, que é mais eficiente para os sistemas operacionais.
- **Security and Control**. Use esse modelo em ambientes com baixa tolerância ao risco, para minimizar os recursos habilitados por padrão no Citrix Virtual Apps and Desktops. Este modelo inclui configurações que desativam o acesso à impressão, área de transferência, dispositivos periféricos, mapeamento de unidade, redirecionamento de porta e aceleração Flash em dispositivos do usuário. A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade do usuário por servidor.

Embora recomendemos usar os modelos Citrix integrados com suas configurações padrão, há configurações que não têm um valor recomendado específico. Por exemplo, **Overall session bandwidth limit**, incluído no otimizado para modelos WAN. Nesse caso, o modelo expõe a configuração para que o administrador entenda que essa configuração provavelmente se aplica ao cenário.



Se você estiver trabalhando com uma implantação (gerenciamento de políticas e VDAs) anterior ao XenApp e XenDesktop 7.6 FP3 e exigir modelos High Server Scalability e Optimized for WAN, use as versões do sistema operacional legado desses modelos quando forem aplicáveis.

> **Nota:**
>
> O Citrix cria e atualiza modelos internos. Não é possível modificar ou excluir esses modelos.

Criar e gerenciar modelos usando o Web Studio

Para criar um modelo baseado em um modelo:

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Policies** e, em seguida, selecione o modelo a partir do qual você criará o modelo.
3. Selecione **Create Template** na barra de ações.

4. Selecione e defina as configurações de política que devem ser incluídas no modelo. Remova as configurações existentes que não sejam pertinentes.
5. Insira um nome para o modelo e clique em **Finish**. O novo modelo é exibido na guia **Templates**.

Para criar um modelo baseado em uma política:

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Policies** e, em seguida, selecione a política a partir da qual você criará o modelo.
3. Selecione **Save as Template** na barra de ações.
4. Selecione e defina quaisquer novas configurações de política a serem incluídas no modelo. Remova as configurações existentes que não sejam pertinentes.
5. Insira um nome e uma descrição para o modelo e clique em **Finish**.

Para importar um modelo:

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Templates** e, em seguida, selecione **Import Template**.
3. Selecione o arquivo de modelo a ser importado e clique em **Open**. Se você importar um modelo com o mesmo nome de um modelo existente, poderá optar por substituir o modelo existente ou salvar o modelo com um nome diferente gerado automaticamente.

Para exportar um modelo:

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Templates** e, em seguida, selecione **Export Template**.
3. Selecione o local onde deseja salvar o modelo e clique em **Save**.

Um `.gpt` arquivo é criado no local especificado.

Criar e gerenciar modelos usando o Group Policy Editor

No Group Policy Editor, expanda Computer Configuration ou User Configuration. Expanda o nó **Policies** e selecione **Citrix Policies**. Escolha a ação apropriada.

Tarefa	Instrução
Criar um modelo a partir de uma política existente	Na guia **Policies**, selecione a política e selecione **Actions > Save as Template**.
Criar uma política a partir de um modelo existente	Na guia **Templates**, selecione o modelo e clique em **New Policy**.
Criar um modelo a partir de um modelo existente	Na guia **Templates**, selecione o modelo e clique em **New Template**.

Tarefa	Instrução
Importar um modelo	Na guia **Templates**, selecione **Actions > Import**.
Exportar um modelo	Na guia **Templates**, selecione **Actions > Export**.
Exibir configurações de modelo	Na guia **Templates**, selecione o modelo e clique na guia **Settings**.
Exibir um resumo das propriedades do modelo	Na guia **Templates**, selecione o modelo e clique na guia **Properties**.
Exibir pré-requisitos do modelo	Na guia **Templates**, selecione o modelo e clique na guia **Prerequisites**.

Modelos e administração delegada

Os modelos de política são armazenados na máquina em que o pacote de gerenciamento de políticas foi instalado. Essa máquina é a máquina do Delivery Controller ou a máquina de gerenciamento de objetos de política de grupo - não o banco de dados Citrix Virtual Apps and Desktops do site. Isso significa que as permissões administrativas do Windows controlam os arquivos de modelo de política em vez de 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 só são visíveis na conta de usuário que os cria e armazenados no perfil do Windows do usuário. Para expor ainda mais um modelo personalizado, crie uma política a partir dele ou exporte-o para um local compartilhado.

Criar políticas

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Antes de criar uma política, decida qual grupo de usuários ou dispositivos ela poderá afetar. Você poderá criar uma política que é baseada na função de trabalho do usuário, tipo de conexão, dispositivo do usuário ou localização geográfica. Você também pode usar os mesmos critérios que usa para 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 política. Depois de editar a política, defina as configurações apropriadas. Evite criar uma política exclusivamente para habilitar uma configuração específica ou para excluir a política da aplicação a determinados usuários.

Ao criar uma política, você pode baseá-la nas configurações em um modelo de política e personalizar as configurações conforme necessário. Você também pode criá-la sem usar um modelo e adicionar todas as configurações necessárias.

No Web Studio, as novas políticas criadas são definidas como desativadas, a menos que a caixa de seleção **Enable policy** esteja explicitamente marcada.

Configurações de política

As configurações de política podem estar ativadas, desativadas ou não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que elas não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

Algumas configurações de política podem estar em um dos seguintes estados:

- Allowed ou Prohibited 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 do menu estiver definida como Allowed, os usuários poderão controlar animações de menu em seu ambiente cliente.
- Enabled ou Disabled ativa ou desativa a configuração. Se você desabilitar uma configuração, ela não será habilitada em políticas de classificação inferior.

Além disso, algumas configurações controlam a eficácia das configurações dependentes. Por exemplo, o redirecionamento da unidade cliente controla se os usuários têm permissão para acessar as unidades nos respectivos dispositivos. Essa configuração e a configuração **Client network drives** devem ser adicionadas à política para permitir que os usuários acessem suas unidades de rede. Se a configuração de **Client drive redirection** estiver desativada, os usuários não poderão acessar suas unidades de rede, mesmo que a configuração de **Client network drives** esteja ativada.

Em geral, as alterações de configuração de política que afetam as máquinas entram em vigor quando a área de trabalho virtual é reiniciada ou quando um usuário faz logon. Alterações de configuração de política que afetam os usuários entram em vigor na próxima vez que os usuários efetuarem logon. 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 do parâmetro selecionando Use default value. Essa seleção desativa a configuração do parâmetro e permite que somente o valor padrão da configuração seja usado quando a política é aplicada. Essa seleção é independente do valor que foi inserido antes de selecionar Use default value.

Práticas recomendadas:

- Atribua políticas a grupos em vez de a usuários separadamente. Se você atribuir políticas a grupos, as atribuições serão atualizadas automaticamente quando você adicionar ou remover usuários do grupo.
- Não ative configurações conflitantes ou sobrepostas na Remote Desktop Session Host Configuration. Às vezes, a Remote Desktop Session Host Configuration oferece funcionalidade semelhante às configurações da política Citrix. Quando possível, mantenha todas as configurações iguais (habilitadas ou desativadas) para facilitar a solução de problemas.
- Desabilite políticas não utilizadas. Políticas sem configurações adicionadas criam processamento desnecessário.

Atribuições de política

Ao criar uma política, você a atribui a determinados usuários e objetos de máquina. Essa política é aplicada às conexões de acordo com critérios ou regras específicas. Em geral, você pode adicionar quantas atribuições quiser a uma política, com base em uma combinação de critérios.

Se você não especificar nenhuma atribuição, ou especificar atribuições, mas desativá-las, a política será aplicada a **todas** as conexões.

> **Nota:**
>
> As atribuições de política também são conhecidas como filtros de política. Para obter informações adicionais, consulte os seguintes tópicos:
>
> - Create, modify, or delete a filter for a policy
> - How do filters get applied?

A tabela a seguir lista as atribuições disponíveis:

Nome da atribuição	Aplica uma política baseada em
Controle de acesso	Condições de controle de acesso através das quais um cliente está se conectando. *Connection type* - se deve aplicar a política a conexões feitas com ou sem NetScaler Gateway. *NetScaler Gateway farm name* - Nome do servidor virtual NetScaler Gateway. *Access condition* - Nome da política de análise de ponto de extremidade ou política de sessão que deve ser usada.
NetScaler SD-WAN	Se uma sessão de usuário é iniciada por meio do NetScaler SD-WAN. **Observação:** você pode adicionar somente uma atribuição do NetScaler SD-WAN a uma política.
Endereço IP do cliente	Endereço IP do dispositivo do usuário usado para se conectar à sessão: exemplos IPv4:12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; exemplos IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nome do cliente	Nome do dispositivo do usuário. Correspondência exata: ClientABCName. Usando curinga: Client*Name.
Grupo de entrega	Associação do Grupo de Entrega.
Tipo de grupo de entrega	Tipo de área de trabalho ou aplicativo: área de trabalho privada, área de trabalho compartilhada, aplicativo privado ou aplicativo compartilhado. **Observação:** as opções de filtro de desktop privado e área de trabalho compartilhada estão disponíveis apenas para o Citrix Virtual Apps and Desktops 7.x. Para obter mais informações, consulte CTX219153.
Unidade Organizacional (UO)	Unidade organizacional.
Marca	Marcas. **Nota:** Aplique esta política a todos os computadores com marcas. As marcas de aplicativo não estão incluídas.
Usuário ou Grupo	Nome do usuário ou do grupo.

Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas em ordem de prioridade e várias instâncias de todas as configurações são comparadas. Cada configuração é aplicada de acordo com a ordem de prioridades da política. Qualquer configuração de política desabilitada tem precedência sobre uma configuração de classificação inferior que esteja ativada. As configurações de política que não estão configuradas são ignoradas.

> **Importante:**
>
> Ao configurar as políticas do Active Directory e do Citrix usando o console de gerenciamento de política de grupo, as atribuições e as configurações podem não ser aplicadas conforme esperado. Para obter mais informações, consulte CTX127461

É fornecida uma política chamada "Unfiltered"por padrão.

- Se você usar o Web Studio para gerenciar políticas Citrix, as configurações adicionadas à política Unfiltered serão aplicadas a todos os servidores, áreas de trabalho e conexões em um site.
- Se você usar o Local Group Policy Editor para gerenciar políticas da Citrix, as configurações adicionadas à política Unfiltered serão aplicadas a todos os sites e conexões. Os sites e as conexões devem estar dentro do escopo dos objetos de política de grupo (GPO) que inclui a política. Por exemplo, a unidade organizacional (UO) de vendas contém um GPO chamado Vendas-EUA que inclui todos os membros da equipe de vendas dos Estados Unidos. O GPO Vendas-EUA é configurado com uma política Unfiltered que inclui várias configurações de política de usuário. Quando o gerente de vendas dos Estados Unidos faz logon no Site, as configurações na política Unfiltered são aplicadas automaticamente à sessão. Essa configuração ocorre porque o usuário é membro do GPO Vendas-EUA.

O modo de uma atribuição determina se a política é aplicada apenas a conexões que correspondem a todos os critérios de atribuição. Se o modo estiver definido como Allow (o padrão), a política será aplicada apenas a conexões que correspondam aos critérios de atribuição. Se o modo estiver definido como Deny, a política será aplicada se a conexão não corresponder aos critérios de atribuição. Os exemplos a seguir ilustram como os modos de atribuição afetam as políticas Citrix quando várias atribuições estão presentes.

- **Exemplo: Atribuições de tipo semelhante com modos diferentes** - Em políticas com duas atribuições do mesmo tipo, uma configurada como Allow (Permitir) e uma como Deny (Negar), a atribuição definida como Deny tem precedência, desde que a conexão satisfaça ambas as atribuições. Por exemplo:

  A política 1 inclui as seguintes atribuições:

  - Atribuição A especifica o grupo Vendas. O modo é definido como Allow.
  - Atribuição B especifica a conta do gerente de vendas. O modo é definido como Deny.

Como o modo de Atribuição B está definido como Deny, a política não é aplicada quando o gerente de vendas faz logon no site, mesmo que o usuário seja membro do grupo Vendas.

- **Exemplo: Atribuições de diferentes tipos com modos semelhantes** - Em políticas com duas ou mais atribuições de diferentes tipos, definidas como Allow, a conexão deve satisfazer pelo menos uma atribuição de cada tipo para que a política seja aplicada. Por exemplo:

  A política 2 inclui as seguintes atribuições:

  - Atribuição C é uma atribuição de usuário que especifica o grupo Vendas. O modo é definido como Allow.
  - A atribuição D é uma atribuição de endereço IP do cliente que especifica 10.8.169.* (a rede corporativa). O modo é definido como Allow.

  Quando o gerente de vendas faz logon no Site a partir do escritório, a política é aplicada porque a conexão satisfaz ambas as atribuições.

  A política 3 inclui as seguintes atribuições:

  - Atribuição E é uma atribuição de usuário que especifica o grupo Vendas. O modo é definido como Allow.
  - Atribuição F é uma atribuição de controle de acesso que especifica as condições de conexão NetScaler Gateway. O modo é definido como Allow.

  Quando o gerente de vendas faz logon no Site a partir do escritório, a política não é aplicada porque a conexão não satisfaz a Atribuição F.

Criar uma política com base em um modelo por meio do Web Studio

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Templates** e selecione um modelo.
3. Selecione **Create Policy from Template** na barra de ações.
4. Por padrão, a nova política usa todas as configurações padrão no modelo. Nesse caso, a opção **Template default settings (recommended)** é selecionada. Se desejar alterar as configurações, selecione **Modify default settings and add more** e, em seguida, adicione ou remova configurações.
5. Especifique como aplicar a política selecionando uma das seguintes opções:

   - **Selected user and machine objects**. Para aplicar a política aos objetos selecionados do usuário e do computador, depois clique em **Assign** para selecionar os objetos do usuário e do computador aos quais a política deve ser aplicada.

- **All objects in the site**. Para aplicar a política a todos os objetos do usuário e do computador no site.

6. Digite um nome para a política. Dê o nome à 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 desativada por padrão; você pode ativá-la. A ativação da política permite que ela seja aplicada imediatamente aos usuários que fazem logon. A desativação impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, é conveniente desabilitar a política até o momento de aplicá-la.

Criar uma política usando o Web Studio

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Selecione a guia **Policies**.
3. Selecione **Create Policy** na barra de ações.
4. Adicione e configure as configurações da política.
5. Especifique como aplicar a política escolhendo uma das seguintes opções:

   - Atribua aos objetos selecionados do usuário e do computador e selecione os objetos do usuário e do computador 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 computador no site.

6. Insira um nome para a política ou aceite o padrão. Dê o nome à 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 ativada por padrão; você pode desativá-la. A ativação da política permite que ela seja aplicada imediatamente aos usuários que fazem logon. A desativação impede que a política seja aplicada. Se você precisar priorizar a política ou adicionar configurações posteriormente, é conveniente desabilitar a política até o momento de aplicá-la.

Criar e gerenciar políticas usando o Group Policy Editor

No Group Policy Editor, expanda **Computer Configuration ou User Configuration**. Expanda o nó **Policies** e selecione **Citrix Policies**. Escolha a ação apropriada:

Tarefa	Instrução
Criar uma política	Na guia **Policies**, clique em **New**.
Editar uma política existente	Na guia **Policies**, selecione a política e clique em **Edit**.
Alterar a prioridade de uma política existente	Na guia **Policies**, selecione a política e clique em **Higher** ou **Lower**.
Exibir informações de resumo sobre uma política	Na guia **Policies**, selecione a política e clique na guia **Summary**.
Exibir e alterar as configurações da política	Na guia **Policies**, selecione a política e clique na guia **Settings**.
Exibir e alterar filtros de política	Na guia **Policies**, selecione a política e clique na guia **Filters**. Quando você adiciona mais de um filtro a uma política, todas as condições do filtro devem ser atendidas para que a política seja aplicada.
Ativar ou desativar uma política	Na guia **Policies**, selecione a política e, em seguida, selecione **Actions > Enable** ou **Actions > Disable**.
Criar uma política a partir de um modelo existente	Na guia **Templates**, selecione o modelo e clique em **New Policy**.

Comparar, priorizar e solucionar problemas de políticas

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Você pode usar várias políticas para personalizar seu ambiente para atender às necessidades dos usuários com base nos respectivos cargos, localizações geográficas ou tipos de conexão. Por exemplo, para maior segurança, crie restrições aos grupos de usuários que interagem regularmente com dados confidenciais.

Você também pode criar uma política que impede que os usuários salvem arquivos confidenciais em suas unidades de cliente locais. No entanto, se alguns usuários no grupo de usuários precisarem acessar suas unidades de disco locais, você poderá criar outra política apenas para esses usuários. Você então 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 eficaz 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 da Citrix interagem com as políticas definidas no seu sistema operacional. Em um ambiente Citrix, as configurações do Citrix substituem as mesmas configurações definidas em uma política do Active Directory ou usando a Configuração do Host de Sessão de Área de Trabalho Remota. Essa configuração inclui configurações relacionadas às configurações típicas de conexão do cliente RDP (Remote Desktop Protocol). 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 no sistema operacional. Se um nível de criptografia de prioridade mais alta for definido em outro lugar, as configurações da **política de ICA segura** que você especificar na política ou quando estiver fornecendo aplicativos e áreas de trabalho poderão ser substituídas.

Por exemplo, as configurações de criptografia especificadas ao criar Grupos de Entrega devem estar no mesmo nível que as configurações de criptografia especificadas em todo o ambiente.

> **Nota:**
>
> No segundo salto em cenários de salto duplo, considere que um VDA com SO de sessão única se conecta ao VDA com SO multissessão. Nesse caso, as políticas da Citrix agem no VDA do SO de sessão única como se esse fosse o dispositivo do usuário. Por exemplo, considere que as políticas estão definidas para armazenar imagens em cache no dispositivo do usuário. Nesse exemplo, as imagens armazenadas em cache para o segundo salto em um cenário de salto duplo são armazenadas em cache na máquina VDA do SO de sessão única.

Comparar políticas e modelos

Você pode comparar as configurações em uma política ou modelo com as configurações de outras políticas ou modelos. Por exemplo, talvez seja necessário verificar a definição de valores para manter

a conformidade com as práticas recomendadas. Você também pode comparar as configurações em uma política ou modelo com as configurações padrão fornecidas pelo Citrix.

1. Faça logon no Web Studio e selecione **Policies** no painel esquerdo.
2. Clique na guia **Comparison** e clique em **Select**.
3. Escolha as políticas ou modelos que devem ser comparados. Para incluir valores padrão na comparação, marque a caixa de seleção **Compare to default settings**.
4. Depois de clicar em **Compare**, as configurações definidas são exibidas em colunas.
5. Para ver todas as configurações, selecione **Show All Settings**. Para retornar à exibição padrão, selecione **Show Common Settings**.

Priorizar políticas

Priorizar políticas permite que você defina 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 todas as configurações são comparadas. Cada configuração é aplicada de acordo com a ordem de prioridades da política.

Priorize as políticas atribuindo a elas números de prioridade diferentes. Por padrão, as políticas novas recebem a prioridade mais baixa. Se as configurações de política entrarem em conflito, uma política com prioridade mais alta (a prioridade número 1 é a mais alta) tem precedência em relação uma política com uma prioridade mais baixa. As configurações são mescladas de acordo com a prioridade e a respectiva condição. Por exemplo, se a configuração está desativada ou ativada. Qualquer configuração desativada se sobrepõe a uma configuração ativada com classificação inferior. As configurações de política que não estão configuradas são ignoradas e não substituem as configurações de classificação inferior.

1. Entre no Web Studio, selecione **Policies** no painel esquerdo e clique na guia **Policies**.
2. Selecione uma política.
3. Selecione **Change Policy Priorities** na barra de ações.
4. Em **Change Policy Priorities**, ajuste as prioridades das políticas usando os ícones correspondentes.
5. Clique em **Save** para salvar as alterações e sair.

Exceções

Quando cria políticas para grupos de usuários, dispositivos de usuário ou computadores, você pode notar que alguns membros do grupo exigem exceções a algumas configurações de política. Você pode criar exceções dos seguintes modos:

- Criando uma política apenas para os membros do grupo que precisam das exceções e, em seguida, classificar a política mais alta do que a política para todo o grupo
- Usando o modo Deny para uma atribuição adicionada à política

Uma atribuição com o modo definido como Deny aplica uma política somente a conexões que não correspondem aos critérios de atribuição. Por exemplo, uma política inclui as seguintes atribuições:

- Atribuição A é uma atribuição de endereço IP dr cliente que especifica o intervalo 208.77.88.*. O modo está definido como Allow.
- Assignment B é uma atribuição de usuário que especifica uma conta de usuário específica. O modo é definido como Deny.

A política 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.

Determine quais políticas se aplicam a uma conexão

Uma conexão pode não responder conforme o esperado porque várias políticas se aplicam. Se uma política de prioridade mais alta se aplicar a uma conexão, ela poderá substituir as configurações configuradas na política original. Você pode calcular o conjunto de políticas resultante e determinar como as configurações finais de política são mescladas para uma conexão.

Você pode calcular o Resultant Set of Policy das seguintes maneiras:

- Use o assistente **Citrix Group Policy Modeling** para simular um cenário de conexão e discernir como as políticas Citrix podem ser aplicadas. Você pode especificar condições para um cenário de conexão, como:
  - Controlador de domínio
  - Usuários
  - Valores de evidência de atribuição de políticas da Citrix
  - Configurações de ambiente simuladas, como conexão de rede lenta

    O relatório que o assistente produz lista as políticas da Citrix que entram em vigor no cenário. Como você se conecta ao Controller como um usuário de domínio, o assistente calcula os resultados usando as configurações de política de site e os objetos de política de grupo (GPOs) do Active Directory.
- Use o **Group Policy Results** para produzir um relatório que descreve as políticas Citrix em vigor para um determinado usuário e controlador. A ferramenta Group Policy Results ajuda a avaliar o estado atual dos GPOs em seu ambiente e gera um relatório. O relatório gerado descreve como esses objetos, incluindo as políticas da Citrix, estão sendo aplicados atualmente a um determinado usuário e controlador.

Você pode iniciar o Citrix Group Policy Modeling Wizard no Web Studio. Ou você pode iniciar a ferramenta Group Policy Results no Console de Gerenciamento de Política de Grupo no Windows.

As configurações da política do site criadas usando o Web Studio não são incluídas no conjunto de políticas resultante nos seguintes casos:

- Se você executa o Citrix Group Policy Modeling Wizard a partir do Console de Gerenciamento de Política de Grupo
- Se você executa a ferramenta Group Policy Results a partir do Console de Gerenciamento de Política de Grupo

Para confirmar que você obteve o conjunto de políticas resultante mais abrangente, a Citrix recomenda iniciar o assistente Citrix Group Policy Modeling no Web Studio, a menos que você crie políticas usando apenas o Console de Gerenciamento de Política de Grupo.

Solucionar problemas de políticas

Usuários, endereços IP e outros objetos atribuídos podem ter várias políticas que se aplicam simultaneamente. Esse cenário pode resultar em conflitos em que uma política pode não se comportar como esperado. Quando você executa o assistente Citrix Group Policy Modeling ou a ferramenta Group Policy Results, você pode descobrir que nenhuma política é aplicada às conexões de usuário. Nesse cenário, as configurações da política não são aplicadas aos usuários que se conectam a seus aplicativos e áreas de trabalho 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.
- As políticas que correspondem à atribuição não têm nenhuma configuração definida.
- As políticas que correspondem à atribuição são desativadas.

Se você quiser aplicar as configurações de política às conexões que atendam aos critérios especificados, verifique se:

- As políticas que você deseja aplicar a essas conexões estão ativadas.
- As políticas que você deseja aplicar têm as configurações apropriadas definidas.

Configurações de política padrão

June 28, 2023

As tabelas a seguir listam as configurações de política, o padrão e as versões do Virtual Delivery Agent (VDA) às quais elas se aplicam.

ICA

Nome	Configuração padrão	VDA
Transporte adaptativo	Off. Usar quando preferir	VDA 7,13-7,15; VDA 7,16 até a atual
Client clipboard redirection	Allowed	Todas as versões de VDA
Client clipboard write allowed formats	Nenhum formato está especificado	VDA 7.6 até a atual
Desktop launches	Prohibited	VDA para o SO multissessão 7 até a atual
ICA listener port number	1494	Todas as versões de VDA
Launching of non-published programs during client connection	Prohibited	VDA para o SO multissessão 7 até a atual
Limit clipboard client to session transfer size	Disabled	VDA 2009
Limit clipboard session to client transfer size	Disabled	VDA 2009
Loss tolerant mode	Allowed	VDA 2003. Nota: o modo de tolerância à perda ainda não está disponível. Essa versão do VDA oferece suporte, quando disponível.
Loss tolerant thresholds	Quando o modo de tolerância a perdas está disponível: perda de pacote: 5%, latência: 300 ms (RTT)	VDA 2003 até a atual
Protocolo Rendezvous	Disabled	Aplica-se apenas a sessões HDX estabelecidas por meio do Citrix Cloud.
Restrict client clipboard write	Prohibited	VDA 7.6 até a atual
Restrict session clipboard write	Prohibited	VDA 7.6 até a atual
Session clipboard write allowed formats	Nenhum formato está especificado	VDA 7.6 até a atual
Tablet mode toggle	Enabled	VDA 7.16 até a atual; para VDA 7.14 e 7.15 LTSR, configure esta configuração usando o registro.

Nome	Configuração padrão	VDA
Lista de permissão de canais virtuais	Enabled	VDA 2109

ICA/Adobe Flash Delivery/Redirecionamento de Flash

Nome	Configuração padrão	VDA
Flash video fallback prevention	Não configurado	VDA 7.6 FP3 até a atual
Flash video fallback prevention error *.swf		VDA 7.6 FP3 até a atual

ICA/Áudio

Nome	Configuração padrão	VDA
Adaptive Audio	Enabled	Aplica-se a sessões de SO de sessão única e sessões de SO multissessão de VDAs usando o Citrix Virtual Apps and Desktops 2109 ou posterior.
Audio over UDP real-time transport	Allowed	Todas as versões de VDA
Audio Plug N Play	Allowed	VDA para o SO multissessão 7 até a atual
Qualidade de áudio	High - áudio de alta definição	Todas as versões de VDA
Client audio redirection	Allowed	Todas as versões de VDA
Client microphone redirection	Allowed	Todas as versões de VDA

Reconexão do cliente ICA/auto

Nome	Configuração padrão	VDA
Auto client reconnect	Allowed	Todas as versões de VDA

Nome	Configuração padrão	VDA
Auto client reconnect authentication	Não requer autenticação	Todas as versões de VDA
Log de reconexão de cliente automático	Não registar no log eventos de reconexão automática	Todas as versões de VDA
Auto client reconnect timeout	120 segundos	VDA 7.13 até a atual
Reconnect UI transparency level	80%	VDA 7.13 até a atual

ICA/largura de banda

Nome	Configuração padrão	VDA
Audio redirection bandwidth limit	0 Kbps	Todas as versões de VDA
Audio redirection bandwidth limit percent	0	Todas as versões de VDA
Client USB device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Client USB device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Clipboard redirection bandwidth limit	0 Kbps	Todas as versões de VDA
Clipboard redirection bandwidth limit percent	0	Todas as versões de VDA
COM port redirection bandwidth limit	0 Kbps	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
COM port redirection bandwidth limit percent	0	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
File redirection bandwidth limit	0 Kbps	Todas as versões de VDA

Nome	Configuração padrão	VDA
File redirection bandwidth limit percent	0	Todas as versões de VDA
HDX MediaStream Multimedia Acceleration bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO 7 multissessão e VDA para SO 7 de sessão única com o VDA atual para o SO de multissessão e o VDA para o SO de sessão única
HDX MediaStream Multimedia Acceleration bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
LPT port redirection bandwidth limit	0 Kbps	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
LPT port redirection bandwidth limit percent	0	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
Overall session bandwidth limit	0 Kbps	Todas as versões de VDA
Printer redirection bandwidth limit	0 Kbps	Todas as versões de VDA
Printer redirection bandwidth limit percent	0	Todas as versões de VDA
TWAIN device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
TWAIN device redirection bandwidth limit percent	0	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Bidirectional content redirection

Nome	Configuração padrão	VDA
Allow bidirectional content redirection	Prohibited	VDA 7.13 até a atual
Allowed URLs to be redirected to client	vazio	VDA 7.13 até a atual
Allowed URLs to be redirected to VDA	vazio	VDA 7.13 até a atual
Client to host (VDA) and client to client bidirectional content redirection		Usar o modelo administrativo do objeto de política de grupo do aplicativo Citrix Workspace

Redirecionamento de conteúdo do navegador/ICA

Nome	Configuração padrão	VDA
Redirecionamento de conteúdo do navegador	Allowed	VDA 7.16 até a atual
Browser content redirection ACL configuration	`https://www.youtube.com/*`	VDA 7.16 até a atual
Suporte a Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador	Prohibited	VDA 2106 até a atual
Browser content redirection proxy configuration	vazio	VDA 7.16 até a atual
Browser content redirection server fetch web proxy authentication	Prohibited	VDA 2012 até a atual

Sensores ICA/cliente

Nome	Configuração padrão	VDA
Allow applications to use the physical location of the client device	Prohibited	VDA 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

IU ICA/Desktop

Nome	Configuração padrão	VDA
Desktop Composition Redirection	Desativado (7.6 FP3 até a atual); Ativado (5.6 a 7.6 FP2)	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Desktop Composition Redirection graphics quality	Médio	VDA 5.6, VDA para SO de sessão única 7 até 7.15
Desktop wallpaper	Allowed	Todas as versões de VDA
Menu animation	Allowed	Todas as versões de VDA
View window contents while dragging	Allowed	Todas as versões de VDA

ICA/End user monitoring

Nome	Configuração padrão	VDA
ICA round trip calculation	Enabled	Todas as versões de VDA
ICA round trip calculation interval	15 segundos	Todas as versões de VDA
ICA round trip calculations for idle connections	Disabled	Todas as versões de VDA

ICA/Enhanced desktop experience

Nome	Configuração padrão	VDA
Enhanced Desktop Experience	Allowed	VDA para o SO multissessão 7 até a atual

Redirecionamento de arquivos de ICA

Nome	Configuração padrão	VDA
Auto connect client drives	Allowed	Todas as versões de VDA
Client drive redirection	Allowed	Todas as versões de VDA
Client fixed drives	Allowed	Todas as versões de VDA
Client floppy drives	Allowed	Todas as versões de VDA
Client network drives	Allowed	Todas as versões de VDA
Client optical drives	Allowed	Todas as versões de VDA
Client removable drives	Allowed	Todas as versões de VDA
Redirecionamento de host para cliente	Disabled	VDA para o SO multissessão 7 até a atual
Preserve client drive letters	Disabled	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Read-only client drive access	Disabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Special folder redirection	Allowed	Somente implantações da interface da Web; VDA para o SO 7 da multissessão até a atual
Use asynchronous writes	Disabled	Todas as versões de VDA

ICA/Gráficos

Nome	Configuração padrão	VDA
Allow visually lossless compression	Disabled	VDA 7.6 até a atual
Display memory limit	65.536 Kb	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Display mode degrade preference	Degrada a profundidade de cor primeiro	Todas as versões de VDA

Nome	Configuração padrão	VDA
Dynamic windows preview	Enabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Indicador de status gráfico	Disabled	VDA 7.16 até a atual
Image caching	Enabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Legacy graphics mode	Disabled	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Maximum allowed color depth	32 bits por pixel	Todas as versões de VDA
Notify user when display mode is degraded	Disabled	VDA para o SO multissessão 7 até a atual
Optimize for 3D graphics workload	Disabled	VDA 7.17 até a atual
Queuing and tossing	Enabled	Todas as versões de VDA
Compartilhamento de tela	Disabled	VDA 2112
Use video codec for compression	Use video codec when preferred	VDA 7.6 FP3 até a atual
Use hardware encoding for video codec	Enabled	VDA 7.11 até a versão atual

ICA/Gráficos/Cache

Nome	Configuração padrão	VDA
Persistent cache threshold	3.000.000 bps	VDA para o SO multissessão 7 até a atual

ICA/Gráficos/Framehawk

Nome	Configuração padrão	VDA
Framehawk display channel	Disabled	VDA 7.6 FP2 até a atual
Framehawk display channel port range	3224,3324	VDA 7.6 FP2 até a atual

ICA/Keep alive

Nome	Configuração padrão	VDA
ICA keep alive timeout	60 segundos	Todas as versões de VDA
ICA keep alives	Não enviar mensagens de keep-alive de ICA	Todas as versões de VDA

ICA/teclado e IME

Nome	Configuração padrão	VDA
Client Keyboard Layout Sync and IME Improvement	Disabled	Aplica-se somente à 1912 LTSR CU2 e versões posteriores.
Enable Unicode Keyboard Layout Mapping	Prohibited	Aplica-se somente à 1912 LTSR CU2 e versões posteriores.
Hide Keyboard Layout Switch Pop-up Message Box	Prohibited	Aplica-se somente à 1912 LTSR CU2 e versões posteriores.

ICA/Acesso a aplicativos locais

Nome	Configuração padrão	VDA
Allow Local App Access	Prohibited	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
URL redirection block list	Nenhum site especificado	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Nome	Configuração padrão	VDA
URL redirection allow list	Nenhum site especificado	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Experiência móvel

Nome	Configuração padrão	VDA
Automatic keyboard display	Prohibited	VDA 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Launch touch-optimized desktop	Allowed	VDA 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual. Esta configuração está desabilitada e não está disponível para máquinas com Windows 10 e Windows Server 2016.
Remote the combo box	Prohibited	VDA 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Multimídia

Nome	Configuração padrão	VDA
HTML5 video redirection	Prohibited	VDA 7.12 até a atual
Limit video quality	Não configurado	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Nome	Configuração padrão	VDA
Microsoft Teams redirection	Allowed	VDA para SO multissessão 1906 até a atual, VDA para o sistema operacional de sessão única 1906 até a atual.
Multimedia conferencing	Allowed	Todas as versões de VDA
Optimization for Windows Media multimedia redirection over WAN	Allowed	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Use GPU for optimizing Windows Media multimedia redirection over WAN	Prohibited	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Windows Media fallback prevention	Não configurado	VDA 7.6 FP3 até a atual
Windows Media client-side content fetching	Allowed	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Redirecionamento do Windows Media	Allowed	Todas as versões de VDA
Windows Media redirection buffer size	5 segundos	VDA 5, 5.5, 5.6 FP1 até a atual
Windows Media redirection buffer size use	Disabled	VDA 5, 5.5, 5.6 FP1 até a atual

Conexões ICA/Multi-stream

Nome	Configuração padrão	VDA
Audio over UDP	Allowed	VDA para o SO multissessão 7 até a atual
Audio UDP port range	16500, 16509	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Multi-Port policy	A porta primária (2598) tem alta prioridade	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Nome	Configuração padrão	VDA
Multi-Stream computer setting	Disabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Multi-Stream user setting	Disabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Multi-Stream virtual channel stream assignment setting	Consulte Configuração de atribuição de canal virtual de multi-stream para obter as atribuições de stream padrão	VDA 2003

Redirecionamento de porta/ICA

Nome	Configuração padrão	VDA
Auto connect client COM ports	Disabled	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
Auto connect client LPT ports	Disabled	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
Client COM port redirection	Prohibited	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro
Client LPT port redirection	Prohibited	Todas as versões de VDA; para VDA 7.0 a 7.8, defina esta configuração usando o registro

ICA/impressão

Nome	Configuração padrão	VDA
Client printer redirection	Allowed	Todas as versões de VDA

Nome	Configuração padrão	VDA
Impressora padrão	Definir a impressora padrão para a impressora principal do cliente	Todas as versões de VDA
Printer assignments	A impressora atual do usuário é usada como a impressora padrão para a sessão	Todas as versões de VDA
Printer auto-creation event log preference	Registrar erros e avisos	Todas as versões de VDA
Session printers	Nenhuma impressora é especificada	Todas as versões de VDA
Wait for printers to be created (desktop)	Disabled	Todas as versões de VDA

Impressoras ICA/impressão/Impressoras cliente

Nome	Configuração padrão	VDA
Auto-create client printers	Criar automaticamente todas as impressoras cliente	Todas as versões de VDA
Auto-create generic universal printer	Disabled	Todas as versões de VDA
Client printer names	Nomes de impressoras padrão	VDA 5.6
Direct connections to print servers	Enabled	Todas as versões de VDA
Printer driver mapping and compatibility	Nenhuma regra é especificada	Todas as versões de VDA
Printer properties retention	Held in profile only if not saved on client	Todas as versões de VDA
Retained and restored client printers	Allowed	VDA 5, 5.5, 5.6 FP1

ICA/Impressão/Drivers

Nome	Configuração padrão	VDA
Automatic installation of in-box printer drivers	Enabled	Todas as versões de VDA
Universal driver preference	EMF; XPS; PCL5c; PCL4; PS	Todas as versões de VDA
Universal print driver usage	Use universal printing only if requested driver is unavailable	Todas as versões de VDA

ICA/impressão/Universal Print Server

Nome	Configuração padrão	VDA
Universal Print Server enable	Disabled	Todas as versões de VDA
Universal Print Server print data stream (CGP) port	7229	Todas as versões de VDA
Universal Print Server print stream input bandwidth limit (kbps)	0	Todas as versões de VDA
Universal Print Server web service (HTTP/SOAP) port	8080	Todas as versões de VDA
Universal Print Servers for load balancing		VDA versões 7.9 até a atual
Universal Print Server out-of-service threshold	180 (segundos)	VDA versões 7.9 até a atual

ICA/impressão/impressão universal

Nome	Configuração padrão	VDA
Universal printing EMF processing mode	Spool directly to printer	Todas as versões de VDA
Universal printing image compression limit	Best quality (lossless compression)	Todas as versões de VDA

Nome	Configuração padrão	VDA
Universal printing optimization defaults	Image Compression: Desired image quality = Standard quality, Enable heavyweight compression = False; Image and Font Caching: Allow caching of embedded images = True; Allow non-administrators to modify these settings = False	Todas as versões de VDA
Universal printing preview preference	Do not use print preview for auto-created or generic universal printers	Todas as versões de VDA
Universal printing print quality limit	No limit	Todas as versões de VDA

ICA/Segurança

Nome	Configuração padrão	VDA
SecureICA minimum encryption level	Basic	VDA para o SO multissessão 7 até a atual

ICA/Limites de servidor

Nome	Configuração padrão	VDA
Server idle timer interval	0 milissegundos	VDA para o SO multissessão 7 até a atual

ICA/Limites de sessão

Nome	Configuração padrão	VDA
Disconnected session timer	Disabled	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual

Nome	Configuração padrão	VDA
Remote PC Access disconnected session timer	Disabled	VDA para SO de sessão única 7 até a atual
Disconnected session timer interval	1.440 minutos	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Session connection timer	Disabled	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Session connection timer interval	1.440 minutos	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Session idle timer	Enabled	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual
Session idle timer interval	1.440 minutos	VDA 5, 5.5, 5,6 FP1, VDA para SO de sessão única 7 até a atual

ICA/Confiabilidade da sessão

Nome	Configuração padrão	VDA
Session reliability connections	Allowed	Todas as versões de VDA
Session reliability port number	2598	Todas as versões de VDA
Session reliability timeout	180 segundos	Todas as versões de VDA

ICA/Controle de Fuso Horário

Nome	Configuração padrão	VDA
Estimate local time for legacy clients	Enabled	VDA para o SO multissessão 7 até a atual
Restore Single-session OS time zone on session disconnect or logoff	Enabled	Versão atual do VDA
Use local time of client	Use server time zone	Todas as versões de VDA

ICA/Dispositivos TWAIN

Nome	Configuração padrão	VDA
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
TWAIN compression level	Médio	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Dispositivos USB

Nome	Configuração padrão	VDA
Client USB device optimization rules	Ativado (VDA 7.6 FP3 até a atual); Desativado (VDA 7.11 até a atual); Por padrão, nenhuma regra é especificada	VDA 7.6 FP3 até a atual
Client USB device redirection	Prohibited	Todas as versões de VDA
Client USB device redirection rules	Nenhuma regra é especificada	Todas as versões de VDA
Client USB Plug and Play device redirection	Allowed	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Exibição ICA/Visual

Nome	Configuração padrão	VDA
Profundidade de cor preferida para gráficos simples	24 bits por pixel	VDA 7.6 FP3 até a atual
Target frame rate	30 fps	Todas as versões de VDA
Visual quality	Médio	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Exibição visual/Imagens em movimento

Nome	Configuração padrão	VDA
Minimum image quality	Normal	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Moving image compression	Enabled	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Progressive compression level	Nenhuma	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Progressive compression threshold value	2.147.483.647 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Target minimum frame rate	10 fps	VDA 5.5, 5.6 FP1, VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

ICA/Exibição visual/Imagens Ainda

Nome	Configuração padrão	VDA
Extra color compression	Disabled	Todas as versões de VDA
Extra color compression threshold	8.192 Kbps	Todas as versões de VDA
Heavyweight compression	Disabled	Todas as versões de VDA
Lossy compression level	Médio	Todas as versões de VDA
Lossy compression threshold value	2.147.483.647 Kbps	Todas as versões de VDA

ICA/WebSockets

Nome	Configuração padrão	VDA
WebSockets connections	Prohibited	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
WebSockets port number	8008	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
WebSockets trusted origin server list	O curinga, *, é usado para confiar em todos os URLs do Prohibited para Web	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Gerenciamento de carga

Nome	Configuração padrão	VDA
Concurrent logon tolerance	2	VDA para o SO multissessão 7 até a atual
Uso de CPU	Disabled	VDA para o SO multissessão 7 até a atual
CPU usage excluded process priority	Abaixo do normal ou Baixo	VDA para o SO multissessão 7 até a atual
Disk usage	Disabled	VDA para o SO multissessão 7 até a atual
Maximum number of sessions	250	VDA para o SO multissessão 7 até a atual
Uso de memória	Disabled	VDA para o SO multissessão 7 até a atual
Memory usage base load	Carga zero: 768 MB	VDA para o SO multissessão 7 até a atual

Profile Management/Configurações avançadas

Nome	Configuração padrão	VDA
Disable automatic configuration	Disabled	Todas as versões de VDA
Log off user if a problem is encountered	Disabled	Todas as versões de VDA
Number of retries when accessing locked files	5	Todas as versões de VDA
Process Internet cookie files on logoff	Disabled	Todas as versões de VDA

Profile Management/Configurações básicas

Nome	Configuração padrão	VDA
Active write back	Disabled	Todas as versões de VDA
Enable Profile Management	Disabled	Todas as versões de VDA
Excluded groups	Disabled. Os membros de todos os grupos de usuários são processados.	Todas as versões de VDA
Offline profile support	Disabled	Todas as versões de VDA
Path to user store	Windows	Todas as versões de VDA
Process logons of local administrators	Disabled	Todas as versões de VDA
Processed groups	Disabled. Os membros de todos os grupos de usuários são processados.	Todas as versões de VDA

Configurações de Profile Management/entre plataformas

Nome	Configuração padrão	VDA
Cross-platform settings user groups	Disabled. Todos os grupos de usuários especificados em Grupos processados são processados	Todas as versões de VDA

Nome	Configuração padrão	VDA
Enable cross-platform settings	Disabled	Todas as versões de VDA
Path to cross-platform definitions	Disabled. Nenhum caminho é especificado.	Todas as versões de VDA
Path to cross-platform settings store	Disabled. Windows\PM_CM é usado.	Todas as versões de VDA
Source for creating cross-platform settings	Disabled	Todas as versões de VDA

Profile Management/Sistema de arquivos/Exclusões

Nome	Configuração padrão	VDA
Exclusion list - directories	Disabled. Todas as pastas no perfil do usuário são sincronizadas.	Todas as versões de VDA
Exclusion list - files	Disabled. Todos os arquivos no perfil do usuário são sincronizados.	Todas as versões de VDA

Profile Management/Sistema de arquivos/Sincronização

Nome	Configuração padrão	VDA
Directories to synchronize	Disabled. Somente pastas não excluídas são sincronizadas.	Todas as versões de VDA
Files to synchronize	Disabled. Somente são sincronizados arquivos não excluídos.	Todas as versões de VDA
Folders to mirror	Disabled. Nenhuma pasta é espelhada.	Todas as versões de VDA

Profile Management/redirecionamento de pastas

Nome	Configuração padrão	VDA
Grant administrator access	Disabled	Todas as versões de VDA
Include domain name	Disabled	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/AppData (Roaming)

Nome	Configuração padrão	VDA
AppData(Roaming) path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for AppData(Roaming)	Os conteúdos são redirecionados para o caminho UNC especificado nas configurações da política de caminho AppData(Roaming)	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Contatos

Nome	Configuração padrão	VDA
Contacts path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Contacts	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Contatos**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Área de Trabalho

Nome	Configuração padrão	VDA
Desktop path	Disabled. Nenhum local é especificado.	Todas as versões de VDA

Nome	Configuração padrão	VDA
Redirection settings for Desktop	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de **política de caminho da área de trabalho**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Documentos

Nome	Configuração padrão	VDA
Documents path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Documents	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de **política de caminho de Documentos**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Downloads

Nome	Configuração padrão	VDA
Downloads path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Downloads	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de **política de caminho de Downloads**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Favoritos

Nome	Configuração padrão	VDA
Favorites path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Favorites	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Favoritos**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Links

Nome	Configuração padrão	VDA
Links path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Links	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Links**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Música

Nome	Configuração padrão	VDA
Music path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Music	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Música**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Imagens

Nome	Configuração padrão	VDA
Pictures path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Pictures	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política de caminho de Imagens**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Jogos salvos

Nome	Configuração padrão	VDA
Saved Games path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Saved Games	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de **política de caminho de Jogos Salvos**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Pesquisas

Nome	Configuração padrão	VDA
Searches path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Searches	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de **política de caminho de Pesquisa**	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Menu Iniciar

Nome	Configuração padrão	VDA
Start Menu path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Start Menu	O conteúdo é redirecionado para o caminho UNC especificado nas configurações de política de caminho do menu Iniciar	Todas as versões de VDA

Profile Management/Redirecionamento de pasta/Vídeo

Nome	Configuração padrão	VDA
Video path	Disabled. Nenhum local é especificado.	Todas as versões de VDA
Redirection settings for Video	O conteúdo é redirecionado para o caminho UNC especificado nas configurações da **política Video path**	Todas as versões de VDA

Profile Management/Configurações de log

Nome	Configuração padrão	VDA
Active Directory actions	Disabled	Todas as versões de VDA
Common information	Disabled	Todas as versões de VDA
Common warnings	Disabled	Todas as versões de VDA
Enable logging	Disabled	Todas as versões de VDA
File system actions	Disabled	Todas as versões de VDA
File system notifications	Disabled	Todas as versões de VDA
Logoff	Disabled	Todas as versões de VDA
Logon	Disabled	Todas as versões de VDA
Maximum size of the log file	1048576	Todas as versões de VDA

Nome	Configuração padrão	VDA
Path to log file	Disabled. Os arquivos de log são salvos no local padrão; %System-Root%\System32\Logfiles\UserProfileManager.	Todas as versões de VDA
Personalized user information	Disabled	Todas as versões de VDA
Policy values at logon and logoff	Disabled	Todas as versões de VDA
Registry actions	Disabled	Todas as versões de VDA
Registry differences at logoff	Disabled	Todas as versões de VDA

Profile Management/Manipulação de perfis

Nome	Configuração padrão	VDA
Delay before deleting cached profiles	0	Todas as versões de VDA
Delete locally cached profiles on logoff	Disabled	Todas as versões de VDA
Local profile conflict handling	Usar perfil local	Todas as versões de VDA
Migration of existing profiles	Local e roaming	Todas as versões de VDA
Path to the template profile	Disabled. 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
Template profile overrides local profile	Disabled	Todas as versões de VDA
Template profile overrides roaming profile	Disabled	Todas as versões de VDA
Template profile used as a Citrix mandatory profile for all logons	Disabled	Todas as versões de VDA

Profile Management/Registro

Nome	Configuração padrão	VDA
Exclusion list	Disabled. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff.	Todas as versões de VDA
Inclusion list	Disabled. Todas as chaves de registro no hive HKCU são processadas quando um usuário faz logoff.	Todas as versões de VDA

Profile Management/Perfis de usuário transmitidos

Nome	Configuração padrão	VDA
Always cache	Disabled	Todas as versões de VDA
Always cache size	0 Mb	Todas as versões de VDA
Profile streaming	Disabled	Todas as versões de VDA
Streamed user profile groups	Disabled. Todos os perfis de usuário dentro de uma OU são processados normalmente.	Todas as versões de VDA
Timeout for pending area lock files (days)	1 dia	Todas as versões de VDA

Citrix Receiver

Nome	Configuração padrão	VDA
StoreFront accounts list	Não são especificados armazenamentos	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual

Camada de personalização de usuário

Nome	Configuração padrão	VDA
User Layer Repository Path	Disabled. Nenhum caminho especificado.	VDA 19.12 e versões posteriores
User Layer Size in GB	10 GB. Uma camada de usuário é um disco com provisionamento fino que se expande para o tamanho definido. As camadas do usuário nunca diminuem de tamanho.	VDA 19.12 ou versões posteriores

Virtual Delivery Agent

Nome	Configuração padrão	VDA
Controller registration IPv6 netmask	Nenhuma máscara de rede especificada	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Controller registration port	80	Todas as versões de VDA
Controller SIDs	Nenhum SID é especificado	Todas as versões de VDA
Controllers	Nenhum controlador é especificado	Todas as versões de VDA
Enable auto update of controllers	Enabled	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Only use IPv6 controller registration	Disabled	VDA para SO multissessão 7 até a atual, VDA para SO de sessão única 7 até a atual
Site GUID	Nenhum GUID é especificado	Todas as versões de VDA

Agente de entrega virtual/HDX 3D Pro

Nome	Configuração padrão	VDA
Enable lossless	Enabled	VDA 5.5, 5.6 FP1

Nome	Configuração padrão	VDA
HDX 3D Pro quality settings		VDA 5.5, 5.6 FP1

Virtual Delivery Agent/Monitoramento

Nome	Configuração padrão	VDA
Enable process monitoring	Disabled	VDA 7.11 até a versão atual
Enable resource monitoring	Enabled	VDA 7.11 até a versão atual

IP virtual

Nome	Configuração padrão	VDA
Virtual IP loopback support	Disabled	VDA 7.6 até a atual
Virtual IP virtual loopback programs list	Nenhuma	VDA 7.6 até a atual

Referência a configurações de política

June 28, 2023

As políticas incluem configurações que são aplicadas quando a política é imposta. As descrições nesta seção também indicam se são necessárias mais configurações para habilitar um recurso ou são semelhantes a uma configuração.

Referência rápida

As tabelas a seguir listam as configurações que você pode definir dentro de uma política. Encontre a tarefa que deseja concluir na coluna da esquerda e, em seguida, localize a configuração correspondente na coluna da direita.

Uma lista completa de todas as configurações de política está disponível no formato .CHM (HTML compilado) e no formato .CSV. Esses arquivos estão disponíveis na pasta `\program files\citrix\grouppolicy` no servidor onde está instalado o corretor (controlador de entrega). Você também pode baixar a versão mais recente das configurações de política clicando aqui.

Áudio

Para esta tarefa	Use esta definição de política
Controlar se deve permitir o uso de vários dispositivos de áudio	Audio Plug N Play
Controlar se deve permitir a entrada de áudio a partir de microfones no dispositivo do usuário	Client microphone redirection
Controlar a qualidade do áudio no dispositivo do usuário	Qualidade de áudio
Controlar o mapeamento de áudio para alto-falantes no dispositivo do usuário	Client audio redirection

Largura de banda para dispositivos do usuário

Para limitar a largura de banda usada para	Use esta definição de política
Mapeamento de áudio do cliente	Audio redirection bandwidth limit or Audio redirection bandwidth limit percent
Cortar e colar usando a área de transferência local	Clipboard redirection bandwidth limit ou Clipboard redirection bandwidth limit percent
Acesso em uma sessão a unidades de cliente locais	File redirection bandwidth limit ou File redirection bandwidth limit percent
Aceleração multimídia HDX MediaStream	HDX MediaStream Multimedia Acceleration bandwidth limit ou HDX MediaStream Multimedia Acceleration bandwidth limit percent
Sessão do cliente	Overall session bandwidth limit
Impressão	Printer redirection bandwidth limit ou Printer redirection bandwidth limit percent
Dispositivos TWAIN (como uma câmera ou scanner)	TWAIN device redirection bandwidth limit or TWAIN device redirection bandwidth limit percent

Para limitar a largura de banda usada para	Use esta definição de política
Dispositivos USB	Client USB device redirection bandwidth limit or Client USB device redirection bandwidth limit percent

Redirecionamento de unidades de cliente e dispositivos de usuário

Para esta tarefa	Use esta definição de política
Controlar se as unidades no dispositivo do usuário são conectadas ou não quando os usuários fazem logon no servidor	Auto connect client drives
Controlar a transferência de dados de corte e colar entre o servidor e a área de transferência local	Client clipboard redirection
Controlar como as unidades são mapeadas a partir do dispositivo do usuário	Client drive redirection
Controlar se os discos rígidos locais dos usuários estão disponíveis em uma sessão	Client fixed drives e Client drive redirection
Controlar se as unidades de disquete locais dos usuários estão disponíveis em uma sessão	Client floppy drives e Client drive redirection
Controlar se as unidades de rede dos usuários estão disponíveis em uma sessão	Client network drives e Client drive redirection
Controlar se as unidades locais de CD, DVD ou Blu-ray dos usuários estão disponíveis em uma sessão	Client optical drives e Client drive redirection
Controlar se as unidades removíveis locais dos usuários estão disponíveis em uma sessão	Client removable drives e Client drive redirection
Controlar se os dispositivos TWAIN dos usuários, como scanners e câmeras, estão disponíveis em uma sessão e controle a compactação de transferências de dados de imagem	Client TWAIN device redirection; TWAIN compression redirection
Controlar se os dispositivos USB estão disponíveis em uma sessão	Client USB device redirection e Client USB device redirection rules
Melhorar a velocidade de gravação e cópia de arquivos para um disco cliente através de uma WAN	Use asynchronous writes

Redirecionamento de conteúdo

Para esta tarefa	Use esta definição de política
Controlar se deve usar o redirecionamento de conteúdo do servidor para o dispositivo do usuário	Redirecionamento de host para cliente

Interface do usuário da área de trabalho

Para esta tarefa	Use esta definição de política
Controle se o papel de parede da área de trabalho é usado ou não nas sessões dos usuários	Desktop wallpaper
Exibir o conteúdo da janela enquanto uma janela é arrastada	View window contents while dragging

Gráficos e multimídia

> **Importante:**
>
> A política do Flash permanece somente 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 VDA não dá suporte ao Flash.

Para esta tarefa	Use esta definição de política
Controlar o número máximo de quadros por segundo enviados para dispositivos de usuário a partir de áreas de trabalho virtuais	Target frame rate
Controlar a qualidade visual das imagens exibidas no dispositivo do usuário	Visual quality
Controlar se os sites podem exibir conteúdo Flash quando acessados em sessões	Flash server-side content fetching URL list; Flash URL compatibility list; configuração de política Flash video fallback prevention; Flash video fallback prevention error *.swf
Compactação de controle de vídeo renderizado pelo servidor	Use video codec for compression; Use hardware encoding for video codec

Para esta tarefa	Use esta definição de política
Controlar a entrega de conteúdo web multimídia HTML5 aos usuários	HTML5 video redirection

Priorizar o tráfego de rede multifluxo

Para esta tarefa	Use esta definição de política
Especificar portas para tráfego ICA em várias conexões e estabelecer prioridades de rede	Multi-Port policy
Ativar suporte para conexões de vários fluxos entre servidores e dispositivos de usuário	Multi-Stream (configurações do computador e do usuário)

Impressão

Para esta tarefa	Use esta definição de política
Controlar a criação de impressoras cliente no dispositivo do usuário	Auto-create client printers and Client printer redirection
Controlar o local onde as propriedades da impressora são armazenadas	Printer properties retention
Controlar se o cliente ou o servidor processam as solicitações de impressão	Direct connections to print servers
Controlar se os usuários podem acessar impressoras conectadas aos seus dispositivos de usuário	Client printer redirection
Controlar a instalação de drivers nativos do Windows ao criar automaticamente impressoras cliente e de rede	Automatic installation of in-box printer drivers
Controlar quando usar o driver da impressora universal	Universal print driver usage
Escolher uma impressora com base em informações de sessão de usuário em roaming	Impressora padrão
Balanceamento de carga e limite de failover definido para servidores de impressão universais	Universal Print Servers for load balancing; Universal Print Servers out-of-service threshold

> **Nota:**
>
> As políticas não podem ser usadas para ativar um protetor de tela em uma área de trabalho ou sessão de aplicativo. Para usuários que necessitam de protetores de tela, o protetor de tela pode ser implementado no dispositivo do usuário.

Configurações de política ICA

September 13, 2023

> **Nota:**
>
> Esta página fornece descrições e valores de configuração compatíveis para as configurações de política do ICA. Para obter mais informações sobre como trabalhar com políticas, consulte a seção Trabalhar com políticas .

Transporte adaptativo

Essa configuração permite ou impede o transporte de dados por EDT como primário e por TCP como fallback.

Por padrão, o transporte adaptativo está habilitado (**Preferred**) e o EDT é usado quando possível, com fallback para o TCP. Você pode alterar sua configuração conforme necessário:

- **Preferred**. O transporte adaptativo por EDT é usado quando possível, com fallback para o TCP.
- **Diagnostic mode**. O EDT é aplicado à força e o fallback para o TCP é desabilitado. Recomendamos essa configuração apenas para a solução de problemas.
- **Off**. O TCP é aplicado à força e EDT é desabilitado.

Para obter mais informações, consulte Transporte adaptativo.

Configuração Drag and Drop

Essa configuração permite ou impede arrastar arquivos entre o cliente e os aplicativos ou áreas de trabalho virtuais. Por padrão, a política de arrastar e soltar está desativada. Você pode ativar essa política, se necessário.

Application launch wait timeout

Essa configuração especifica o valor de tempo limite de espera em milissegundos para que uma sessão aguarde o início do primeiro aplicativo. Se o início do aplicativo exceder esse período de tempo, a sessão termina.

Você pode escolher o tempo padrão (10.000 milissegundos) ou especificar um número em milissegundos.

Client clipboard redirection

Essa configuração permite ou impede que a área de transferência no dispositivo do usuário seja mapeada para a área de transferência no servidor.

Por padrão, o redirecionamento da área de transferência é permitido.

Para evitar a transferência de dados por copiar e colar entre uma sessão e a área de transferência local, selecione **Prohibit**. Os usuários ainda podem copiar e colar dados entre aplicativos em execução em sessões.

Depois de permitir essa configuração, configure a largura de banda máxima permitida que a área de transferência pode consumir em uma conexão de cliente. Use a configuração **Clipboard redirection bandwidth limit** ou **Clipboard redirection bandwidth limit percent**.

Client clipboard write allowed formats

Quando a configuração **Restrict client clipboard write** é **Enabled**, os dados da área de transferência do host não podem ser compartilhados com o ponto de extremidade do cliente. Você pode usar essa configuração para permitir que formatos de dados específicos sejam compartilhados com a área de transferência do endpoint do cliente. Para usar essa configuração, habilite e adicione os formatos específicos que devem ser 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 no XenApp e XenDesktop e Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

O formato HTML é desativado por padrão. Para ativar este recurso:

- Confirme que **Client clipboard redirection** está definida como **Allowed**.
- Confirme que **Restrict client clipboard write** está definida como **Enabled**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja suportado) em **Client clipboard write allowed formats**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos que devem ser registrados no sistema. Os nomes de formato diferenciam maiúsculas e minúsculas.

Essa configuração não se aplica se a política **Client clipboard redirection** for definida como **Prohibited** ou a política **Restrict client clipboard write** for definida como **Disabled**.

> **Nota:**
>
> Ativar o suporte a cópia da área de transferência no formato HTML (CF_HTML) copia todos os scripts da origem do conteúdo copiado para o destino. Verifique se você confia na fonte antes de começar a copiar. Se você copiar conteúdo contendo scripts, eles só estarão ativos se você salvar o arquivo de destino como um arquivo HTML e o executar.

Limit clipboard client to session transfer size

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de um ponto de extremidade cliente para uma sessão virtual durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, ative a configuração **Limit clipboard client to session transfer size**. Em seguida, no campo **Size Limit**, 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 desativada e não há limite para transferências de cliente para sessão.

Limit clipboard session to client transfer size

Essa configuração especifica o tamanho máximo dos dados da área de transferência que um usuário pode transferir de uma sessão virtual para um ponto de extremidade cliente durante uma única operação de copiar e colar.

Para limitar o tamanho da transferência da área de transferência, ative a configuração **Limit clipboard session to client transfer size**. Em seguida, no campo **Size Limit**, 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 desativada e não há limite para transferências de sessão para cliente.

Restrict client clipboard write

Se essa configuração for **Enabled**, os dados da área de transferência do host não poderão ser compartilhados com o ponto de extremidade do cliente. Você pode permitir formatos específicos ativando a configuração **Client clipboard write allowed formats**.

Por padrão, essa configuração é **Disabled**.

Restrict session clipboard write

Quando essa configuração é **Enabled**, os dados da área de transferência do cliente não podem ser compartilhados dentro da sessão do usuário. Você pode permitir formatos específicos ativando a configuração **Session clipboard write allowed formats**.

Por padrão, essa configuração é **Disabled**.

Session clipboard write allowed formats

Quando a configuração **Restrict session clipboard write** é **Enabled**, os dados da área de transferência do cliente não podem ser compartilhados com aplicativos de 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 no XenApp e XenDesktop e Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

O formato HTML é desativado por padrão. Para ativar este recurso:

- Confirme que **Client clipboard redirection** está definida como **Allowed**.

- Confirme que **Restrict session clipboard write** está definida como **Enabled**.
- Adicione uma entrada para **CF_HTML** (e quaisquer outros formatos que você deseja suportado) em **Session clipboard write allowed formats**.

Você pode adicionar mais formatos personalizados. O nome do formato personalizado deve corresponder aos formatos que devem ser registrados no sistema. Os nomes de formato diferenciam maiúsculas e minúsculas.

Essa configuração não se aplica se a política **Client clipboard redirection** for definida como **Prohibited** ou a política **Restrict session clipboard write** for definida como **Disabled**.

> **Nota:**
>
> Ativar o suporte a cópia da área de transferência no formato HTML (CF_HTML) copia todos os scripts da origem do conteúdo copiado para o destino. Verifique se você confia na fonte antes de começar a copiar. Se você copiar conteúdo contendo scripts, eles só estarão ativos se você salvar o arquivo de destino como um arquivo HTML e o executar.

Desktop starts

Essa configuração permite ou impede conexões com uma sessão nesse VDA usando uma conexão ICA por usuários não administrativos em um grupo de usuários de acesso direto VDA.

Por padrão, os usuários não administrativos não podem se conectar a essas sessões.

Essa configuração não afeta usuários não administrativos em um grupo de usuários de acesso direto VDA que estejam usando uma conexão RDP. Esses usuários podem se conectar ao VDA quando a configuração estiver ativada ou desativada. 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 a configuração estiver ativada ou desativada.

FIDO2 redirection

Essa configuração ativa ou desativa o redirecionamento FIDO2. O redirecionamento FIDO2 permite que os usuários aproveitem os componentes FIDO2 do ponto de extremidade local em uma máquina virtual. Os usuários podem autenticar a sessão virtual por meio de chaves de segurança FIDO2 ou biometria integrada em dispositivos com TPM 2.0 e Windows Hello.

Quando essa configuração é **Allowed**, os usuários podem realizar a autenticação FIDO2 usando os recursos do ponto de extremidade local. Por padrão, essa configuração é **Allowed**.

O redirecionamento FIDO2 também pode ser ativado ou desativado em pontos de extremidade do 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:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

ICA listener connection timeout

Essa configuração especifica o tempo máximo de espera para que seja concluída uma conexão por meio o protocolo ICA.

Por padrão, o tempo máximo de espera é 120.000 milissegundos, ou dois minutos.

ICA listener port number

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 0-65535 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 tenha efeito. Se você alterar o número da porta no servidor, também deverá alterá-lo em cada aplicativo ou plug-in Citrix Workspace que se conecte ao servidor.

Teclado e Editor de Método de Entrada (IME)

Esta configuração ativa ou desativa o seguinte:

- Sincronização dinâmica do layout do teclado
- Editor de método de entrada (IME)
- Mapeamento de layout de teclado Unicode
- Ocultar ou exibir a mensagem da caixa de diálogo de notificação de alternância de layout de teclado

1. No Web Studio, selecione **Keyboard and IME**.

2. Selecione **Client keyboard layout synchronization and IME improvement** para controlar os recursos de sincronização de layout de teclado dinâmico e os recursos genérico de Input Method Editor (IME) no VDA. Você pode configurar:

   Disabled - sincronização de layout de teclado dinâmico e cliente genérico Input Method Editor (IME).

   Support dynamic client keyboard layout synchronization - permite a sincronização dinâmica do layout do teclado.

   Support dynamic client keyboard layout synchronization and IME improvement - permite sincronização dinâmica de layout de teclado e Input Method Editor (IME) genérico de cliente.

3. Selecione **Enable Unicode keyboard layout mapping** para ativar ou desativar o mapeamento de teclado Unicode.

4. Selecione **Hide keyboard layout switch pop-up message box** para controlar se deve ou não ser exibida uma mensagem que indica 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 precisam aguardar alguns instantes antes de digitar para evitar a entrada incorreta de caracteres.

Configurações padrão:

- **Client keyboard layout synchronization and IME improvement**
  - Desativado no Windows Server 2016 e no Windows Server 2019.
  - Support dynamic client keyboard layout synchronization and IME improvement no Windows Server 2012 e Windows 2010.
- **Disable Unicode keyboard layout mapping**
- **Show keyboard layout switch pop-up message box**

Esta política substitui as configurações do registro listadas na seção **Description** das configurações de política.

Logoff checker startup delay

Essa configuração especifica a duração para atrasar a inicialização do verificador de logoff. Use esta política para definir o tempo (em segundos) que uma sessão do cliente deve aguardar antes de desconectar a sessão.

Essa configuração também aumenta o tempo necessário para que um usuário faça logoff do servidor.

Loss tolerant mode

> **Importante:**
>
> - O recurso requer, no mínimo, o aplicativo Citrix Workspace 2002 para Windows. Essa versão do VDA oferece suporte, quando disponível.
> - O modo de tolerância a perdas não é suportado no Citrix Gateway ou no Citrix Gateway Service. Esse modo está disponível apenas com conexões diretas.

Esta configuração habilita ou desabilita o modo de tolerância a perdas.

Por padrão, o modo de tolerância a perdas é **Allowed**.

Quando permitido, o modo é incorporado quando a perda e a latência do pacote estão acima de um limite. Você pode definir os limites usando a política Loss-tolerant thresholds.

Para obter mais informações, consulte Limites de tolerância a perdas.

Loss-tolerant thresholds

Quando loss tolerant mode está disponível, essa configuração especifica os limites de métricas de rede nos quais a sessão muda para o modo de tolerância a perdas.

Os limites padrão são:

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

Para obter mais informações, consulte Limites de tolerância a perdas.

Protocolo Rendezvous

Essa configuração altera a forma como as sessões HDX são proxy ao usar o Citrix Gateway Service. Quando ativado, o tráfego HDX não flui mais pelo Citrix Cloud Connector. Em vez disso, o VDA estabelece uma conexão de saída diretamente ao Citrix Gateway Service (aprimorando a escalabilidade do Cloud Connector).

> **Importante:**
>
> Uma alternância de funcionalidades no Citrix Cloud e uma configuração de política HDX controla esse recurso. A alternância do recurso Citrix Cloud é ativada por padrão enquanto a configuração HDX é desativada por padrão. A configuração HDX afeta apenas as sessões HDX estabelecidas por meio do Citrix Gateway Service. Essa configuração não afeta as sessões estabelecidas diretamente entre o cliente e o VDA ou por meio de um Citrix Gateway local.

Para obter informações, consulte Rendezvous protocol.

Rendezvous proxy configuration

Essa configuração permite configurar um proxy explícito para uso com o protocolo Rendezvous. Se estiver usando um proxy transparente, essa configuração não precisará ser ativada.

Por padrão, essa configuração está desativada.

Quando desabilitado, o VDA não roteia o tráfego de saída através de nenhum proxy não transparente ao se tentar estabelecer uma conexão de encontro com o serviço de gateway.

Quando ativado, o VDA tenta estabelecer uma conexão de encontro com o serviço de gateway por meio do proxy definido nesta configuração.

O VDA suporta o uso de proxies HTTP e SOCKS5 para conexões de Rendezvous. Para configurar o VDA para usar um proxy para a conexão Rendezvous, você deve habilitar essa configuração. Além disso, especifique o endereço do proxy ou o caminho para o arquivo PAC. Por exemplo:

- Endereço 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 com suporte para a configuração do proxy com um arquivo PAC. Para obter mais informações sobre o esquema de arquivo PAC para proxies SOCKS5, consulte Proxy configuration.

> **Nota:**
>
> Apenas os proxies SOCKS5 dão suporte ao transporte de dados através do EDT. Para um proxy HTTP, use TCP como o protocolo de transporte para ICA.

Para obter mais informações, consulte Rendezvous protocol.

Início de programas não publicados durante a conexão do cliente

Essa configuração especifica se deseja permitir a inicialização de aplicativos iniciais por meio do RDP no servidor.

Por padrão, não é permitido iniciar aplicativos iniciais através do RDP no servidor.

Tablet mode toggle policy settings

A alternância do modo tablet otimiza a aparência e o comportamento dos aplicativos da loja, dos aplicativos Win32 e do shell do Windows no VDA. Ele faz isso alternando automaticamente a área de trabalho virtual para o modo Tablet ao conectar a partir de dispositivos de formato pequeno, como telefones e tablets, ou qualquer dispositivo ativado por toque.

Se esta política estiver desativada, o VDA está no modo em que o usuário o define e mantém o mesmo modo por toda parte, independentemente do tipo de cliente.

Configurações da política de reconexão automática do cliente

June 28, 2023

A seção **Auto Client Reconnect** contém configurações de política para controlar a reconexão automática de sessões.

Auto client reconnect

Essa configuração permite ou impede a reconexão automática pelo mesmo cliente após uma conexão ter sido interrompida.

Para o Citrix Receiver para Windows 4.7 e posterior e para o aplicativo Citrix Workspace 1808 e posterior, a reconexão automática do cliente usa apenas as configurações de política do Citrix Studio. Atualizações a essas políticas no Studio sincronizam a reconexão automática do cliente do servidor para o cliente. Com versões mais antigas do Citrix Receiver for Windows, para configurar a reconexão automática do cliente, use uma política do Studio e altere o registro ou o arquivo .ica padrão.

Permitir a reconexão automática do cliente permite que os usuários retomem o trabalho onde foram interrompidos quando uma conexão foi interrompida. A reconexão automática detecta conexões quebradas e, em seguida, reconecta os usuários às suas sessões.

Se o cookie do aplicativo Citrix Workspace que contém a chave para o ID da sessão e as credenciais não for usado, a reconexão automática pode resultar no início de uma nova sessão. Ou seja, em vez de se 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 inseridas novamente. Se os usuários se desconectarem intencionalmente, a reconexão automática do cliente não será acionada.

Uma janela de sessão fica acinzentada quando uma reconexão está em andamento. Um temporizador de contagem regressiva exibe o tempo restante antes da sessão ser reconectada. Quando o tempo limites de uma sessão se esgota, ela é desconectada.

Para sessões de aplicativos, quando a reconexão automática é permitida, um temporizador de contagem regressiva aparece na área de notificação. Esse temporizador especifica o tempo restante antes da reconexão da sessão. O aplicativo Citrix Workspace tenta se reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de usuário, quando a reconexão automática é permitida, o aplicativo Citrix Workspace tenta se reconectar à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou se o usuário cancele as tentativas de reconexão. Por padrão, esse período é de dois minutos. Para alterar esse período, edite a política.

Por padrão, a reconexão automática do cliente é permitida. Você pode desativá-la definindo a política como **Prohibited**.

Auto client reconnect authentication

Essa configuração especifica se a autenticação é necessária para reconexões automáticas do cliente.

Quando um usuário faz logon inicialmente, as credenciais são criptografadas, armazenadas na memória e um cookie é criado contendo a chave de criptografia. O cookie é enviado para o aplicativo Citrix Workspace. Quando esta configuração é definida, não são usados cookies. Em vez disso, é exibida uma caixa de diálogo para os usuários que solicita credenciais quando o aplicativo Citrix Workspace tenta se reconectar automaticamente.

Por padrão, a autenticação não é necessária.

Log de reconexão de cliente automático

Essa configuração ativa ou desativa a gravação de reconexões automáticas de cliente no log de eventos.

Quando o registro é ativado, o registro do sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e com falha. Um site não fornece um log combinado de eventos de reconexão para todos os servidores.

Por padrão, o registro em log está desativado.

Auto client reconnect timeout

Por padrão, o tempo limite da reconexão do cliente automático é ajustado a 120 segundos, o valor configurável máximo para um tempo limite da reconexão do cliente automático é 300 segundos. Use essa política para definir o valor do tempo limite.

Reconnect UI transparency level

Essa configuração permite especificar o nível de opacidade aplicado à janela da sessão do XenApp ou do XenDesktop durante o tempo de reconexão da confiabilidade da sessão.

Por padrão, a transparência da interface do usuário de reconexão é definida como 80%.

Configurações de política de áudio

June 28, 2023

A seção **Audio** inclui configurações de política que permitem que os dispositivos do usuário enviem e recebam áudio em sessões sem reduzir o desempenho.

Adaptive Audio

Essa configuração ativa ou desativa o áudio adaptativo. Quando você ativa essa política, as configurações de qualidade de áudio são ajustadas dinamicamente para fornecer a melhor experiência de usuário. Essa configuração se aplica a sessões de SO de sessão única e sessões de SO multissessão de VDAs usando o Citrix Virtual Apps and Desktops 2109 ou posterior.

Quando essa configuração for proibida, a política de qualidade de áudio será aplicada. Para obter mais informações, consulte Qualidade de áudio.

Por padrão, a política de áudio adaptativo está ativada.

Audio over UDP real-time transport

Essa configuração permite ou impede a transmissão e o recebimento de áudio entre o VDA e o dispositivo do usuário através do RTP usando o User Datagram Protocol (UDP). Quando essa configuração é desabilitada, o áudio é enviado e recebido por TCP.

Por padrão, é permitido áudio por UDP.

Audio Plug N Play

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 aos computadores do sistema operacional Windows multissessão.

Qualidade de áudio

Essa configuração especifica o nível de qualidade do som recebido nas sessões do usuário.

Por padrão, a qualidade do som é definida como High - high definition.

Para controlar a qualidade do som, escolha uma das seguintes opções:

- Selecione Low - para conexões de baixa velocidade para conexões de baixa largura de banda. Os sons enviados para o dispositivo do usuário são compactados 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 Medium –otimizado para fala para fornecer aplicativos de protocolo VoIP. Essa configuração fornece aplicativos de mídia em conexões de rede difíceis com linhas inferiores a 512 Kbps, ou congestionamento e perda de pacotes significativos. Este codec oferece tempo de codificação rápido, tornando-o ideal para uso com softphones e aplicativos de comunicações unificadas quando você precisar de processamento de mídia do lado do servidor.

  O áudio enviado para o dispositivo do usuário é compactado até 64 Kbps. Esta compressão resulta em uma redução moderada na qualidade do áudio reproduzido no dispositivo do usuário, mas proporcionando baixa latência e consumindo baixa largura de banda. Se a qualidade do Protocolo Voice over Internet for insatisfatória, verifique se a configuração de política Audio over UDP Real-time Transport está definida como Allowed.

  Agora, o Real-time Transport (RTP) por UDP só é suportado quando esta qualidade de áudio é selecionada. Use essa qualidade de áudio mesmo para fornecer aplicativos de mídia para conexões de rede desafiadoras, como linhas baixas (menos de 512 Kbps). Além disso, quando há congestionamento e perda de pacotes na rede.
- Selecione High - áudio de alta definição para conexões onde a largura de banda é abundante e a qualidade do som é importante. Os clientes podem reproduzir som na 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. Transmitir essa quantidade de dados pode resultar em maior uso da CPU e congestionamento de rede.

A largura de banda é consumida somente enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo de largura de banda será dobrado.

Para especificar a quantidade máxima de largura de banda, configure **Audio redirection bandwidth limit** ou **Audio redirection bandwidth limit percent**.

Client audio redirection

Essa configuração especifica se os aplicativos hospedados no servidor podem reproduzir sons através de um dispositivo de som instalado no dispositivo do usuário. Essa configuração também especifica

se os usuários podem gravar a entrada de áudio.

Por padrão, o redirecionamento de áudio é permitido.

Depois de permitir essa configuração, você pode limitar a largura de banda consumida para reproduzir ou gravar áudio. Limitar a quantidade de largura de banda consumida pelo áudio pode melhorar o desempenho do aplicativo, mas também pode degradar a qualidade do áudio. A largura de banda é consumida somente enquanto o áudio está sendo gravado ou reproduzido. Se ambos ocorrerem ao mesmo tempo, o consumo de largura de banda será dobrado. Para especificar a quantidade máxima de largura de banda, configure **Audio redirection bandwidth limit** ou **Audio redirection bandwidth limit percent**.

Em computadores com SO Windows multissessão, verifique se a configuração **Audio Plug and Play** está ativada para dar suporte a vários dispositivos de áudio.

Importante: proibir o redirecionamento de áudio do cliente desativa toda a funcionalidade de áudio HDX.

Client microphone redirection

Essa configuração ativa ou desativa o redirecionamento do microfone do cliente. Quando ativada, os usuários podem usar microfones para gravar a entrada de áudio em uma sessão.

Por padrão, o redirecionamento do microfone é permitido.

Por segurança, os usuários são alertados quando servidores que não são confiáveis por seus dispositivos tentam acessar microfones. Os usuários podem optar por aceitar ou não aceitar o acesso. Users can disable the alert on Citrix Workspace app.

Em computadores com SO Windows multissessão, verifique se a configuração Audio Plug and Play está ativada para dar suporte a vários dispositivos de áudio.

Se a configuração **Client audio redirection** estiver desativada no dispositivo do usuário, essa regra não terá efeito.

Configurações da política de largura de banda

June 28, 2023

A seção **Bandwidth** inclui configurações de política para evitar problemas de desempenho relacionados ao uso da largura de banda da sessão do cliente.

Importante: usar essas configurações de política com as configurações **Multi-Stream policy** pode produzir resultados inesperados. Se você usar configurações de Multi-Stream em uma política, essas configurações da política do limite da largura de banda não deverão ser incluídas.

Audio redirection bandwidth limit

Essa configuração especifica a largura de banda máxima permitida para reproduzir ou gravar áudio em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Audio redirection bandwidth limit percent**, a configuração mais restritiva (valor mais baixo) será aplicada.

Audio redirection bandwidth limit percent

Essa configuração especifica o limite máximo de largura de banda permitido para reproduzir ou gravar áudio como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Audio redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

Client USB device redirection bandwidth limit

Essa configuração especifica a largura de banda máxima permitida para o redirecionamento de dispositivos USB de e para o cliente. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Client USB device redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Client USB device redirection bandwidth limit percent

Essa 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, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa 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 definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

Clipboard redirection bandwidth limit

Essa configuração especifica a largura de banda máxima permitida para 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, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Clipboard redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Clipboard redirection bandwidth limit percent

Essa configuração especifica a largura de banda máxima permitida para transferência de dados entre uma sessão e a área de transferência local como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Clipboard redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

COM port redirection bandwidth limit

Observação: para o Virtual Delivery Agent 7.0 a 7.8, defina essa configuração por meio do registro; consulte Configurar os parâmetros de redirecionamento de porta LPT e porta COM usando o registro.

Essa 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 essa configuração e um valor para a configuração **COM port redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

COM port redirection bandwidth limit percent

Observação: para o Virtual Delivery Agent 7.0 a 7.8, defina essa configuração por meio do registro; consulte Configurar os parâmetros de redirecionamento de porta LPT e porta COM usando o registro.

Essa configuração especifica a largura de banda máxima permitida para acessar portas COM em uma conexão de cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **COM port redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente

File redirection bandwidth limit

Essa configuração especifica a largura de banda máxima permitida para acessar uma unidade cliente em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **File redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) entrará em vigor.

File redirection bandwidth limit percent

Essa configuração especifica o limite máximo de largura de banda permitido para acessar unidades cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **File redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

HDX MediaStream Multimedia Acceleration bandwidth limit

Essa configuração especifica o limite máximo de largura de banda permitido para fornecer streaming de áudio e vídeo usando a aceleração multimídia HDX MediaStream. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) entrará em vigor.

HDX MediaStream Multimedia Acceleration bandwidth limit percent

Essa configuração especifica a largura de banda máxima permitida para fornecer streaming de áudio e vídeo usando a aceleração multimídia HDX MediaStream como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **HDX MediaStream Multimedia Acceleration bandwidth limit**, a configuração mais restritiva (o valor mais baixo) entrará em vigor.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

LPT port redirection bandwidth limit

Observação: para o Virtual Delivery Agent 7.0 a 7.8, defina essa configuração por meio do registro; consulte Configurar os parâmetros de redirecionamento de porta LPT e porta COM usando o registro.

Essa 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, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **LPT port redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

LPT port redirection bandwidth limit percent

Observação: para o Virtual Delivery Agent 7.0 a 7.8, defina essa configuração por meio do registro; consulte Configurar os parâmetros de redirecionamento de porta LPT e porta COM usando o registro.

Essa 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, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **LPT port redirection bandwidth limit**, a configuração mais restritiva (o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

Overall session bandwidth limit

Essa 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, não é especificado nenhum máximo (zero).

Limitar a quantidade de largura de banda consumida por uma conexão de cliente pode melhorar o desempenho quando outros aplicativos fora da conexão do cliente estão competindo por largura de banda limitada.

Printer redirection bandwidth limit

Essa configuração especifica a largura de banda máxima permitida para acessar impressoras cliente em uma sessão de usuário. A largura de banda máxima permitida é especificada em kilobits por segundo.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Printer redirection bandwidth limit percent**, será aplicada a configuração mais restritiva (o valor mais baixo).

Printer redirection bandwidth limit percent

Essa configuração especifica a largura de banda máxima permitida para acessar impressoras cliente como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **Printer redirection bandwidth limit**, será aplicada a configuração mais restritiva (com o valor mais baixo).

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

TWAIN device redirection bandwidth limit

Essa 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, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **TWAIN device redirection bandwidth limit percent**, a configuração mais restritiva (o valor mais baixo) será aplicada.

TWAIN device redirection bandwidth limit percent

Essa configuração especifica a largura de banda máxima permitida para controlar dispositivos de imagem TWAIN a partir de aplicativos publicados como uma porcentagem da largura de banda total da sessão.

Por padrão, não é especificado nenhum máximo (zero).

Se você inserir um valor para essa configuração e um valor para a configuração **TWAIN device redirection bandwidth limit**, a configuração mais restritiva (com o valor mais baixo) será aplicada.

Se você definir essa configuração, deverá igualmente configurar **Overall session bandwidth limit**, que especifica a quantidade total de largura de banda disponível para sessões do cliente.

Configurações de política de redirecionamento de conteúdo bidirecional

June 28, 2023

A seção **Bidirectional Content Redirection** contém configurações de política para habilitar ou desabilitar o cliente para redirecionamento de URL de cliente para host e de host para cliente.

As políticas do servidor são definidas no Web Studio. As políticas de cliente são definidas a partir do modelo de administração de objeto de política de grupo do aplicativo Citrix Workspace

A Citrix oferece redirecionamento de host para cliente e Acesso de aplicativo local para redirecionamento de 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 essa política como **Allowed** para habilitar o redirecionamento entre o servidor (VDA) e o cliente. A definição padrão é **Prohibited**.

Use a política **URLs permitidos para redirecionar ao Cliente** para configurar a lista de URLs para o redirecionamento do VDA para o cliente.

> **Nota:**
>
> Essa política deve ser definida com a política de **Bidirectional Content Redirection** no cliente para que o redirecionamento seja permitido.

URLs permitidos para redirecionar ao Cliente

Especifica a lista de URLs que devem ser abertas no cliente quando o redirecionamento de conteúdo bidirecional é permitido.

O delimitador é o ponto e vírgula (;). Um asterisco (*) pode ser usado como curinga. Por exemplo:

```
*.xyz.com;https://www.example.com
```

Configurações da política de redirecionamento de conteúdo do navegador

June 28, 2023

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 maneira como o Citrix Virtual Apps and Desktops fornece qualquer conteúdo de navegador da Web (por exemplo, HTML5) aos usuários. Somente a área visível do navegador onde o conteúdo é exibido é redirecionada.

O redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador são recursos independentes. As políticas de redirecionamento de vídeo HTML5 não são necessárias para que esse recurso funcione. No entanto, o Citrix HDX HTML5 Video Redirection Service é usado para o redirecionamento de conteúdo do navegador. Para obter mais informações, consulte Redirecionamento de conteúdo do navegador.

> **Nota:**
>
> As configurações de política disponíveis no Web Studio podem ser substituídas por chaves de

> registro no VDA, mas as chaves de registro são opcionais.

TLS e redirecionamento de conteúdo do navegador

Você pode usar o redirecionamento de conteúdo do navegador para redirecionar sites HTTPS. O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o serviço de redirecionamento de vídeo Citrix HTML5 (WebSocketService.exe) em execução no VDA. Para obter esse redirecionamento e manter a integridade de TLS da página da Web, o serviço de redirecionamento de vídeo HTML5 Citrix HDX gera dois certificados personalizados no repositório de certificados no VDA.

HdxVideo.js usa soquetes Secure Web para se comunicar com o WebSocketService.exe em execução no VDA. Este processo é executado no sistema local, e realiza a terminação SSL e o mapeamento da sessão do usuário.

WebSocketService.exe está ouvindo em 127.0.0.1 na porta 9001.

Redirecionamento de conteúdo do navegador

Por padrão, o aplicativo Citrix Workspace tenta a busca do cliente e a renderização do cliente. Ocorre uma tentativa de renderização do lado do servidor quando a busca do cliente e a renderização do cliente falham. Se você também habilitar a política de configuração do proxy de redirecionamento de conteúdo do navegador, o aplicativo Citrix Workspace tentará somente a busca do servidor e a renderização do cliente.

Por padrão, essa configuração é Allowed.

Configuração de suporte a Autenticação Integrada do Windows para redirecionamento de conteúdo do navegador

O redirecionamento de conteúdo do navegador permite a sobreposição que usa o esquema Negociar para autenticação. Este aprimoramento fornece logon único para um servidor Web configurado com a Autenticação Integrada do Windows (IWA) dentro do mesmo domínio que o VDA.

Quando definida como **Allowed**, a sobreposição de redirecionamento de conteúdo do navegador obtém um ticket Negociar usando as credenciais VDA do usuário. Em seguida, o usuário se autentica no servidor da Web com logon único.

Quando definida como **Prohibited**, a sobreposição de redirecionamento de conteúdo do navegador não solicita um ticket Negociar do VDA. O usuário se autentica em um servidor Web usando um método básico de autenticação. Esse método de autenticação exige que os usuários insiram suas credenciais VDA sempre que acessarem o servidor da Web.

Por padrão, essa configuração é Prohibited.

Configuração de autenticação de proxy web do servidor de redirecionamento de conteúdo do navegador (Browser content redirection server fetch web proxy authentication setting)

Essa configuração roteia o tráfego HTTP que se origina em uma sobreposição através de um proxy da 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 Negociar.

Você deve configurar o redirecionamento de conteúdo do navegador para o modo de busca do servidor no arquivo PAC usando a política de configuração do proxy de redirecionamento de conteúdo do navegador. No script PAC, forneça instruções para distribuir o tráfego de sobreposição através de um proxy da Web downstream. Configure então o proxy da Web downstream para autenticar os usuários VDA através do esquema de autenticação Negociar.

Quando definido como **Allowed**, o proxy da Web responde com um desafio 407 Negotiate, que inclui um cabeçalho **Proxy-Authenticate: Negotiate**. O redirecionamento de conteúdo do navegador 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 da Web.

Quando definido como **Prohibited**, o redirecionamento de conteúdo do navegador proxies todo o tráfego TCP entre a sobreposição e o proxy da Web sem interferir. A sobreposição usa credenciais básicas de autenticação ou quaisquer outras credenciais disponíveis para autenticar no proxy da Web.

Por padrão, essa configuração é Prohibited.

Configurações da política da lista de controle de acesso (ACL) de redirecionamento de conteúdo do navegador (Browser content redirection Access Control List (ACL) policy settings)

Use essa configuração para configurar uma Lista de Controle de Acesso (ACL) de URLs que podem usar o redirecionamento de conteúdo do navegador ou que tenham acesso negado ao redirecionamento de conteúdo do navegador.

URLs autorizados são os URLs na lista de permissões cujo conteúdo é redirecionado para o cliente.

O curinga * é permitido, mas não é permitido dentro do protocolo ou na parte do endereço de domínio da URL. No entanto, a partir do Citrix Virtual Apps and Desktops 7 2206, o curinga * é permitido na parte do endereço do subdomínio da URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Não permitido: `http://*.*.com/`

Você pode obter melhor granularidade especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, somente a página index.html será redirecionada.

Por padrão, essa configuração é definida como `https://www.youtube.com/*`

Para obter mais informações, consulte o artigo do Knowledge Center CTX238236.

Browser content redirection authentication sites

Use essa configuração para configurar uma lista de URLs. Sites redirecionados por meio do redirecionamento de conteúdo do navegador usam a lista para autenticar um usuário. A configuração especifica os URLs para os quais o redirecionamento de conteúdo do navegador permanece ativo (redirecionado) ao navegar para fora de um 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 de autenticação. O administrador usa a política de configuração ACL de redirecionamento de conteúdo do navegador para adicionar `www.xyz.com` à lista de permissão. Em seguida, usa sites de autenticação de redirecionamento de conteúdo do navegador para adicionar `www.xyz.okta.com` à lista de permissão.

Para obter mais informações, consulte o artigo do Knowledge Center CTX238236.

Browser content redirection block list setting

Essa configuração funciona junto com a definição de configuração de ACL de redirecionamento de conteúdo do navegador. Considere que URLs estão presentes na definição de configuração de ACL de redirecionamento de conteúdo do navegador e na definição de configuração da lista de bloqueio. Nesse caso, a configuração da lista de bloqueio tem precedência e o conteúdo do navegador da URL não é redirecionado.

Unauthorized URLs: 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 na 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 melhor granularidade especificando caminhos na URL. Por exemplo, se você especificar `https://www.xyz.com/sports/index.html`, somente index.html estará na lista de bloqueio.

Browser content redirection proxy setting

Essa configuração fornece opções de configuração para configurações de proxy no VDA para redirecionamento de conteúdo do navegador. Se habilitada com um endereço proxy válido e número de porta, URL PAC/WPAD ou configuração Direct/Transparente, o aplicativo Citrix Workspace tentará somente a busca do servidor e a renderização do cliente.

Se estiver desativada ou não configurada e usando um valor padrão, o aplicativo Citrix Workspace tentará a busca do cliente e a renderização do cliente.

Por padrão, essa configuração é Prohibited.

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 de política.

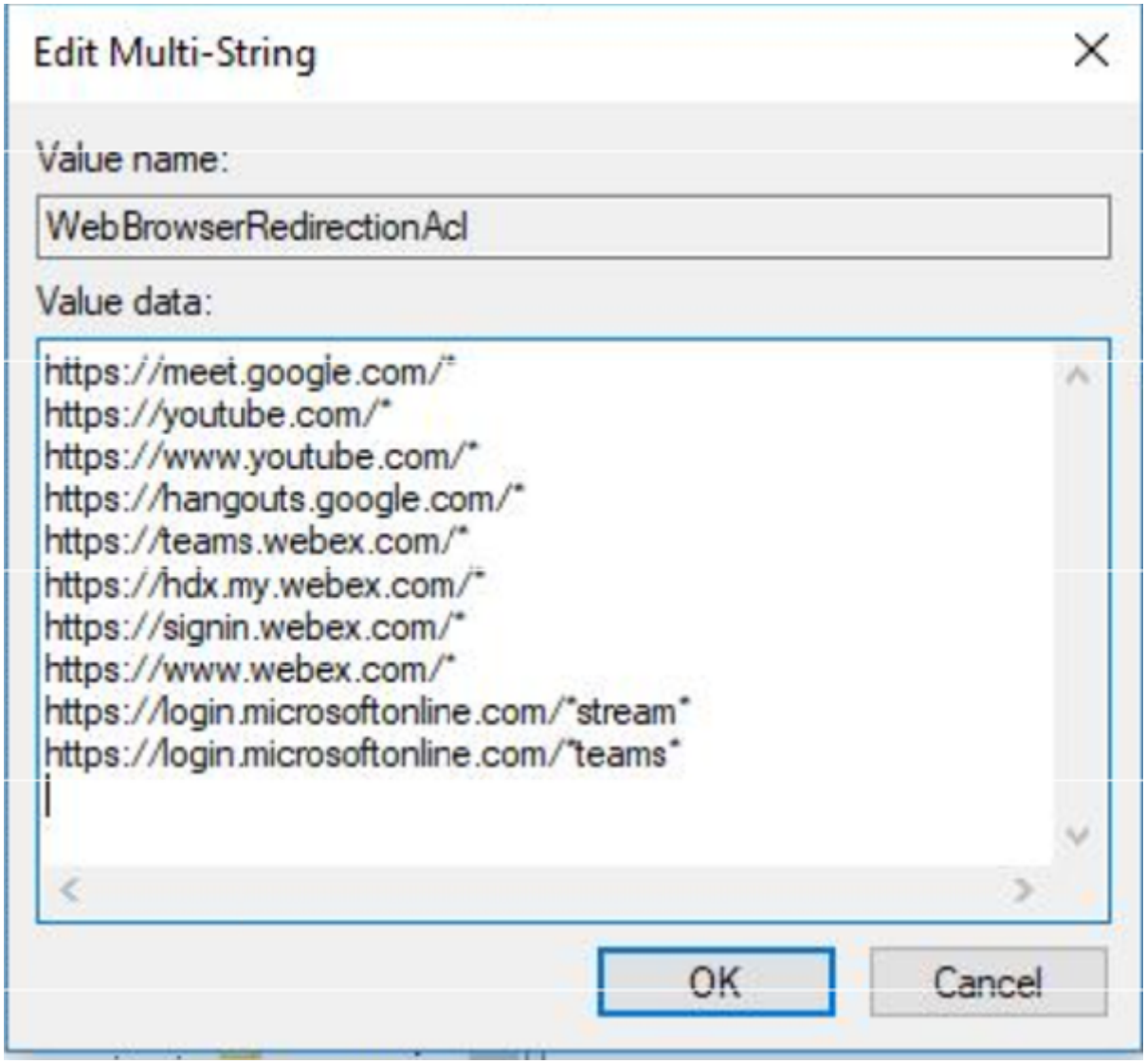
Substituições de chave de registro de redirecionamento de conteúdo do navegador

> **Aviso:**
>
> Editar o registro incorretamente pode causar sérios problemas que podem exigir a reinstalação do sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha

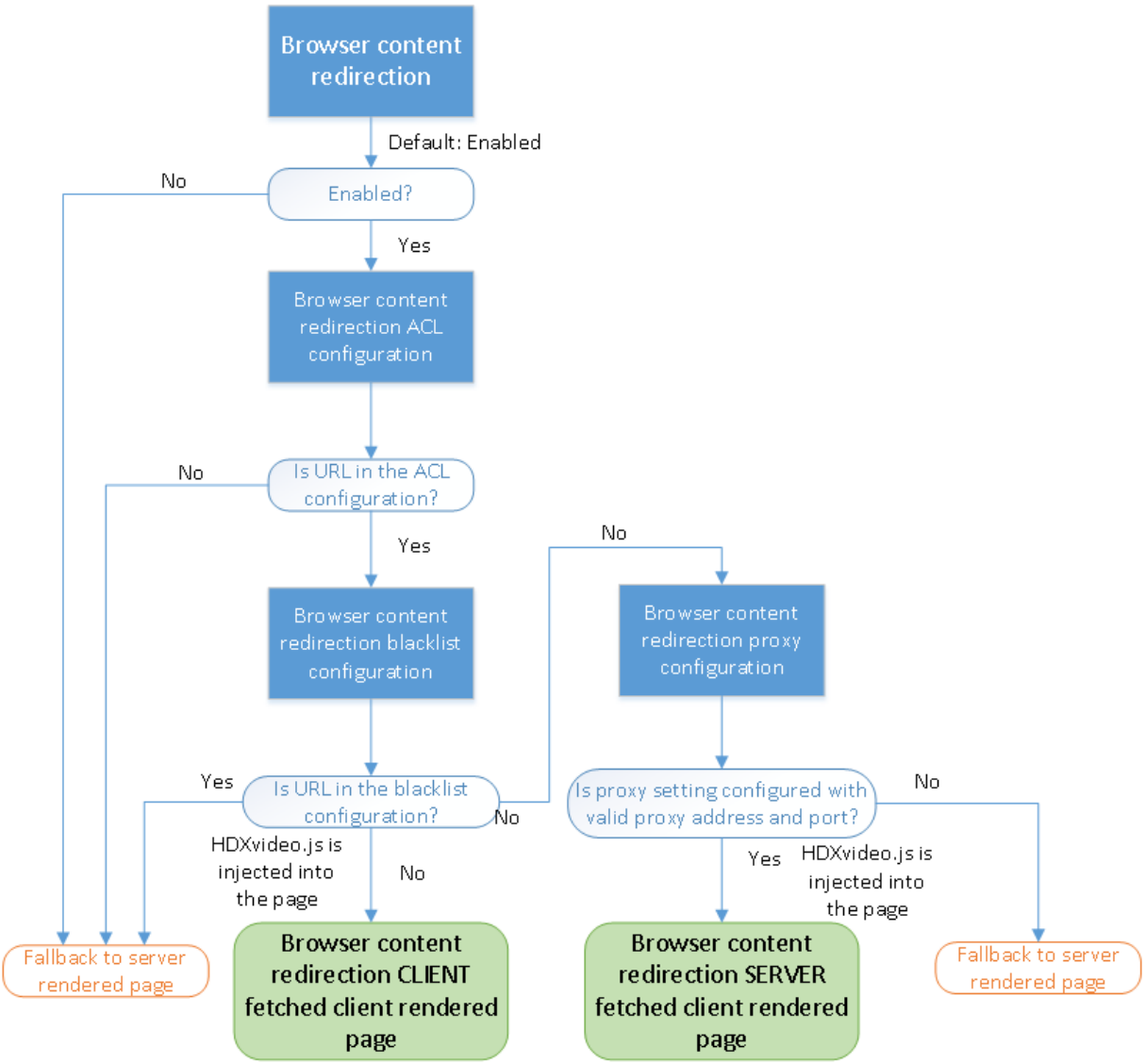
> o cuidado de fazer backup do registro antes de editá-lo.
>
> Opções de substituição de registros para configurações de política:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

Nome	Tipo	Valor
WebBrowserRedirection	DWORD	1=Allowed, 0=Prohibited
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	



Inserção HDXVideo.js para redirecionamento de conteúdo do navegador



HdxVideo.js é injetado na página da Web usando o redirecionamento de conteúdo do navegador extensão Chrome ou o Internet Explorer Browser Helper Object (BHO). 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 Document Object Model (DOM) da página para controlar a navegação.

O BHO decide se deve injetar HdxVideo.js em uma determinada página. A decisão baseia-se nas políticas administrativas apresentadas no fluxograma anterior.

Depois que decide injetar o JavaScript e redirecionar o conteúdo do navegador para o cliente, a página da Web fica em branco no navegador do Internet Explorer no VDA. Definir o **Document.body.innerHTML** como vazio remove todo o corpo da página da Web no VDA. A página está pronta para ser enviada ao cliente para ser exibida no navegador de sobreposição (Hdxbrowser.exe)

no cliente.

Configurações da política de sensores do cliente

June 28, 2023

A seção **Client Sensors** inclui configurações de política para controlar como as informações do sensor do dispositivo móvel são tratadas em uma sessão de usuário.

Allow applications to use the physical location of the client device

Essa configuração determina se os aplicativos em execução em uma sessão em um dispositivo móvel podem 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 para 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 de aplicativo Citrix Workspace para acessar o local. Os dispositivos Android e iOS emitem um aviso na primeira solicitação de informações de localização em cada sessão.

Ao desenvolver aplicativos hospedados que usam a configuração Allow applications to use the physical location of the client device, considere o seguinte:

- Verifique se um aplicativo habilitado para localização não confia que as informações de localização estejam disponíveis porque:
  - Um usuário pode não permitir acesso a informações de localização.
  - O local pode não estar disponível ou pode ser alterado enquanto o aplicativo estiver 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:
  - Estar com o recurso de localização desativado por padrão.
  - Fornecer ao usuário uma opção para permitir ou não permitir o recurso enquanto o aplicativo estiver em execução.
  - Fornecer ao usuário uma opção para limpar os dados de localização que o aplicativo armazena em cache. (O aplicativo Citrix Workspace não armazena em cache os dados de localização.)

- Um aplicativo habilitado para localização deve gerenciar a granularidade das informações de localização. Esse gerenciamento garante que os dados adquiridos sejam adequados à 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 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 da política da interface do usuário

June 28, 2023

A seção **Desktop UI** inclui configurações de política que controlam efeitos visuais, como papel de parede da área de trabalho, animações de menu e arrasto de imagens. Essas configurações de política ajudam a gerenciar a largura de banda usada nas conexões 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 legado e ao Desktop Composition Redirection (DCR) nesta versão. Essa política é incluída somente 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.

Desktop Composition Redirection

Essa configuração especifica se os recursos de processamento a seguir devem ser usados para renderização gráfica local do DirectX para fornecer aos usuários uma experiência de área de trabalho do Windows mais fluida:

- Unidade de processamento gráfico (GPU) no dispositivo do usuário
- Ou,
- Processador gráfico integrado (IGP) no dispositivo do usuário

Quando ativado, o **Desktop Composition Redirection** oferece uma experiência altamente responsiva do Windows, mantendo a alta escalabilidade no servidor.

Por padrão, o **Desktop Composition Redirection** de trabalho está desativado.

Para cancelar a seleção **Desktop Composition Redirection** e reduzir a largura de banda necessária nas sessões do usuário, selecione **Disabled** quando adicionar essa configuração a uma política.

Desktop Composition Redirection graphics quality

Essa configuração especifica a qualidade dos gráficos usados para o Redirecionamento de Composição da Área de Trabalho.

O padrão é High.

Escolha entre qualidade High, Medium, Low ou Lossless.

Desktop wallpaper

Esta configuração permite ou impede que o papel de parede seja exibido nas sessões do usuário.

Por padrão, as sessões do usuário podem mostrar 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 **Prohibited** ao adicionar essa configuração a uma política.

Menu animation

Essa configuração permite ou impede a animação do menu nas sessões do usuário.

Por padrão, a animação de menu é permitida.

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 aos poucos. 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 esta definição de política estiver definida como **Allowed** e se estiver ativada a configuração de preferência pessoal da Microsoft de a animação de menu.

> **Nota:**
>
> Alterações na animação do menu Configuração de preferência pessoal da Microsoft afetam a área de trabalho. Vamos considerar que você configurou a área de trabalho para descartar as alterações quando a sessão terminar. Nesse caso, um usuário que tenha ativado animações de menu talvez não tenha animação de menu nas sessões subsequentes. Para usuários que necessitam de animação de menu, ative a configuração da Microsoft na imagem principal da área de trabalho ou verifique se a área de trabalho retém as alterações do usuário.

View window contents while dragging

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 **Allowed**, a janela inteira aparece para mover quando você a arrastar. Quando definido como **Prohibited**, somente o contorno da janela aparece para se mover até que você o solte.

Configurações da política de monitoramento do usuário final

June 28, 2023

A seção **End User Monitoring** inclui configurações de política para medir o tráfego da sessão.

ICA round trip calculation

Essa configuração determina se os cálculos de ida e volta da ICA são feitos para conexões ativas.

Por padrão, os cálculos para conexões ativas são ativados.

Por padrão, cada início de medição de ida e volta da ICA fica atrasado. Esse atraso ocorre até que ocorra um tráfego que indique a interação do usuário. Este atraso pode ter duração indeterminada e foi concebido para evitar que a medição ICA de ida e volta seja o único motivo do tráfego ICA.

ICA round trip calculation interval

Essa configuração especifica a frequência, em segundos, na qual os cálculos de ida e volta de ICA são executados.

Por padrão, o processo de ida e volta da ICA é calculado a cada 15 segundos.

ICA round trip calculations for idle connections

Essa configuração determina se os cálculos de ida e volta da ICA são feitos para conexões ociosas.

Por padrão, não são realizados cálculos para conexões ociosas.

Por padrão, cada início de medição de ida e volta da ICA fica atrasado. Esse atraso ocorre até que ocorra um tráfego que indique a interação do usuário. Este atraso pode ter duração indeterminada e foi concebido para evitar que a medição ICA de ida e volta seja o único motivo do tráfego ICA.

Configuração da política de experiência de desktop aprimorada

June 28, 2023

A configuração de política de experiência de área de trabalho aprimorada executa sessões em sistemas operacionais de servidor que se parecem com áreas de trabalho locais do Windows 7.

Por padrão, essa configuração é Allowed.

Se existir um perfil de usuário com o tema do Windows Classic na área de trabalho virtual, essa política não fornecerá uma experiência de área de trabalho aprimorada para esse usuário. Vamos considerar que um usuário com um perfil de usuário com o tema do Windows 7 faz logon em uma área de trabalho virtual executando o Windows Server 2012. Além disso, a política não está configurada nem desativada. Nesse caso, esse usuário vê uma mensagem de erro indicando falha na aplicação do tema.

Em ambos os casos, a redefinição do perfil de usuário resolve o problema.

Se você desabilitar a política em uma área de trabalho virtual com sessões de usuário ativas, a interface dessas sessões se tornará inconsistente nas áreas de trabalho do Windows 7 e Windows Classic. Para evitar essa inconsistência, tenha o cuidado de reiniciar a área de trabalho virtual depois de alterar essa configuração de política. Em seguida, exclua todos os perfis de roaming na área de trabalho virtual. A Citrix também recomenda excluir todos os demais perfis de usuário na área de trabalho virtual para evitar inconsistências entre perfis.

Vamos considerar que você está usando perfis de usuário de roaming em seu ambiente. Nesse caso, verifique se o recurso Enhanced Desktop Experience está ativado ou desativado para todas as áreas de trabalho virtuais que compartilham um mesmo perfil.

A Citrix não recomenda o compartilhamento de perfis de roaming entre desktops virtuais que executam sistemas operacionais de servidor e sistemas operacionais cliente. Os perfis para sistemas operacionais de cliente e servidor são diferentes. O compartilhamento de perfis de roaming em ambos os tipos pode causar inconsistências nas propriedades do perfil quando um usuário passa de um para o outro.

Configurações da política de redirecionamento de arquivos

June 28, 2023

A seção **File Redirection** inclui configurações de política relacionadas ao mapeamento da unidade cliente e à otimização da unidade cliente.

Auto connect client drives

Essa configuração permite ou impede a conexão automática de unidades de cliente quando os usuários fazem logon.

Por padrão, a conexão automática é permitida.

Ao adicionar essa configuração a uma política, tenha o cuidado de ativar 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, defina essa configuração e a configuração **Client optical drives**.

As seguintes configurações de política são correlatas:

- **Client drive redirection**
- **Client floppy drives**
- **Client optical drives**
- **Client fixed drives**
- **Client network drives**
- **Client removable drives**

Client drive redirection

Essa configuração ativa ou desativa o redirecionamento de arquivos de e para unidades no dispositivo do usuário.

Por padrão, o redirecionamento de arquivo está habilitado.

> **Nota:**
>
> As configurações de política de redirecionamento da unidade do cliente não se aplicam a unidades mapeadas para sessões por meio de redirecionamento USB genérico.

Quando ativadas, os usuários podem salvar arquivos em todas as unidades de cliente. Quando desativado, todo o redirecionamento de arquivos é impedido. Essa configuração é aplicável independentemente do estado das configurações de redirecionamento de arquivo individual. As configurações de redirecionamento de arquivo individual incluem unidades de disquete do cliente e unidades de rede do cliente.

As seguintes configurações de política são correlatas:

- **Client floppy drives**
- **Client optical drives**
- **Client fixed drives**
- **Client network drives**
- **Client removable drives**

Client fixed drives

Essa configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades fixas no dispositivo do usuário.

Por padrão, é permitido o acesso a unidades fixas do cliente.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed. Se essas configurações estiverem desativadas, as unidades fixas do cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente, independentemente do estado da configuração **Client fixed drives**.

Defina a configuração **Auto connect client drives** para garantir que as unidades fixas sejam conectadas automaticamente quando os usuários fazem logon.

Client floppy drives

Essa configuração permite ou impede que os usuários acessem ou salvem arquivos em unidades de disquete no dispositivo do usuário.

Por padrão, é permitido acessar unidades de disquete do cliente.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed. Se essas configurações estiverem desativadas, as unidades de disquete do cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente, independentemente do estado da configuração **Client floppy drives**.

Para garantir que as unidades de disquete sejam conectadas automaticamente quando os usuários fazem logon, defina a configuração **Auto connect client drives**.

Client network drives

Essa configuração permite ou impede que os usuários acessem e salvem arquivos em unidades de rede (remotas) através do dispositivo de usuário.

Por padrão, o acesso às unidades de rede cliente é permitido.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed. Se essas configurações estiverem desativadas, as unidades de rede cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente. Essa configuração é aplicável independentemente do estado da configuração **Client network drives**.

Para garantir que as unidades de rede sejam conectadas automaticamente quando os usuários fazem logon, defina a configuração **Auto connect client drives**.

Client optical drives

Essa configuração permite ou impede que os usuários acessem ou salvem arquivos em:

- CD-ROM no dispositivo do usuário
- DVD-ROM no dispositivo do usuário
- Unidades BD-ROM no dispositivo do usuário.

Por padrão, é permitido acessar unidades óticas do cliente.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como **Allowed**. Se essas configurações estiverem desativadas, as unidades óticas do cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente. Essa configuração é aplicável independentemente do estado da configuração **Client optical drives**.

Para garantir que as unidades óticas sejam conectadas automaticamente quando os usuários fazem logon, defina a configuração **Auto connect client drives**.

Client removable drives

Essa 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 essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed. Se essas configurações estiverem desativadas, as unidades removíveis do cliente não serão mapeadas e os usuários não poderão acessar essas unidades manualmente. Essa configuração é aplicável independentemente do estado da configuração **Client removable drives**.

Defina a configuração **Auto connect client drives** para garantir que as unidades removíveis sejam conectadas automaticamente quando os usuários fazem logon.

Redirecionamento de host para cliente

Essa configuração ativa ou desativa associações de tipos de arquivo para URLs e alguns conteúdos de mídia a serem abertos no dispositivo do usuário. Quando desativado, o conteúdo é aberto no servidor.

Por padrão, a associação de tipo de arquivo está desativada.

Esses tipos de URL são abertos localmente quando você ativa esta configuração:

- HTTP
- HTTPS
- Real Player and QuickTime (RTSP)
- Real Player and QuickTime (RTSPU)
- Legacy Real Player (PNM)
- Microsoft Media Server (MMS)

Preserve client drive letters

Essa configuração ativa ou desativa o mapeamento de unidades de cliente para a mesma letra de unidade na sessão.

Por padrão, as letras da unidade do cliente não são preservadas.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed.

Read-only client drive access

Essa configuração permite ou impede que usuários e aplicativos:

- Criem arquivos em unidades cliente mapeadas
- Alterem arquivos em unidades cliente mapeadas
- Alterem pastas em unidades cliente mapeadas

Por padrão, arquivos e pastas em unidades de cliente mapeadas podem ser alterados.

Se definida como ativada, arquivos e pastas serão acessíveis com permissões somente leitura.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed.

Special folder redirection

Essa configuração permite ou impede que os usuários do aplicativo Citrix Workspace e 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.

Essa configuração impede que todos os objetos filtrados por meio de uma política tenham redirecionamento de pasta especial, independentemente das configurações que existam em outros lugares. Quando essa configuração é proibida, todas as configurações correlatas especificadas para o aplicativo StoreFront, Web Interface ou Citrix Workspace são ignoradas.

Para definir quais usuários podem ter redirecionamento de pasta especial, selecione **Allowed** e inclua essa configuração em uma política filtrada nos usuários que você deseja que tenham esse recurso. Essa configuração substitui todas as outras configurações de redirecionamento de pastas especiais.

As configurações de política que impedem que os usuários acessem ou salvem arquivos em seus discos rígidos locais também impedem que o redirecionamento de pasta especial funcione. Essa situação ocorre porque o redirecionamento de pasta especial deve interagir com o dispositivo do usuário.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client fixed drives** está presente e definida como Allowed.

Políticas de transferência de arquivos

Por padrão, a transferência de arquivos está habilitada. Use o Web Studio para alterar essas políticas, localizadas em **User setting - ICA\File Redirection**. Considere o seguinte ao usar políticas de transferência de arquivos:

- **Transferência de arquivos para o aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários transfiram arquivos entre uma sessão do Citrix Virtual Apps and Desktops e seus dispositivos.
- **Carregar arquivo para o aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários carreguem arquivos de seus dispositivos para uma sessão do Citrix Virtual Apps and Desktops.
- **Baixar arquivo do aplicativo Citrix Workspace para Chrome OS/HTML5** - Permite ou impede que os usuários baixem arquivos de uma sessão do Citrix Virtual Apps and Desktops para seus dispositivos.

> **Nota:**
>
> As políticas de transferência de arquivos são aplicáveis somente ao aplicativo Citrix Workspace para HTML5 e ao aplicativo Citrix Workspace para Chrome OS.

Use asynchronous writes

Essa configuração ativa ou desativa gravações de disco assíncronas.

Por padrão, as gravações assíncronas são desativadas.

As gravações de disco assíncronas podem melhorar a velocidade das transferências de arquivos e gravação em discos clientes em WANs, que normalmente caracterizam a largura de banda relativamente alta e a alta latência. No entanto, se houver uma falha de conexão ou disco, o arquivo cliente ou os arquivos 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 de disco assíncronas somente para usuários que precisam de conectividade remota com boa velocidade de acesso a arquivos. E quem pode facilmente recuperar arquivos ou dados perdidos se houver uma falha de conexão ou disco.

Ao adicionar essa configuração a uma política, verifique se a configuração **Client drive redirection** está presente e definida como Allowed. Se essa configuração estiver desativada, as gravações assíncronas não ocorrerão.

Configurações da política de gráficos

September 13, 2023

A seção **Graphics** inclui configurações de política para controlar como as imagens são tratadas nas sessões do usuário.

Allow visually lossless compression

Essa configuração permite que a compactação visualmente sem perdas seja usada em vez da verdadeira compressão sem perdas para gráficos. O recurso "visually lossless"melhora o desempenho se comparado a "true lossless", mas acarreta pequenas perdas que não são perceptíveis para o olho humano. Essa configuração altera a maneira como os valores da configuração de qualidade visual são usados.

Por padrão, essa configuração está desativada.

Indicador de status gráfico

Essa configuração define o indicador de status gráfico que deve ser executado na sessão do usuário. Essa ferramenta permite que o usuário veja informações sobre o modo gráfico ativo. As informações incluem detalhes sobre codec de vídeo, codificação de hardware, qualidade de imagem e monitores em uso para a sessão. Com o indicador de status gráfico, o usuário também pode ativar ou desativar o modo de pixel perfeito.

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 uma 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 das versões anteriores. Essa política ativa o indicador sem perdas para o Citrix Virtual Apps and Desktops versões 7.16 a 1809.

Compartilhamento de tela

Esta configuração permite que os usuários compartilhem suas sessões, incluindo conteúdo da tela, teclado e mouse, com outros usuários.

Por padrão, a configuração está desativada.

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 o tráfego de entrada e de saída.

Por padrão, o intervalo de portas TCP é definido como 52525-52625.

A porta usada para o compartilhamento de tela deve ser adicionada à lista de exceções do firewall. Essa opção é exibida como uma caixa de seleção ao instalar o VDA. Por padrão, essa opção não está selecionada.

Display memory limit

Essa configuração especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão.

Por padrão, o limite de memória de exibição é 65.536 kilobytes.

Especifica o tamanho máximo do buffer de vídeo em kilobytes para a sessão. Especifique uma quantidade em kilobytes de 128 a 4.194.303. O valor máximo de 4.194.303 não limita a memória do visor. Por padrão, a memória de exibição é 65.536 kilobytes. O uso de mais profundidade de cor e resolução mais alta para conexões requer mais memória. No modo gráfico legado, se o limite de memória for atingido, a tela se degrada de acordo com a configuração "Preferência de degradação do modo de exibição".

Para conexões que exigem mais profundidade de cor e resolução mais alta, 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. Nesse caso, a memória máxima necessária é (32 / 8) x (600) x (800) = 1920000 bytes, o que gera um limite de memória de exibição de 1920 KB.

Profundidades de cores diferentes de 32 bits só estarão disponíveis se a configuração de política de modo gráfico legado estiver ativada.

O HDX aloca apenas a quantidade de memória de exibição necessária para cada sessão. Portanto, se apenas alguns usuários exigem mais do que o padrão, não há impacto negativo na escalabilidade, aumentando o limite de memória de exibição.

Display mode degrade preference

> **Nota:**
>
> No Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Quando o limite de memória de exibição da sessão é atingido, essa configuração especifica se a profundidade de cor ou a resolução se degrada primeiro.

Por padrão, a profundidade de cor é degradada primeiro.

Quando o limite de memória da sessão for atingido, você pode reduzir a qualidade das imagens exibidas. Você pode reduzir a qualidade escolhendo se a profundidade de cor ou a resolução será 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 forem degradadas, defina a configuração Notify user when display mode is degraded.

Dynamic windows preview

Essa configuração ativa ou desativa a exibição de janelas contínuas em:

- Virar
- Virar 3D
- Visualização da barra de tarefas
- Espiar as 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.
Espiar as janelas	Quando o usuário passa o mouse sobre uma imagem de visualização da barra de tarefas, uma imagem de tamanho normal da janela aparece na tela.
Virar	Quando o usuário pressiona ALT+TAB, são mostrados pequenos ícones de visualização para cada janela aberta.
Virar 3D	Quando o usuário pressiona a tecla do logotipo tab+Windows, imagens grandes das janelas são abertas em cascata na tela.

Por padrão, essa configuração está ativada.

Image caching

> **Nota:**
>
> No Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração ativa ou desativa o cache e a recuperação de seções de imagens em sessões. Armazenar imagens em cache em seções e recuperar essas seções quando necessário faz 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.

> **Nota:**
>
> A configuração de cache de imagens controla como as imagens são armazenadas em cache e recuperadas. A configuração não controla se as imagens são armazenadas em cache. As imagens serão armazenadas em cache se a configuração do modo gráfico legado estiver ativada.

Modo gráfico legado - não suportado. Apenas para compatibilidade com versões anteriores

> **Importante:**
>
> Não oferecemos suporte ao modo gráfico legado e ao Desktop Composition Redirection (DCR) nesta versão. Esta política foi incluída apenas para compatibilidade com versões anteriores quando são usados o XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores VDA com Windows 7 e Windows 2008 R2.

Essa configuração desativa a alta qualidade gráfica. Use essa configuração para reverter para a experiência gráfica legada, reduzindo o consumo de largura de banda em uma conexão WAN ou móvel. As reduções de largura de banda introduzidas no XenApp e no XenDesktop 7.13 tornam esse modo obsoleto.

Por padrão, essa configuração está desativada e os usuários recebem alta qualidade gráfica.

O modo gráfico legado é compatível com:

- Windows 7
- VDAs do Windows Server 2008 R2.

O modo gráfico legado não é compatível com:

- 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 no XenDesktop 7.6 FP3 ou superior.

Maximum allowed color depth

> **Nota:**
>
> No Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração especifica a profundidade máxima de cor 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 do Thinwire. Ele não se aplica a VDAs que tenham um driver não ThinWire como driver de vídeo primário. Esses VDAs são VDAs que usam um driver WDDM (Windows Display Driver Model) como o driver de vídeo primário. Para VDAs de SO de sessão única que usam um driver WDDM como o driver de exibição principal, como o Windows 8, essa configuração não tem efeito. No caso de VDAs com SO Windows multissessão que usam um driver WDDM, como o Windows Server 2012 R2, essa configuração pode impedir que os usuários se conectem ao VDA.

Definir uma profundidade de cor alta requer mais memória. Para degradar a profundidade de cor quando o limite de memória for atingido, defina a configuração de **Display mode degrade preference**. Quando a profundidade de cor é degradada, as imagens exibidas usam menos cores.

Notify user when display mode is degraded

> **Nota:**
>
> No Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração exibe uma breve explicação para o usuário quando a profundidade de cor ou resolução é degradada.

Por padrão, a notificação de usuários é desativada.

Optimize for 3D graphics workload

Essa configuração configura as configurações padrão apropriadas que melhor se adequam a cargas de trabalho com profusão de imagens. Ative essa configuração para usuários cuja carga de trabalho se concentra em aplicativos com profusão de imagens. Aplique esta política somente nos casos em que uma GPU esteja disponível para a sessão. Todas as outras configurações que substituam explicitamente as configurações padrão definidas por esta política têm precedência.

Por padrão, a otimização da carga de trabalho de gráficos 3D está desativada.

Queuing and tossing

> **Nota:**
>
> No Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Com essa configuração, são descartadas as imagens em fila que são substituídas por outra imagem.

Por padrão, o enfileiramento e o descarte estão habilitados.

Essa configuração melhora a resposta quando os gráficos são enviados para o dispositivo do usuário. Se essa configuração for definida, as animações poderão ficar entrecortadas devido a quadros descartados.

Use video codec for compression

Permite o uso de um codec de vídeo para compactar gráficos quando a decodificação de vídeo estiver disponível no endpoint. Quando a opção **For the entire screen** é selecionada, o codec de vídeo é aplicado como o codec padrão para todos. Quando a opção **For actively changing regions** é selecionada, o codec de vídeo é usado para áreas onde há mudança constante na tela, outros dados usam compactação de imagem fixa e cache de bitmap. Quando a decodificação de vídeo não está disponível no ponto de extremidade, ou quando você especifica **Do not use video codec**, é usada uma combinação de compactação de imagem fixa e cache de bitmap. Quando a opção **Use when preferred** é selecionada, o sistema faz a escolha, com base em vários fatores. Os resultados podem variar entre as versões à medida que o método de seleção é aprimorado.

Selecione **Use when preferred** para permitir que o sistema faça o melhor possível para escolher as configurações apropriadas para o cenário atual.

Selecione **For the entire screen** para otimizar para melhorar a experiência do usuário e largura de banda, especialmente em casos com uso intenso de vídeo renderizado por servidor e gráficos 3D.

Selecione **For actively changing regions** para otimizar o desempenho de vídeo melhorado, especialmente em baixa largura de banda, mantendo a escalabilidade para conteúdo estático e que se altera lentamente. Essa configuração é suportada em implantações com vários monitores.

Selecione **Do not use video codec** para otimizar a carga da CPU do servidor e para casos que não têm inúmeros vídeos renderizados pelo servidor ou outros aplicativos com profusão de imagens.

O padrão é **Use when preferred**.

Usar codificação de hardware para vídeo (Use hardware encoding for video)

Esta configuração permite o uso de hardware gráfico, se disponível, para comprimir elementos de tela com o codec de vídeo. Se esse hardware não estiver disponível, o VDA recorre à codificação baseada em CPU usando o codec de vídeo do software.

A opção padrão para esta configuração de política é **Enabled**.

Há suporte para vários monitores.

Qualquer aplicativo Citrix Workspace compatível com decodificação de vídeo pode ser usado com codificação de hardware.

NVIDIA

Para GPUs NVIDIA GRID, a codificação de hardware é suportada com VDAs para SO multissessão e SO de sessão única.

As GPUs NVIDIA devem suportar codificação de hardware NVENC. Consulte o Codec de vídeo NVIDIA SDK para obter uma lista de GPUs compatíveis.

NVIDIA GRID requer a versão 3.1 ou superior do driver. A NVIDIA Quadro requer a versão 362.56 ou superior do driver. A Citrix recomenda drivers do ramo NVIDIA Release R361.

O texto sem perdas não é compatível com a codificação de hardware NVENC. Se você habilitou o texto sem perdas, o texto sem perdas terá prioridade sobre a codificação de hardware NVENC.

O uso seletivo do codec de hardware H.264 para regiões em mudança ativa é suportado.

A compressão visualmente sem perdas (YUV 4:4:4) tem suporte. Visualmente sem perdas (configuração de política gráfica Allow visually lossless compression) requer o aplicativo Citrix Workspace 1808 ou superior ou Citrix Receiver para Windows 4.5 ou superior.

Intel

Para os processadores gráficos Intel Iris Pro, a codificação de hardware é suportada com VDAs para SO de sessão única e SO multissessão.

Os processadores gráficos Intel Iris Pro na família de processadores Intel Broadwell e posterior são suportados. O Intel Remote Displays SDK versão 1.0 é necessário e pode ser baixado no site da Intel: SDK de monitores remotos.

O texto sem perdas é suportado somente quando a política de codec de vídeo é definida para toda a tela e a política **Optimize for 3D graphics workload** está desativada.

Visualmente sem perdas (YUV 4:4:4) não tem suporte.

O codificador Intel oferece uma boa experiência ao 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 a quantos monitores a máquina virtual se conecta. O administrador decide definir essa configuração de política por usuário ou por máquina para manter uma boa experiência do usuário.

AMD

Para AMD, a codificação de hardware é suportada com VDAs para SO de sessão única.

As GPUs AMD devem suportar o SDK RapidFire. Por exemplo, as GPUs AMD Radeon Pro ou FirePro.

Para que a codificação funcione, instale os drivers AMD mais recentes. Você pode baixar esses drivers de https://www.amd.com/en/support.

O texto sem perdas não é compatível com a codificação de hardware AMD. Se você habilitou o texto sem perdas, o texto sem perdas terá 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

June 28, 2023

Esta seção inclui configurações de política que permitem armazenar em cache dados de imagem em dispositivos de usuário quando as conexões cliente são limitadas em largura de banda.

Persistent cache threshold

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração **Legacy graphics mode** estiver ativada.

Essa configuração armazena em cache bitmaps no disco rígido do dispositivo do usuário e, portanto, permite a reutilização de imagens de sessões anteriores grandes e usadas com frequência.

Por padrão, o limite é 3000000 bits por segundo.

O valor de limite representa o ponto abaixo do qual o recurso de cache persistente é ativado. Por exemplo, usando o valor padrão, bitmaps são armazenados em cache no disco rígido do dispositivo do usuário quando a largura de banda cai abaixo de 3000000 bps.

Configurações da política do Framehawk

June 28, 2023

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não tem mais suporte. Em vez disso, use o Thinwire com o transporte adaptativo ativado.

A seção **Framehawk** inclui configurações de política que habilitam e definem o canal de exibição do Framehawk no servidor.

Framehawk display channel

Quando ativado, o servidor tenta usar o canal de exibição do Framehawk para os gráficos do usuário e a entrada remota. Esse canal de exibição usa o UDP para fornecer uma melhor experiência ao usuário em redes com características de alta perda e latência. No entanto, ele também pode usar mais recursos de servidor e largura de banda do que outros modos gráficos.

Por padrão, o canal de exibição do Framehawk está desativado.

Framehawk display channel port range

Essa configuração de política especifica o intervalo de números de porta UDP que o VDA usa para trocar dados do canal de exibição do 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 pelo menor número de porta e incrementando em cada tentativa subsequente. A porta lida com o tráfego de entrada e de saída.

Por padrão, o intervalo de portas é 3224,3324.

Configurações da política Keep Alive

June 28, 2023

A seção **Keep Alive** contém configurações de política para gerenciar mensagens de manutenção de atividade de ICA.

Tempo limite de manutenção de vida da ICA

Esta configuração especifica o número de segundos entre mensagens sucessivas de manutenção de atividade ICA.

Por padrão, o intervalo entre mensagens de keep-alive é 60 segundos.

Especifique um intervalo entre 1-3600 segundos em que enviar mensagens de manutenção de ICA. Não defina essa configuração se o software de monitoramento de rede for responsável pelo fechamento de conexões inativas.

Mensagens de manutenção da ICA

Essa configuração permite ou desabilita o envio de mensagens de manutenção de atividade ICA periodicamente.

Por padrão, as mensagens de manutenção de vida não são enviadas.

Ativar essa configuração evita que conexões interrompidas sejam desconectadas. Se o servidor não detectar nenhuma atividade, essa configuração impede que os Serviços de Área de Trabalho Remota (RDS) desconectem a sessão. O servidor envia mensagens de manutenção de vida a cada poucos segundos para detectar se a sessão está ativa. Se a sessão não estiver mais ativa, o servidor marca a sessão como desconectada.

O ICA keep-alive não funciona se você estiver usando a confiabilidade da sessão. Configure a manutenção da atividade de ICA somente para conexões que não estão usando a confiabilidade da sessão.

Configurações de política correlatas: Conexões de confiabilidade da sessão.

Configurações da política de acesso ao aplicativo local

June 28, 2023

A seção **Local App Access** inclui configurações de política que gerenciam os aplicativos dos usuários instalados localmente com aplicativos hospedados. Essas configurações de política gerenciam a integração em um ambiente de área de trabalho hospedado.

Allow Local App Access

Essa configuração permite ou impede a integração de aplicativos dos usuários instalados localmente com aplicativos hospedados. Essas configurações de política gerenciam a integração em um ambiente de área de trabalho hospedado.

Quando um usuário inicia um aplicativo instalado localmente, esse aplicativo parece ser executado em sua área de trabalho virtual, mesmo que ele esteja realmente sendo executado localmente.

Se você definir a configuração de política **Allow local app access** como **Enabled**, o redirecionamento de conteúdo do navegador não será suportado e o status da bateria da área de notificação do lado do cliente não será exibido nas sessões da área de trabalho.

Por padrão, **Allow Local App Access** é proibido.

URL redirection block list

Essa configuração especifica 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
- Sites com conteúdo de mídia avançada que são melhor renderizados no dispositivo do usuário.

Por padrão, nenhum site é especificado.

URL redirection allow list

Essa configuração especifica sites que são renderizados no ambiente em que são iniciados.

Por padrão, nenhum site é especificado.

Configurações da política de experiência móvel

June 28, 2023

A seção **Mobile Experience** inclui configurações de política para lidar com o Citrix Mobility Pack.

Automatic keyboard display

Essa configuração ativa ou desativa a exibição automática do teclado em telas de dispositivos móveis.

Por padrão, a exibição automática do teclado está desativada.

Launch touch-optimized desktop

Esta configuração está desativada e não está disponível para máquinas Windows 10 ou Windows Server 2016.

Essa configuração determina o comportamento geral da interface do aplicativo Citrix Workspace. Essa configuração permite ou proíbe uma interface sensível ao toque otimizada para tablets.

Por padrão, é usada uma interface sensível ao toque.

Para utilizar apenas a interface do Windows, defina esta configuração de política como Prohibited.

Remote the combo box

Essa configuração determina os tipos de caixas de combinação que você pode exibir em sessões em dispositivos móveis. Defina essa configuração de política como Allowed para exibir o controle de caixa de combinação nativa do dispositivo. Quando essa configuração é permitida, um usuário pode alterar uma configuração de sessão do aplicativo Citrix Workspace para iOS para usar a caixa de combinação do Windows.

Por padrão, o recurso **Remote the combo box** é proibido.

Configurações de política multimídia

June 28, 2023

A seção **Multimedia** inclui configurações de política para gerenciar streaming HTML5 e áudio e vídeo do Windows nas sessões do usuário.

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

Políticas multimídia

Por padrão, todas as políticas multimídia definidas no Delivery Controller são armazenadas nestes registros:

Políticas da máquina:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

Políticas do usuário:

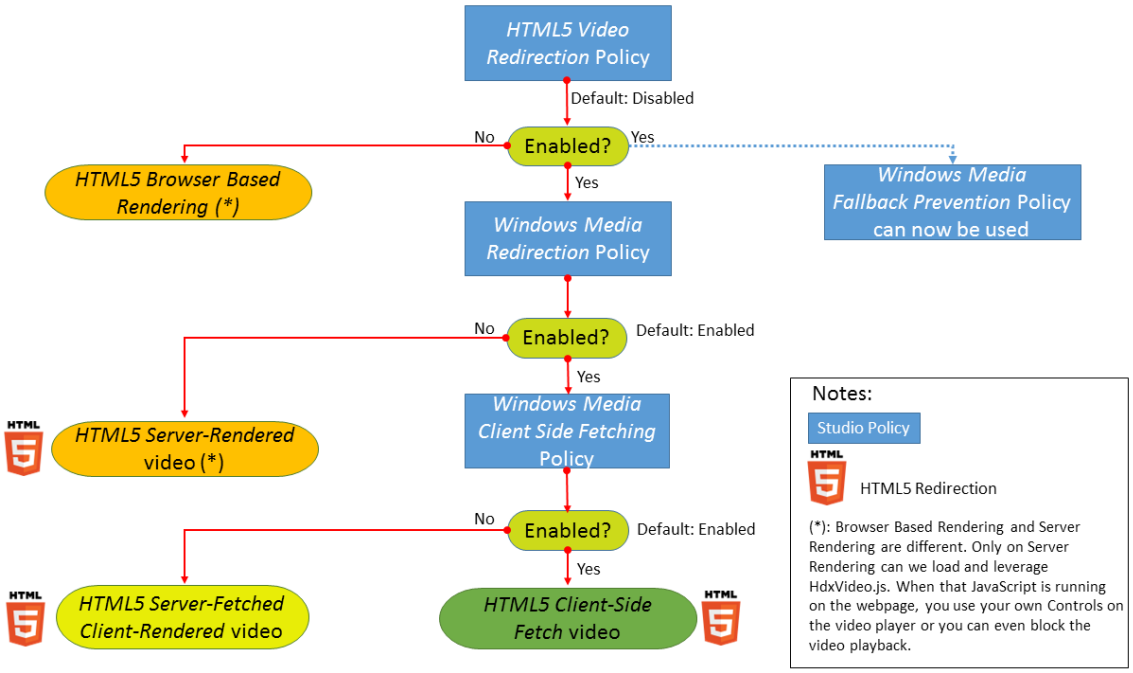
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

Para localizar o ID da sessão de usuário atual, emita o comando **qwinsta** na linha de comando do Windows.

HTML5 video redirection

Controla e otimiza a forma como os servidores Citrix Virtual Apps and Desktops oferecem conteúdo multimídia da Web HTML5 aos usuários.

Por padrão, essa configuração está desativada.



Nesta versão, esse recurso está disponível apenas para páginas da Web controladas. Requer a adição de JavaScript às páginas web em que 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%Arquivos de programas%/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 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 até ele.

Vamos considerar que o JavaScript não é adicionado às suas páginas da Web controladas e o usuário reproduz um vídeo HTML5. Nesse caso, o Citrix Virtual Apps and Desktops usa como padrão a renderização do lado do servidor.

Para que o redirecionamento de vídeos HTML5 funcione, permita ***Windows Media Redirection***. Essa política é obrigatória para Server Fetch Client Render e necessária para Client Side Fetching. Por sua vez, Client Side Fetching também exige que *Windows Media client-side content fetching* esteja Allowed.

O Microsoft Edge não oferece suporte a esse recurso.

HdxVideo.js substitui os controles do navegador HTML5 Player com o seu próprio. 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 em que a política de **HTML5 video redirection** é Prohibited:

(O cliente da Citrix controla quando a política é permitida)

(A página da Web nativa controla quando a política é proibida ou não configurada)

Os seguintes controles de vídeo são suportados:

- play
- pause
- seek
- repeat
- audio
- full screen

Você pode visualizar uma página de teste de redirecionamento de vídeo HTML5 em https://www.citrix.com/virtualization/hdx/html5-redirect.html.

Redirecionamento de vídeo TLS e 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 todo o site

O JavaScript injetado nesses sites deve estabelecer uma conexão TLS com o serviço de redirecionamento de vídeo Citrix HTML5 (WebSocketService.exe) em execução no VDA. O Citrix HDX HTML5 Video Redirection Service no armazenamento de certificados no VDA gera dois certificados personalizados para:

- Obter redirecionamento de vídeo
- Manter a integridade do TLS da página da web

O HdxVideo.js usa o Secure WebSockets para se comunicar com o WebSocketService.exe em execução no VDA. Este processo é executado como uma conta do Sistema Local e faz a terminação SSL e o mapeamento da sessão do usuário.

WebSocketService.exe está ouvindo em 127.0.0.1 na porta 9001.

Limit video quality

Essa configuração se aplica apenas ao Windows Media e não ao HTML5. Ele exige que você habilite a **Optimization for Windows Media multimedia redirection over WAN**.

Essa configuração especifica o nível máximo de qualidade de vídeo permitido para uma conexão HDX. Quando configurada, a qualidade máxima de vídeo é limitada ao valor especificado, garantindo que a qualidade de serviço multimídia (QoS) seja mantida dentro de um ambiente.

Por padrão, essa configuração não está definida.

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.

Microsoft Teams redirection

Essa configuração permite a otimização do Microsoft Teams, com base na tecnologia HDX.

Se essa política estiver ativada e você estiver usando uma versão compatível do aplicativo Citrix Workspace, essa chave de registro será definida como **1** no VDA. O aplicativo Microsoft Teams lê a chave a ser carregada no modo de VDI.
Observe que não é necessário definir a chave do Registro manualmente.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Name: MSTeamsRedirSupport

Valor: DWORD (1 - ativado, 0 - desativado)

> **Nota:**
>
> Vamos considerar que você está usando VDAs da versão 1906.2 ou posterior com versões mais antigas do Controller, que não têm a política disponível no Web Studio. Um exemplo de uma versão mais antiga do controlador é a versão 7.15. Nesse 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 advertências na mistura 7.15 LTSR Controllers e CR VDAs, consulte o artigo do Knowledge Center CTX205549.
>
> Nesse caso, para desativar o recurso para usuários específicos, você pode substituir a configu-

> ração do registro. Substitua as configurações do registro usando uma política de grupo para aplicar um script de logon à unidade organizacional do usuário.

Por padrão, o redirecionamento do Microsoft Teams está habilitado.

Multimedia conferencing

Esta configuração permite ou impede o uso de tecnologia otimizada de redirecionamento de webcam por aplicativos de videoconferência.

Por padrão, o suporte de videoconferência é permitido.

Ao adicionar essa configuração a uma política, verifique se a configuração **Windows Media Redirection** está presente e definida como **Allowed** (o padrão).

Quando usar **Multimedia conferencing**, verifique se as seguintes condições são atendidas:

- Os drivers fornecidos pelo fabricante para a webcam usada para conferências 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 de cada vez. Se várias webcams estiverem instaladas no dispositivo do usuário, o servidor tentará usar cada webcam sucessivamente. Essa tentativa continua até que uma sessão de videoconferência seja criada com êxito.

Esta política não é necessária ao redirecionar a webcam usando o redirecionamento USB genérico. Nesse caso, instale os drivers da webcam no VDA.

Optimization for Windows Media multimedia redirection over WAN

Essa configuração se aplica apenas ao Windows Media e não ao HTML5. A configuração permite o seguinte:

- Transcodificação de multimídia em tempo real
- Permite streaming de mídia de áudio e vídeo para dispositivos móveis por redes degradadas
- Melhora a experiência do usuário melhorando a forma como o conteúdo do Windows Media é entregue pela WAN.

Por padrão, a entrega de conteúdo do Windows Media pela WAN é otimizada.

Ao adicionar essa configuração a uma política, verifique se a configuração de **Windows Media Redirection** está presente e definida como **Allowed**.

Quando essa configuração é ativada, a transcodificação de multimídia em tempo real é implantada automaticamente, conforme necessário, para habilitar o streaming de mídia. Além disso, proporciona uma experiência de usuário perfeita, mesmo em condições extremas de rede.

Use GPU for optimizing Windows Media multimedia redirection over WAN

Essa configuração se aplica apenas ao Windows Media e permite que a transcodificação multimídia em tempo real seja feita na Unidade de Processamento Gráfico (GPU) no Virtual Delivery Agent (VDA). Isso melhora a escalabilidade do servidor. A transcodificação de GPU está disponível somente se o VDA tiver uma GPU compatível para aceleração de hardware. Caso contrário, a transcodificação é feita pela CPU.

Observação: a transcodificação de GPU é suportada somente em GPUs NVIDIA.

Por padrão, é proibido usar a GPU no VDA para otimizar o fornecimento de conteúdo do Windows Media pela WAN.

Ao adicionar essa configuração a uma política, verifique se as seguintes configurações estão presentes e definidas como Allowed:

- **Redirecionamento do Windows Media**
- **Optimization for Windows Media multimedia redirection over WAN settings**

Windows Media fallback prevention

Essa configuração se aplica ao redirecionamento de conteúdo do navegador, HTML5 e Windows Media. Para que ele suporte HTML5, defina a política **HTML5 video redirection** como **Allowed**.

Os administradores podem usar a configuração da política **Windows Media fallback prevention** para especificar os métodos com os quais ocorrem tentativas de fornecer conteúdo por stream aos usuários.

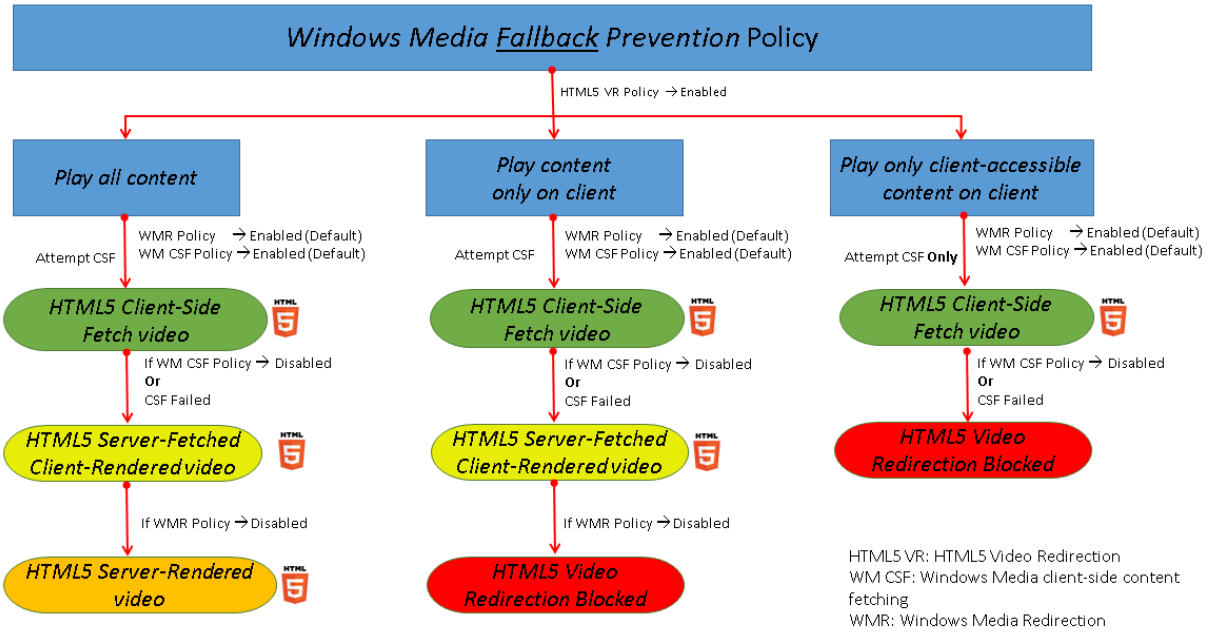
Por padrão, essa configuração não está definida. Quando a configuração é definida como Not Configured, o comportamento é o mesmo que **Play all content**.

Para definir essa configuração, escolha uma das seguintes opções:

- **Play all content**. Tente buscar conteúdo do lado do cliente e, em seguida, Windows Media Redirection. Se não tiver êxito, reproduza o conteúdo no servidor.
- **Play all content only on client**. Tente buscar no lado do cliente e, em seguida, Windows Media Redirection. Se não for bem-sucedido, o conteúdo não será reproduzido.
- **Play only client-accessible content on client**. Tente apenas buscar 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):

```
1 "Company has blocked video because of lack of resources"
```

A duração desta mensagem de erro pode ser personalizada com a seguinte chave de registro no VDA. Se a entrada do Registro não existir, a duração seguirá o padrão 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 limite de DWORD (padrão = 5)

Unidade: segundos

Windows Media client-side content fetching

Essa configuração se aplica tanto ao HTML5 quanto ao Windows Media. A configuração permite que um dispositivo do usuário transmita arquivos multimídia diretamente do provedor de origem na internet ou na intranet, em vez de através do XenApp servidor host XenDesktop.

Por padrão, essa configuração é **Allowed**. Permitir essa configuração melhora o uso da rede e a escalabilidade do servidor. Essa melhoria é obtida movendo-se qualquer processamento na mídia do servidor host para o dispositivo do usuário. Ele também remove o requisito de que uma estrutura

multimídia avançada, como o Microsoft DirectShow ou Media Foundation, seja instalada no dispositivo do usuário. O dispositivo do usuário requer apenas a capacidade de reproduzir um arquivo a partir de um URL

Ao adicionar essa configuração a uma política, verifique se a configuração de **Windows Media Redirection** está presente e definida como **Allowed**. Se **Windows Media Redirection** estiver desativado, a transmissão de arquivos multimídia para o dispositivo do usuário diretamente do provedor de origem também será desativada.

Redirecionamento do Windows Media

Essa configuração se aplica a HTML5 e Windows Media e controla e otimiza a maneira como os servidores fornecem streaming de áudio e vídeo aos usuários.

Por padrão, essa configuração é **Allowed**. Para HTML5, essa configuração não tem efeito se a política de **HTML5 video redirection** for **Prohibited**.

Quando essa configuração está habilitada, a qualidade do áudio e vídeo renderizados do servidor aumenta para um nível que se compara com o áudio e vídeo reproduzidos localmente em um dispositivo de usuário. O servidor transmite multimídia para o cliente na forma original e compactada e permite que o dispositivo do usuário descompacte e renderize a mídia.

O redirecionamento do Windows Media otimiza arquivos multimídia codificados com codecs que aderem aos padrões Microsoft DirectShow, DirectX Media Objects (DMO) e Media Foundation. Para reproduzir um determinado arquivo multimídia, deve estar presente no dispositivo do usuário um codec compatível com o formato de codificação do arquivo multimídia.

Por padrão, o áudio é desativado no aplicativo Citrix Workspace. Para permitir que os usuários executem aplicativos multimídia em sessões do ICA, ative o áudio ou dê aos usuários permissão para ativar o áudio na interface do aplicativo Citrix Workspace.

Selecione **Prohibited** somente se a reprodução de mídia por meio do redirecionamento do Windows Media tiver pior qualidade do que quando renderizada por meio de compressão básica ICA e áudio normal. Essa situação é rara, mas pode acontecer em condições de baixa largura de banda, por exemplo, com mídia com baixa frequência de quadros principais.

Windows Media Redirection buffer size

Esta configuração é um legado e não se aplica ao HTML5.

Essa configuração especifica um tamanho de buffer de 1 a 10 segundos para aceleração multimídia.

Por padrão, o tamanho do buffer é de 5 segundos.

Windows Media Redirection buffer size use

Esta configuração é um legado e não se aplica ao HTML5.

Essa configuração ativa ou desativa o uso do tamanho do buffer especificado na configuração **Windows Media Redirection buffer size**.

Por padrão, o tamanho do buffer especificado não é usado.

Se essa configuração estiver desativada ou se a configuração **Windows Media Redirection buffer size** não estiver configurada, o servidor usará o valor padrão de tamanho do buffer (cinco segundos).

Configurações de políticas de conexões multi-stream

June 28, 2023

A seção **Multi-Stream connections** inclui configurações de política para gerenciar a priorização da Qualidade de Serviço para várias conexões ICA em uma sessão.

> **Nota:**
>
> A descoberta do MTU não tem suporte se a política Multi-Stream connection for permitida.

Audio over UDP

Esta configuração permite ou impede áudio sobre UDP no servidor.

Por padrão, o áudio por UDP é permitido no servidor.

Quando ativada, essa configuração abre uma porta UDP no servidor para oferecer suporte a todas as conexões configuradas para usar o Audio over UDP Real-Time Transport.

Audio UDP port range

Essa configuração especifica o intervalo de números de porta (número de porta mais baixo, número de porta mais alto) usado pelo Virtual Delivery Agent (VDA). Essa 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 aumentando dois a cada tentativa subsequente. Cada porta lida com o tráfego de entrada e de saída.

Por padrão, esse intervalo é definido como 16500,16509.

Multi-Port policy

Essa configuração especifica as portas TCP que devem ser usadas para o tráfego ICA e estabelece a prioridade de rede para cada porta.

Por padrão, a porta primária (2598) tem prioridade Alta.

As configurar portas, você pode atribuir as seguintes prioridades:

- **Very High:** para atividades em tempo real, como conferências de webcam
- **High:** para elementos interativos, como tela, teclado e mouse
- **Medium:** para processos em massa, como mapeamento de drive do cliente
- **Low:** para atividades em segundo plano, como impressão

Cada porta deve ter uma prioridade exclusiva. Por exemplo, você não pode atribuir ao mesmo tempo uma prioridade Very High à porta 1 CGP e à porta CGP 3.

Para remover uma porta da priorização, defina o número da porta como 0. Você não pode remover a porta primária e você não pode alterar o respectivo nível de prioridade.

Quando definir essa configuração, reinicie o servidor. Esta definição só entra em vigor quando a definição da política de configuração **Multi-Stream computer** estiver ativada.

Multi-Stream computer setting

Essa configuração ativa ou desativa o Multi-Stream no servidor.

Por padrão, o Multi-Stream está desativado. Defina a configuração de política Multi-Stream computer se você usar o Citrix SD-WAN ou roteadores de terceiros para obter a qualidade de serviço desejada.

Se o Multi-Stream estiver habilitado, a MTU Discovery, um recurso do transporte adaptável, não tem suporte.

Ao definir essa configuração, reinicie o servidor para garantir que as alterações entrem em vigor.

> **Importante:**
>
> Usar essa configuração de política com configurações de política de limite de largura de banda, como limite geral de largura de banda de sessão, pode produzir resultados inesperados. Ao incluir essa configuração em uma política, verifique se as configurações de limite de largura de banda não estão incluídas.

Multi-Stream user setting

Essa configuração ativa ou desativa o Multi-Stream no dispositivo do usuário.

Por padrão, o Multi-Stream está desativado para todos os usuários. Configure a configuração de usuário Multi-Stream se você usar o Citrix SD-WAN ou roteadores de terceiros para alcançar a Qualidade de Serviço desejada.

Essa configuração só entra em vigor em hosts onde a configuração de política de configuração **Multi-Stream computer** está ativada.

> **Importante:**
>
> Usar essa configuração de política com configurações de política de limite de largura de banda, como limite geral de largura de banda de sessão, pode produzir resultados inesperados. Ao incluir essa configuração em uma política, verifique se as configurações de limite de largura de banda não estão incluídas.

Configurações de atribuição de canal virtual de vários fluxos (Multi-Stream virtual channel assignment)

Essa configuração especifica o fluxo ICA aos quais os canais virtuais são atribuídos quando é usado fluxo múltiplo.

Se você não definir essas configurações, os canais virtuais serão mantidos em seu fluxo padrão. Para atribuir um canal virtual a um fluxo de ICA, selecione o número de fluxo desejado (0, 1, 2, 3) na lista **Stream Number** ao lado do nome do canal virtual.

Se houver um canal virtual personalizado em uso no ambiente, clique em **Add**, especifique o nome do canal virtual na caixa de texto em **Virtual Channels** e selecione o número de fluxo desejado na lista **Stream Number** ao lado dele. O nome especificado deve ser o nome real do canal virtual e não um nome amigável. Por exemplo, CTXSBR em vez de Citrix Browser Acceleration.

Essas configurações só entram em vigor quando você tiver ativado a configuração do computador de multifluxo.

Por padrão, os canais virtuais e suas atribuições de fluxo são:

- AppFlow: 2
- Audio: 0
- Browser Content Redirection: 2
- Client COM Port Mapping: 3
- Client Drive Mapping: 2
- Client Printer Mapping: 3
- Clipboard: 2
- CTXDND: 1 (**Nota:** Com isso é possível arrastar e soltar arquivos entre uma sessão Citrix e um ponto de extremidade local.)
- Plug-in DVC (nome VC estático gerado automaticamente a partir do nome amigável do plug-in DVC, ou atribuído pelo administrador): 2

- End User Experience Monitoring: 1
- File Transfer (HTML5 Receiver): 2
- Generic Data Transfer: 2
- ICA Control: 1
- Input Method Editor: 1
- Legacy Client Printer Mapping (COM1): 1, 3
- Legacy Client Printer Mapping (COM2): 2, 3
- Legacy Client Printer Mapping (LPT1): 1, 3
- Legacy Client Printer Mapping (LPT2): 2, 3
- License Management: 1
- Microsoft Teams/WebRTC Redirection: 1
- Mobile Receiver: 1
- MultiTouch: 1
- Port Forwarding: 2
- Remote Audio and Video Extensions (RAVE): 2
- Seamless (Transparent Window Integration): 1
- Sensor and Location: 1
- Smart Card: 1
- Thinwire Graphics: 1
- Transparent UI Integration/Logon Status: 2
- TWAIN Redirection: 2
- USB: 2
- Zero Latency Font and Keyboard: 2
- Zero Latency Data Channel: 2

Para obter mais informações sobre atribuições e prioridades de canal virtual, consulte o artigo do Knowledge Center CTX131001.

Configurações de política de redirecionamento de porta

June 28, 2023

A seção **Port Redirection** contém configurações da política para o mapeamento da porta do cliente LPT e COM.

Para versões do Virtual Delivery Agent **anteriores à versão 7.0**, use as seguintes configurações de política para configurar o redirecionamento de porta. Para o VDA versões **7.0 a 7.8**, defina essa configuração por meio do registro; consulte Configurar os parâmetros de redirecionamento de porta LPT e porta COM usando o registro. Para o VDA versão **7.9**, use as seguintes configurações de política.

Auto connect client COM ports

Essa configuração ativa ou desativa a conexão automática de portas COM nos dispositivos do usuário quando os usuários fazem logon em um site.

Por padrão, as portas COM do cliente não são conectadas automaticamente.

Auto connect client LPT ports

Essa configuração ativa ou desativa a conexão automática de portas LPT nos dispositivos do usuário quando os usuários fazem logon em um site.

Por padrão, as portas LPT do cliente não são conectadas automaticamente.

Client COM port redirection

Essa configuração permite ou impede o acesso às portas COM no dispositivo do usuário.

Por padrão, o redirecionamento da porta COM é proibido.

As seguintes configurações de política são correlatas:

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

Client LPT port redirection

Essa configuração permite ou impede o acesso às portas LPT no dispositivo do usuário.

Por padrão, o redirecionamento da porta LPT é proibido.

As portas LPT são usadas somente 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 atualmente 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 da porta COM do cliente seja bidirecional, o redirecionamento da porta LPT é apenas saída e limitado a \\client\LPT1 e \\client\LPT2 dentro de uma sessão ICA.

As seguintes configurações de política são correlatas:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

Configurações de política de impressão

June 28, 2023

A seção Impressão contém configurações de política para gerenciar a impressão do cliente.

Client printer redirection

Essa configuração controla se as impressoras cliente são mapeadas para um servidor quando um usuário faz logon em uma sessão.

Por padrão, o mapeamento da impressora do cliente é permitido. Se essa configuração estiver desativada, a impressora PDF da sessão não será criada automaticamente.

Configurações de política correlatas: criar automaticamente impressoras cliente

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 dos Serviços de Área de Trabalho Remota 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 de sessão ou 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 através das configurações de perfil (conhecidas como impressão por proximidade).

Printer assignments

Essa configuração fornece uma alternativa às configurações padrão da impressora e das impressoras de sessão. Use as configurações da impressora padrão e das impressoras de sessão para definir

comportamentos para um site, grupo grande ou unidade organizacional. Use a configuração **Printer assignments** 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.

Ele também especifica as impressoras de rede que devem ser criadas automaticamente em uma sessão para cada dispositivo do usuário. Por padrão, nenhuma impressora é especificada.

- Ao definir o valor padrão da impressora:

  Para usar a impressora padrão atual para o dispositivo do usuário, selecione Do not adjust.

  Para usar a configuração atual do perfil de usuário dos Serviços de Ambiente de Trabalho Remoto ou do Windows para a impressora padrão, selecione Do not adjust. Se você escolher essa opção, a impressora padrão não será salva no perfil e não será alterada de acordo com outras propriedades de sessão ou cliente. A impressora padrão em uma sessão é a primeira impressora criada automaticamente na sessão, que é:

  - 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 deseja criar automaticamente. Depois de adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual em cada logon.

Printer auto-creation event log preference

Essa configuração especifica os eventos registrados durante o processo de criação automática da impressora. Você pode optar por não registrar nenhum erro ou aviso, apenas erros ou erros e avisos.

Por padrão, são registrados erros e avisos.

Um exemplo de aviso é um evento no qual 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 Universal print driver usage como Use universal printing ou Use universal printing somente se o driver solicitado não estiver disponível.

Session printers

Essa configuração especifica as impressoras de rede que devem ser 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 **Use universal printing**. 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 Servidor de Impressão Windows ou em um Citrix Universal Print Server.

- **Servidor de Impressão Windows:** Compartilha uma ou mais impressoras de rede. Ele também tem os drivers de impressora nativos necessários para usar as impressoras de rede.
- **Servidor de Impressão Universal:** Um Servidor de Impressão Windows onde o software Citrix Universal Print Server foi instalado.

Ao usar um Servidor de Impressão Windows, o serviço Citrix Print Manager cria as conexões de impressora de rede usando drivers de impressora nativos. O servidor Citrix Virtual Apps deve ter os drivers de impressora nativos instalados nele.

Ao usar um 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 Driver de Impressão Universal.

Todos os drivers de impressora Windows atualmente se enquadram na versão do 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, faça o seguinte:

1. Entre no Web Studio, selecione **Policies** no painel esquerdo e clique na guia **Policies**.
2. Habilite a política **Session printers**.
3. Na política, adicione a impressora de sessão. Para adicionar impressoras, digite o caminho UNC da impressora que você deseja criar automaticamente. Depois de adicionar a impressora, você pode aplicar configurações personalizadas para a sessão atual em cada logon. A impressora de sessão deve ser exibida na lista.
4. Após a definição da política, o aplicativo publicado pode não exibir impressoras de sessão. Esse problema pode ocorrer porque o driver da impressora está ausente no servidor Citrix Virtual Apps ou a política foi criada, mas não ativada.

   > **Nota:**
   >
   > Se uma impressora de sessão precisar de um driver de impressora nativo e o driver de impressora nativo não estiver instalado no VDA, talvez a impressora de sessão não seja criada na sessão.

5. Inicie a área de trabalho publicada e adicione manualmente a impressora de sessão em **Dispositivos e Impressoras > Painel de controle**.

6. Se isso não der resultado, investigue a comunicação entre o servidor Citrix Virtual Apps e o servidor de impressão. Considere executar um teste com o RDP.

Wait for printers to be created

Use a política no Delivery Controller para ativar o recurso no Citrix Virtual Desktops.

Wait for printers to be created (Server Desktop):

Essa configuração permite inserir um atraso na conexão a uma sessão para que as impressoras redirecionadas para o cliente possam ser criadas automaticamente.

Por padrão, não ocorre nenhum atraso de conexão.

> **Nota:**
>
> Essa política é compatível com o Citrix Virtual Apps and Desktops versão 7.17 e posterior.

Configurações de política de impressoras cliente

June 28, 2023

A seção **Client Printers** inclui configurações de política para impressoras cliente, incluindo configurações para criar impressoras cliente automaticamente, manter as propriedades da impressora e conectar-se a servidores de impressão.

Auto-create client printers

Essa configuração especifica as impressoras cliente que são criadas automaticamente. Essa configuração substitui as configurações padrão de criação automática da impressora cliente.

Por padrão, todas as impressoras cliente são criadas automaticamente.

Essa configuração só se tornará ativa se a configuração **Client printer redirection** estiver presente e definida como **Allowed**.

Ao adicionar essa configuração a uma política, selecione uma opção:

- **Auto-create all client printers** cria automaticamente todas as impressoras em um dispositivo do usuário.
- **Auto-create the client's default printer only** cria automaticamente apenas a impressora selecionada como a impressora padrão no dispositivo do usuário.

- **Auto-create local (non-network) client printers only** cria automaticamente apenas impressoras diretamente conectadas ao dispositivo do usuário por meio de uma porta LPT, COM, USB, TCP/IP ou outra porta local.
- **Do not auto-create client printers** desativa a criação automática de todas as impressoras cliente quando os usuários fazem logon. A escolha desta opção faz com que as configurações de RDS (Serviços de Área de Trabalho Remota) para a criação automática de impressoras cliente substituam essa configuração nas políticas de prioridade mais baixa.

Auto-create generic universal printer

Essa configuração ativa ou desativa a criação automática do objeto genérico Citrix Universal Printer para sessões. Essas sessões incluem apenas as sessões em que um dispositivo de usuário compatível com a Impressão Universal está em uso.

Por padrão, o objeto Universal Printer genérico não é criado automaticamente.

As seguintes configurações de política são correlatas:

- Universal print driver usage
- Universal driver preference

Auto-create PDF universal printer

Essa configuração ativa ou desativa a criação automática da impressora Citrix PDF para sessões usando:

- Aplicativo Citrix Workspace para Windows (a partir do VDA 7.19)
- Aplicativo Citrix Workspace para HTML5
- Aplicativo Citrix Workspace para Chrome

Por padrão, a impressora Citrix PDF não é criada automaticamente.

Client printer names

Essa configuração seleciona a convenção de nomenclatura para impressoras cliente criadas automaticamente.

Por padrão, são usados os nomes de impressoras padrão.

Selecione **Standard printer names** para usar nomes de impressora, como "HPLaserJet 4 do nome do cliente na sessão 3".

Selecione **Legacy printer names** para usar nomes de impressora cliente de estilo antigo e preservar a compatibilidade com os nomes de impressoras legadas, conforme presente nas versões XenApp e XenDesktop do produto. Você pode usar essa opção com as versões atuais do Citrix Virtual Apps and Desktops do produto. Um exemplo de um nome de impressora legado é "Client/clientname#/HPLaserJet 4."Esta opção é menos segura.

Quando você usa a impressora Citrix PDF em uma sessão iniciada a partir do aplicativo Citrix Workspace para HTML5, defina a configuração **Client printer names** como padrão ou selecione **Standard printer names**. Se você selecionar **Legacy printer names**, o aplicativo Citrix Workspace para HTML5 não oferece suporte à opção Citrix PDF Printer.

Direct connections to print servers

Essa configuração ativa ou desativa conexões diretas dos aplicativos de hospedagem de servidor ou área de trabalho virtual a um servidor de impressão para impressoras cliente. Aqui, as impressoras cliente são hospedadas em um compartilhamento de rede acessível.

Por padrão, as conexões diretas são ativadas.

Ative conexões diretas se o servidor de impressão de rede não estiver em uma WAN a partir da área de trabalho virtual ou dos aplicativos de hospedagem de servidor. A comunicação direta resulta em impressão mais rápida se o servidor de impressão de rede e os aplicativos de hospedagem de servidor ou área de trabalho 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 pelo dispositivo do usuário onde são redirecionados para o servidor de impressão de rede. Os dados enviados para o dispositivo do usuário são compactados, portanto, é consumida menos largura de banda à medida que os dados viajam pela WAN.

Se duas impressoras de rede tiverem o mesmo nome, será usada a impressora na mesma rede que o dispositivo do usuário.

Printer driver mapping and compatibility

Essa configuração especifica as regras de substituição de driver para impressoras cliente criadas automaticamente.

Esta configuração é definida para excluir o Microsoft OneNote e o Gravador de Documentos XPS da lista de impressoras cliente criadas automaticamente.

Ao definir regras de substituição de driver, você pode permitir ou impedir que sejam criadas impressoras com o driver especificado. Além disso, você pode permitir que as impressoras criadas usem apenas drivers de impressão universais. A troca do driver substitui ou mapeia os nomes dos drivers

de impressora que o dispositivo do usuário fornece, substituindo um driver equivalente no servidor. Essas regras dão aos aplicativos de servidor acesso a impressoras cliente que têm os mesmos drivers que o servidor, mas nomes de driver diferentes.

Você pode fazer o seguinte:

- Adicionar um mapeamento de driver
- Editar um mapeamento existente
- Substituir configurações personalizadas de um mapeamento
- Remover um mapeamento
- Alterar a ordem das entradas do driver na lista

Ao adicionar um mapeamento, insira o nome do driver da impressora cliente e selecione o driver do servidor que deseja substituir.

Printer properties retention

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 de usuário.

Ao adicionar essa configuração a uma política, selecione uma opção:

- A opção Saved on the client device only é para dispositivos do usuário que têm um perfil obrigatório ou de roaming que não é armazenado. Escolha essa opção somente se todos os servidores em seu ambiente estiverem executando o XenApp 5 e posterior. Além disso, seus usuários estão usando o plug-in on-line Citrix versões 9 a 12.x ou Citrix Receiver 3.x.
- A opção Retained in user profile only é para dispositivos de usuário restritos pela largura de banda (esta opção reduz o tráfego de rede) e a velocidade de logon ou para usuários com plug-ins herdados. Esta opção armazena as propriedades da impressora no perfil de usuário no servidor e evita que qualquer troca de propriedades com o dispositivo do usuário. Use esta opção com o MetaFrame Presentation Server 3.0 ou anterior e MetaFrame Presentation Server Client 8.x ou anterior. Essa opção só é aplicável se for usado um perfil de roaming de Serviços de Área de Trabalho Remota (RDS).
- A opção Held in profile only if not saved on the client 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 de usuário. Embora esta opção seja a mais flexível, ela também pode retardar o tempo de logon e usar largura de banda extra para verificação do sistema.
- A opção Do not retain printer properties impede o armazenamento das propriedades da impressora.

Retained and restored client printers

Essa configuração ativa ou desativa a retenção e a recriação de impressoras no dispositivo do usuário. Por padrão, as impressoras cliente são retidas automaticamente e restauradas automaticamente.

As impressoras retidas são impressoras criadas pelo usuário que são criadas novamente ou lembradas no início da sessão seguinte. Quando o Citrix Virtual Apps recria uma impressora retida, ele considera todas as configurações de política, exceto a configuração **Criar impressoras cliente automaticamente**.

As impressoras restauradas são impressoras totalmente personalizadas por um administrador, com um estado salvo que está permanentemente conectado a uma porta do cliente.

Citrix PDF Universal Printer driver

O driver Citrix PDF Universal Printer permite aos usuários imprimir documentos abertos com aplicativos hospedados ou aplicativos executados em áreas de trabalho virtuais fornecidas pelo Citrix Virtual Apps and Desktops. Quando um usuário seleciona a opção **Citrix PDF Printer**, o driver converte o arquivo em PDF e transfere o PDF para o dispositivo local. Em seguida, o PDF é aberto para visualização e impressão a partir de uma impressora conectada localmente. PDF é um dos formatos suportados com Citrix Universal Printing (além do EMF e XPS).
A impressora PDF pode ser ativada, configurada e definida como padrão usando uma Política Citrix. A opção **Citrix PDF Printer** está disponível para usuários do aplicativo Citrix Workspace para Windows, Chrome e HTML5.

> **Nota:**
>
> É necessário um visualizador de PDF para pontos de extremidade do Windows. O cliente deve ter um aplicativo que tenha associação de tipo de arquivo registrada no Windows para abrir arquivos PDF.

Configurações de política de drivers

June 28, 2023

A seção **Drivers** inclui as configurações de política relacionadas aos drivers de impressora.

Automatic installation of in-box printer drivers

> **Nota**
>
> Esta política não suporta VDAs nesta versão.

Essa configuração ativa ou desativa a instalação automática de drivers de impressora a partir de:

- Conjunto de drivers nativos do Windows
- Pacotes de driver preparados no host usando `pnputil.exe /a`

Por padrão, esses drivers são instalados conforme necessário.

Universal driver preference

Essa configuração especifica a ordem em que os drivers de impressora universais são usados, começando com a primeira entrada na lista.

Por padrão, a ordem de preferência é:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Você pode adicionar, editar ou remover drivers e alterar a ordem dos drivers na lista.

Universal print driver usage

Essa configuração especifica quando usar a impressão universal.

Por padrão, a impressão universal é usada somente se o driver solicitado não estiver disponível.

A impressão universal emprega drivers de impressora genéricos em vez de drivers específicos do modelo padrão, potencialmente simplificando a carga do gerenciamento de drivers em computadores host. A disponibilidade de drivers de impressão universais depende dos recursos do dispositivo do usuário, host e software de servidor de impressão. Em determinadas configurações, a impressão universal pode não estar disponível.

Ao adicionar essa configuração a uma política, selecione uma opção da tabela a seguir:

Opção	Descrição
Use only printer model specific drivers	Especifica que a impressora cliente usa somente os drivers específicos do modelo padrão que são criados automaticamente durante o logon. Se o driver solicitado não estiver disponível, a impressora cliente não poderá ser criada automaticamente.
Use universal printing only	Especifica que nenhum driver padrão específico do modelo é usado. Somente drivers de impressão universais são usados para criar impressoras.
Use universal printing only if requested driver is unavailable	Usa drivers específicos do modelo padrão para 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.
Use printer model specific drivers only if universal printing is unavailable	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 da política Universal Print Server

June 28, 2023

A seção **Universal Print Server** inclui configurações de política para lidar com o servidor de impressão universal.

Pacote de codificação SSL (SSL cipher suite)

Essa configuração especifica o conjunto de pacotes de codificação SSL/TLS que são usados no Universal Print Client para conexões de fluxo de dados de impressão criptografada (CGP).

Para controlar o pacote de codificação usado pelo Universal Print Client para conexões de serviço web de impressão criptografado (HTTPS/SOAP), consulte [SCHANNEL].

Valor padrão: ALL

Essa configuração tem os seguintes valores: ALL, COM ou GOV.

Os pacotes de codificação correspondentes a cada valor são os seguintes:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL compliance mode

Essa configuração especifica o nível de conformidade com a Publicação Especial 800-52 do NIST que é usada pelo Universal Print Client para conexões criptografadas de fluxo de dados de impressão (CGP).

Valor padrão: None.

Essa configuração tem os seguintes valores:

Nenhuma.

As conexões criptografadas do fluxo de dados de impressão (CGP) usam o modo de conformidade padrão.

SP800-52.

As conexões criptografadas do fluxo de dados de impressão (CGP) usam o modo de conformidade NIST Special Publication 800-52.

SSL enabled

Essa configuração especifica se o SSL/TLS é usado pelo Universal Print Client para o seguinte:

- Conexões de fluxo de dados de impressão (CGP)
- Conexões de serviço Web (HTTP/SOAP)

Quando você define o **Universal Print Server enable** como **Enabled with fallback to Windows' native remote printing**, as conexões de reserva são feitas pelo Microsoft Windows Network Print Provider. Essa configuração não afeta essas conexões de fallback.

Valor padrão: Disabled

Essa configuração tem os seguintes valores:

Enabled.

O Universal Print Client usa SSL/TLS para se conectar ao Universal Print Server.

Disabled.

O Universal Print Client usa SSL/TLS para se conectar ao Universal Print Server.

SSL FIPS mode

Essa configuração especifica se o módulo criptográfico SSL/TLS usado pelo Universal Print Client para conexões de fluxo de dados de impressão (CGP) é executado no modo FIPS.

Valor padrão: Disabled

Essa configuração tem os seguintes valores:

Enabled.

O modo FIPS está ativado.

Disabled.

O modo FIPS está desligado.

SSL protocol version

Essa configuração especifica a versão do protocolo SSL/TLS usada pelo Universal Print Client.

Valor padrão: ALL

Essa configuração tem os seguintes valores:

ALL.

Use TLS versions 1.0, 1.1 or 1.2.

TLSv1.

Use TLS version 1.0.

TLSv1.1.

Use TLS version 1.1.

TLSv1.2.

Use TLS version 1.2.

Porta de fluxo de dados de impressão criptografada (CGP) do Universal Print Server SSL (SSL Universal Print Server encrypted print data stream (CGP) port)

Essa configuração especifica o número da porta TCP da porta CGP (CGP) criptografada do Universal Print Server. Esta porta recebe dados para trabalhos de impressão.

Valor padrão: 443

Porta de serviço web criptografada SSL Universal Print Server (HTTPS/SOAP)

Essa configuração especifica o número da porta TCP da porta do serviço web criptografado do Universal Print Server (HTTPS/SOAP). Esta porta recebe dados para comandos de impressão.

Valor padrão: 8443

Universal Print Server enable

Essa política ativa ou desativa o uso do Citrix Universal Print Server (UPS). Aplique essa configuração de política às unidades organizacionais (UOs) que incluem aplicativos de área de trabalho virtual ou de hospedagem de servidores. Essas configurações de política incluem opções de fallback para permitir conexões com servidores de impressão usando o serviço de impressão remota nativo do Windows no caso de o componente Citrix UPS não estar instalado ou não estar disponível no servidor de impressão solicitado. As alterações nesta política são aplicáveis somente após o VDA ser reiniciado.

Por padrão, o Universal Print Server está desativado.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- **Enabled with fallback to Windows native remote printing**: o Universal Print Server atende às conexões de impressora de rede, se possível. Se o Universal Print Server não estiver disponível, o Windows Print Provider será usado. O Windows Print Provider continua a lidar com todas as impressoras criadas anteriormente com o Windows Print Provider.
- **Enabled with no fallback to Windows native remote printing**: o Universal Print Server atende às conexões de impressora de rede exclusivamente. Se o Universal Print Server não estiver disponível, ocorrerá falha na conexão da impressora de rede. Essa configuração desativa efetivamente a impressão de rede por meio do Windows Print Provider. As impressoras criadas anteriormente com o Windows Print Provider não são criadas enquanto estiver ativa uma política que contém essa configuração.

- **Disabled**: o recurso Universal Print Server está desativado. Não é feita nenhuma tentativa de se conectar ao Universal Print Server durante a conexão a uma impressora de rede com um nome UNC. As conexões com impressoras remotas continuam a usar a instalação de impressão remota nativa do Windows.

Universal Print Server print data stream (CGP) port

Essa 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 definição de política apenas às unidades organizacionais que contenham o servidor de impressão.

Por padrão, o número da porta é definido como 7229.

Os números de porta válidos devem estar no intervalo de 1-65535.

Universal Print Server print stream input bandwidth limit (Kbps)

Essa configuração especifica o limite superior (em kilobits por segundo) para a taxa de transferência de dados de impressão. A taxa de transferência é calculada para os dados de impressão que são entregues de cada trabalho de impressão para o Universal Print Server usando CGP. Aplique esta configuração de política às unidades operacionais que contenham os aplicativos de hospedagem de servidor ou área de trabalho virtual.

Por padrão, o valor é 0, que não especifica nenhum limite superior.

Universal Print Server web service (HTTP/SOAP) port

Essa configuração especifica o número da porta TCP usado pelo ouvinte do serviço Web do Universal Print Server (HTTP/SOAP). O Universal Print Server é um componente opcional que permite o uso de drivers de impressão universal Citrix para cenários de impressão em rede.

Quando o Universal Print Server é usado, os comandos de impressão são enviados dos hosts Citrix Virtual Apps and Desktops para o Universal Print Server via SOAP via HTTP. Essa configuração modifica a porta TCP padrão na qual o Universal Print Server escuta solicitações HTTP/SOAP recebidas.

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 host não se conecta ao Universal Print Server. Essa 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 0-65535.

Universal Print Servers for load balancing

Essa configuração lista os Universal Print Servers que devem ser usados para balancear as conexões de impressora de balanceamento de carga estabelecidas na inicialização da sessão, depois de avaliar outras configurações de política de impressão 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.

Essa configuração também implementa a detecção de failover do servidor de impressão e a recuperação de conexões da impressora. Os servidores de impressão são verificados periodicamente quanto à disponibilidade. Se uma falha do servidor for detectada, esse servidor será removido do esquema de balanceamento de carga. Além disso, as conexões da impressora no servidor são redistribuídas entre outros servidores de impressão disponíveis. Quando o servidor de impressão com falha é recuperado, ele é retornado ao esquema de balanceamento de carga.

Clique em **Validate Servers** para verificar se cada servidor é um servidor de impressão, se a lista de servidores não incluem nomes de servidor duplicados e se todos os servidores têm um conjunto idêntico de impressoras compartilhadas instalado. Esta operação pode levar algum tempo.

Universal Print Servers out-of-service threshold

Essa configuração especifica por quanto tempo o balanceador de carga deve aguardar a recuperação de um servidor de impressão indisponível antes de determinar que o servidor está permanentemente offline e redistribua sua carga para outros servidores de impressão disponíveis.

Por padrão, o valor de limite é definido como 180 (segundos).

Universal Print Server web service (HTTP/SOAP) connect timeout

Essa configuração especifica o número de segundos que o Universal Print Client deve esperar até que a operação connect() do serviço web do Universal Print Server atinja o tempo limite. Essa configuração tem os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são em segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de conexão de soquete TCP. Os

soquetes são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Essa configuração era a configuração disponível presente nas versões anteriores do Universal Print Client antes da alteração.

O Universal Print Client é o componente do Virtual Delivery Agent (VDA) que se comunica com o Universal Print Server.

> **Nota:**
>
> Essa configuração de política é aplicável na versão 7.35 e posteriores do VDA.

Universal Print Server web service (HTTP/SOAP) receive timeout

Essa configuração especifica o número de segundos que o Universal Print Client deve esperar até que a operação recv() do serviço web do Universal Print Server atinja o tempo limite. Essa configuração tem os seguintes valores e todos elas são numéricos e as unidades (de tempo) são em segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de recebimento de soquete TCP. Os soquetes são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Essa configuração era a configuração disponível presente nas versões anteriores do Universal Print Client antes da alteração.

O Universal Print Client é o componente do Virtual Delivery Agent (VDA) que se comunica com o Universal Print Server.

> **Nota:**
>
> Essa configuração de política é aplicável na versão 7.35 e posteriores do VDA.

Universal Print Server web service (HTTP/SOAP) send timeout

Essa configuração especifica o número de segundos que o Universal Print Client deve esperar até que a operação send() do serviço web do Universal Print Server atinja o tempo limite. Essa configuração tem os seguintes valores. Todos esses valores são numéricos e as unidades (de tempo) são em segundos.

- O valor mínimo é 0.
- O valor máximo é 60.
- O valor padrão é 10.

Quando o tempo limite está entre 1 e 60 (inclusive), o Universal Print Client aguarda o tempo especificado para que a operação seja concluída. A operação é uma operação de envio de soquete TCP. Os soquetes são um recurso do sistema operacional Windows que permite a comunicação entre processos em redes TCP/IP.

Quando o tempo limite é 0, o Universal Print Client usa o tempo limite padrão definido pelo sistema operacional. Essa configuração era a configuração disponível presente nas versões anteriores do Universal Print Client antes da alteração.

O Universal Print Client é o componente do VDA que se comunica com o Universal Print Server.

> **Nota:**
>
> Essa configuração de política é aplicável na versão 7.35 e posteriores do VDA.

Configurações de política de impressão universal

June 28, 2023

A seção **Universal Printing** inclui configurações de política para gerenciar a impressão universal.

Universal printing EMF processing mode

Essa configuração controla o método de processamento do arquivo de spool EMF no dispositivo do usuário Windows.

Por padrão, os registros EMF são postos em spool diretamente para a impressora.

Ao adicionar essa configuração a uma política, selecione uma opção:

- Reprocess EMFs for printer força o arquivo de spool EMF a ser reprocessado e enviado através do subsistema GDI no dispositivo do usuário. Você pode usar essa configuração para drivers que exigem reprocessamento EMF, mas que podem não ser selecionados automaticamente em uma sessão.
- A opção Spool directly to printer, quando usada com o driver de impressão Citrix Universal, garante que os registros EMF sejam postos em spool e fornecidos ao dispositivo do usuário para processamento. Normalmente, esses arquivos do carretel 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.

Universal printing image compression limit

Essa configuração especifica o seguinte:

- Qualidade máxima disponível para imagens impressas com o driver de impressão universal Citrix
- Nível mínimo de compactação disponível para imagens impressas com o driver de impressão universal Citrix

Por padrão, o limite de compactação de imagem é definido como Best quality (lossless compression).

Se No Compression estiver selecionada, a compactação será desativada somente para impressão EMF.

Ao adicionar essa configuração a uma política, selecione uma opção:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)

Ao adicionar essa configuração a uma política que inclua a configuração **Universal printing optimization defaults**, esteja ciente do seguinte:

- Considere que o nível de compactação na configuração **Universal printing image compression limit** é inferior ao nível definido na configuração **Universal printing optimization defaults**. Nesse caso, as imagens são compactadas no nível definido na configuração de Universal printing image compression limit.
- Se a compactação estiver desativada, as opções Desired image quality e Enable heavyweight compression da configuração Universal printing optimization defaults não terão efeito na política.

Universal printing optimization defaults

Essa configuração especifica os valores padrão para a 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 Standard Quality está ativada, o que significa que os usuários só podem imprimir imagens usando compactação de qualidade padrão ou reduzida.

- Ativar a compactação intensa ativa ou desativa a redução da largura de banda além do nível de compactação definido pela qualidade de imagem desejada, sem perder a qualidade da imagem. Por padrão, a compactação intensa está desativada.
- As configurações de Image e Font Caching especificam se deve ser feito ou não o cache de imagens e fontes que aparecem várias vezes no fluxo de impressão. Essa configuração garante que cada imagem ou fonte exclusiva seja enviada para a impressora apenas uma vez. Por padrão, imagens incorporadas e fontes são armazenadas em cache. Essas configurações se aplicam somente se o dispositivo do usuário suportar esse comportamento.
- Allow non-administrators to modify these settings 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.

Nota: Todas estas opções são suportadas para a impressão EMF. Para impressão XPS, apenas a opção Desired image quality é suportada.

Ao adicionar essa configuração a uma política que inclua a configuração **Universal printing image compression limit**, esteja ciente do seguinte:

- Considere que o nível de compactação na configuração **Universal printing image compression limit** é inferior ao nível definido na configuração **Universal printing optimization defaults**. Nesse caso, as imagens são compactadas no nível definido na configuração de Universal printing image compression limit.
- Se a compactação estiver desativada, as opções Desired image quality e Enable heavyweight compression da configuração Universal printing optimization defaults não terão efeito na política.

Universal printing preview preference

Essa configuração especifica se deve ou não ser usada a função de visualização de impressão para impressoras universais criadas automaticamente ou genéricas.

Por padrão, a visualização de impressão não é usada para impressoras universais criadas automaticamente ou genéricas.

Ao adicionar essa configuração a uma política, selecione uma opção:

- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

Universal printing print quality limit

Essa configuração especifica o máximo de pontos por polegada (dpi) disponíveis para gerar saída impressa em uma sessão.

Por padrão, No Limit está ativado, o que significa que os usuários podem selecionar a qualidade de impressão máxima permitida pela impressora à qual se conectam.

Se essa configuração estiver definida, ela limita a qualidade máxima de impressão disponível para os usuários em termos de resolução de saída. Tanto a qualidade de impressão em si quanto os recursos de qualidade de impressão da impressora à qual o usuário se conecta estão restritos à configuração configurada.

Por exemplo, se configurado como Medium Resolution (600 DPI), os usuários podem imprimir a saída com uma qualidade máxima de 600 DPI somente. Além disso, a configuração de **Print Quality** na guia **Advanced** de **Universal Printer** mostra as configurações de resolução somente até e inclusive Medium Quality (600 DPI).

Ao adicionar essa configuração a uma política, selecione uma opção:

- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

Configurações da política de segurança

June 28, 2023

A seção **Security** inclui a configuração de política para configurar a criptografia de sessão e a criptografia de dados de logon.

SecureICA minimum encryption level

Essa configuração especifica o nível mínimo no qual criptografar os dados de sessão enviados entre o servidor e um dispositivo de usuário.

Importante: No Virtual Delivery Agent 7.x, essa configuração de política só pode ser usada para habilitar a criptografia dos dados de logon com criptografia RC5 de 128 bits. Outras configurações são fornecidas apenas para compatibilidade com versões anteriores do Citrix Virtual Apps and Desktops.

Para o VDA 7.x, a criptografia de dados da sessão é definida usando as configurações básicas do grupo de entrega do VDA. Se Enable Secure ICA estiver selecionado para o grupo de entrega, os dados da sessão serão criptografados usando criptografia RC5 (128 bits). Se Enable Secure ICA não estiver 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:

- A opção Basic criptografa a conexão do cliente usando um algoritmo não RC5. Ela protege o fluxo de dados de ser lido diretamente, mas pode ser descriptografada. Por padrão, o servidor usa criptografia básica para tráfego cliente-servidor.
- O logon RC5 (128 bits) criptografa somente os dados de logon usando criptografia RC5 128 bits e a conexão do cliente usando criptografia básica.
- RC5 (40 bits) criptografa a conexão do cliente usando criptografia RC5 de 40 bits.
- O RC5 (56 bit) criptografa a conexão do cliente usando a criptografia RC5 de 56 bits.
- RC5 (128 bits) criptografa a conexão do cliente usando criptografia RC5 128 bits.

As configurações especificadas para criptografia cliente-servidor podem interagir com quaisquer outras configurações de criptografia no ambiente e no sistema operacional Windows. Considere que um nível de criptografia de prioridade mais alta está definido em um servidor ou dispositivo de usuário. Nesse caso, as configurações especificadas para os recursos publicados podem ser substituídas.

Você pode aumentar os níveis de criptografia para proteger ainda mais as comunicações e a integridade da mensagem para determinados usuários. Se uma política exigir um nível de criptografia mais alto, a conexão por meio de um nível de criptografia mais baixo será negados aos Citrix Receivers.

SecureICA não executa autenticação nem verifica a integridade dos dados. Para fornecer criptografia de ponta a ponta para seu site, use SecureICA com criptografia TLS.

SecureICA não usa algoritmos compatíveis com FIPS. Se essa configuração for um problema, configure o servidor e o Citrix Receivers para evitar o uso do SecureICA.

O SecureICA usa a codificação de bloco RC5 conforme descrito no RFC 2040 para confidencialidade. O tamanho do bloco é de 64 bits (um múltiplo de unidades de palavras de 32 bits). O comprimento da chave é 128 bits. O número de rodadas é 12.

As chaves para a codificação de bloco RC5 são negociadas quando uma sessão é criada. A negociação é realizada usando o algoritmo Diffie-Hellman. Essa negociação usa parâmetros públicos Diffie-Hellman. Esses parâmetros são armazenados no registro do Windows quando o Virtual Delivery Agent é instalado. Parâmetros públicos não são secretos. O resultado da negociação Diffie-Hellman é uma chave secreta, da qual as chaves de sessão para a codificação de bloco RC5 são derivadas. Chaves de sessão separadas são usadas para logon do usuário e transferência de dados. Além disso, chaves de sessão separadas são usadas para 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. Vetores de inicialização para a codificação de bloco RC5 também são derivados da chave secreta.

Configurações de política de limites do servidor

June 28, 2023

A seção **Server Limits** inclui a configuração de política para controlar conexões ociosas.

Server idle timer interval

Essa configuração determina quanto tempo uma sessão de usuário ininterrupta é mantida se não houver entrada do usuário. Os dados são calculados em milissegundos.

Por padrão, as conexões ociosas não são desconectadas (intervalo de temporizador ocioso do servidor = 0). A Citrix recomenda definir esse valor com um mínimo de 60000 milissegundos (60 segundos).

Para exibir a política, selecione **Multiple Versions**, desmarque as versões do SO de sessão única e selecione **Server Limit**.

> **Nota**
>
> Quando esta configuração de política é usada, uma caixa de diálogo "Timer de ociosidade expirado"pode aparecer para os usuários quando a sessão tiver permanecido ociosa durante o tempo especificado. As configurações de política do Citrix não controlam essa 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

June 28, 2023

A seção **Session Limits** inclui configurações de política que controlam quanto tempo as sessões permanecem conectadas antes de serem forçadas a fazer logoff.

Disconnected session timer

Essa configuração ativa ou desativa um temporizador que especifica por quanto tempo uma área de trabalho desconectada e bloqueada permanece bloqueada antes que seja feito o logoff da sessão.

Se este timer for ativado, será feito o logoff da sessão desconectada quando o timer expirar.

Por padrão, não é feito o logoff das sessões desconectadas.

Remote PC Access disconnected session timer

Essa configuração ativa ou desativa um timer que faz logoff de uma sessão de usuário desconectada após o timer expirar. Se você ativar essa configuração, use **Disconnected session timer interval** para especificar quantos minutos uma área de trabalho desconectada permanece bloqueada antes que seja feito o logoff da sessão do usuário.

Por padrão, essa configuração está desativada.

Disconnected session timer interval

Essa configuração especifica quantos minutos uma área de trabalho desconectada e bloqueada permanece bloqueada antes que seja feito o logoff da sessão.

Por padrão, o período de tempo é de 1.440 minutos (24 horas).

Disconnected session timer –Multi-session

Essa configuração ativa ou desativa um timer para determinar por quanto tempo uma sessão do RDS desconectada pode persistir antes que seja feito o logoff da sessão. Por padrão, o timer fica desativado e não é feito logoff das sessões desconectadas.

Disconnected session timer interval –Multi-session

Essa configuração determina quantos minutos uma sessão do RDS desconectada pode persistir antes que seja feito o logoff da sessão. Por padrão, o período de tempo é de 1440 minutos (24 horas).

Session connection timer

Essa configuração ativa ou desativa um timer que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo do usuário e uma área de trabalho. Se este timer estiver ativado, a sessão será desconectada ou será feito o logoff quando o timer expirar. A configuração de **Encerrar sessão quando os limites de tempo forem atingidos** determina o próximo estado para a sessão.

Por padrão, este timer é desativado.

Session connection timer interval

Essa configuração especifica o número máximo de minutos para uma conexão ininterrupta entre um dispositivo de usuário e uma área de trabalho.

Por padrão, a duração máxima é de 1.440 minutos (24 horas).

Session connection timer –Multi-session

Essa configuração ativa ou desativa um timer que especifica a duração máxima de uma conexão ininterrupta entre um dispositivo do usuário e um servidor de terminal. Por padrão, este timer é desativado.

Session connection timer interval –Multi-session

Essa configuração especifica o número máximo de minutos de uma conexão ininterrupta entre um dispositivo de usuário e uma sessão RDS. Por padrão, a duração máxima é de 1440 minutos (24 horas).

Session idle timer

Quando um usuário não fornece nenhuma entrada, essa configuração é usada para habilitar ou desabilitar:

- Um timer que especifica por quanto tempo uma conexão ininterrupta do dispositivo do usuário a uma área de trabalho é mantida.

Quando este timer expira, a sessão é colocada no estado desconectado e aplica-se o que está definido por **Disconnected session timer**. Se a opção **Disconnected session timer** estiver desativada, não será feito o logoff da sessão.

Por padrão, esse timer está habilitado.

Session idle timer interval

Quando não há entrada do usuário, esta configuração é usada para especificar:

- O número de minutos durante os quais uma conexão ininterrupta do dispositivo do usuário com uma área de trabalho é mantida.

Por padrão, as conexões ociosas são mantidas por 1.440 minutos (24 horas).

Session idle timer –Multi-session

Essa configuração ativa ou desativa um timer para determinar a duração máxima de uma conexão ociosa entre um dispositivo de usuário e um servidor de terminal. Por padrão, este timer é desativado.

Session idle timer interval–Multi-session

Essa configuração especifica o número de minutos de uma conexão ociosa entre um dispositivo de usuário e uma sessão do RDS. Por padrão, a duração máxima é de 1440 minutos (24 horas).

> **Nota:**
>
> As configurações do timer de máquinas multissessão definidas usando as políticas Citrix devem substituir as configurações do timer definidas por meio das Políticas de Grupo da Microsoft. Para evitar comportamentos inesperados, recomendamos que você defina as configurações do timer usando um dos dois métodos.

Configurações da política de confiabilidade da sessão

June 28, 2023

A seção **session reliability** inclui configurações de política para gerenciar conexões de confiabilidade de sessão.

Session reliability connections

Essa configuração permite ou impede que as sessões sejam mantidas abertas durante uma perda de conectividade de rede. A confiabilidade da sessão, juntamente com a reconexão automática do cliente, permite que os usuários se reconectem automaticamente às sessões de aplicativos do Citrix Workspace após se recuperarem de interrupções de rede. Por padrão, a confiabilidade da sessão é Allowed.

As configurações no Web Studio são aplicadas no cliente para o seguinte:

- Aplicativo Citrix Workspace 1808 e posterior
- Citrix Receiver para Windows 4.7 e posterior.

A política do Web Studio substitui o objeto de política de grupo do Citrix Receiver nos clientes. As atualizações dessas políticas no Web Studio sincronizam a confiabilidade da sessão de servidor para cliente.

> **Nota:**
>
> - Citrix Receiver para Windows 4.7 e posterior e aplicativos Citrix Workspace para Windows - Defina a política no Web Studio.
> - Citrix Receivers para Windows anteriores a 4.7 - Defina políticas no Web Studio. Também defina o modelo de objeto de política de grupo do Citrix Receiver no cliente para um com-

> portamento 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 está perdida, a exibição do usuário torna-se opaca. O usuário pode ver uma sessão congelada durante a interrupção. O usuário pode continuar a interagir com o aplicativo quando a conexão de rede for restaurada. A confiabilidade da sessão reconecta usuários sem alertas de reautenticação.

Se você usa a confiabilidade da sessão e a reconexão automática de cliente, os dois recursos funcionam em sequência. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração de tempo limite de confiabilidade da sessão. Depois disso, as configurações de reconexão automática de cliente entram em vigor, tentando reconectar o usuário à sessão desconectada.

Por padrão, a confiabilidade da sessão é Allowed.

> **Nota:**
>
> Quando o Citrix ADC está em uso, você deve selecionar **Enable session reliability** em Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority** para o proxy das conexões ICA.

Session reliability port number

Essa configuração especifica o número da porta TCP para conexões de confiabilidade de sessão de entrada.

Por padrão, o número da porta é definido como 2598.

Session reliability timeout

Essa configuração especifica o tempo, em segundos. Esse tempo é o período que o proxy de confiabilidade da sessão espera até que um usuário se reconecte antes de permitir que a sessão seja desconectada.

Embora você possa estender a quantidade de tempo que uma sessão é mantida aberta, esse recurso é uma conveniência e não solicita ao usuário para reautenticação. Quanto mais tempo uma sessão estiver aberta, as chances aumentam de que um usuário pode deixar o dispositivo autônomo sem vigilância e potencialmente acessível a usuários não autorizados.

Por padrão, o tempo limite é definido como 180 segundos, ou três minutos.

Configurações da política de marca d'água

June 28, 2023

A seção **session watermark** inclui configurações de política para configurar esse recurso.
Ativar esse recurso causa um aumento significativo na largura de banda de rede e no uso da CPU pela máquina VDA. Recomendamos que você configure a marca d'água da sessão para máquinas VDA selecionadas com base nos recursos de hardware disponíveis.

> **Importante**
>
> Ative a marca d'água da sessão para que as outras configurações de política de marca d'água sejam efetivas. Para obter uma melhor experiência do usuário, não ative mais de dois itens de texto de marca d'água.

Enable session watermark

Quando você habilita essa configuração, a exibição da sessão tem uma marca d'água de texto opaca que exibe informações específicas da sessão. As outras configurações de marca d'água dependem de esta estar ativada.

Por padrão, a marca d'água da sessão está desativada.

Include client IP address

Quando você habilita essa configuração, a sessão exibe o endereço IP do cliente atual como uma marca d'água.

Por padrão, a opção Include client IP address está desativada.

Include connection time

Quando você habilita essa configuração, a marca d'água da sessão exibe um tempo de conexão. O formato é aaaa/mm/dd hh:mm. A hora exibida é baseada no relógio do sistema e no fuso horário.

Por padrão, a opção Include connection time está desativada.

Include logon user name

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 20 caracteres no máximo. Quando um nome de usuário tem mais de 20 caracteres, as fontes podem ter um tamanho excessivamente pequeno ou pode ocorrer truncamento, o que diminui a eficácia da marca d'água.

Por padrão, a opção Include logon user name está desativada.

Incluir o nome do host VDA

Quando você habilita essa configuração, a sessão exibe o nome do host VDA da sessão atual do ICA como uma marca d'água.

Por padrão, a opção Include VDA host name está ativada.

Include VDA IP address

Quando você habilita essa configuração, a sessão exibe o endereço IP da sessão ICA atual como uma marca d'água.

Por padrão, a opção VDA IP address está desativada.

Session watermark style

Essa configuração controla se você exibe um único rótulo de texto de marca d'água ou vários rótulos. Escolha **Multiple** ou **Single** do menu suspenso **Value**.

Vários exibe cinco rótulos de marca d'água na sessão. Um no centro e quatro nos cantos.

Single exibe um único rótulo de marca d'água no centro da sessão.

Por padrão, Session watermark style é Multiple.

Watermark custom text

Essa configuração permite aplicar texto personalizado (por exemplo, o nome corporativo) a ser exibido na marca d'água da sessão. Quando você configura uma string não vazia, ela exibe o texto em uma nova linha e acrescenta outras informações ativadas na marca d'água. O texto personalizado da marca d'água é limitado a 25 caracteres Unicode. Se você configurar uma string mais longa, ela será truncada em 25 caracteres.

Não há texto padrão.

A partir do Citrix Virtual Apps and Desktops 7 2206, você pode personalizar ainda mais usando marcas personalizadas no texto. Como resultado, o número máximo de caracteres no texto personalizado aumentou para 1024.

As marcas disponíveis para configurações de marca d'água estão descritas na tabela a seguir:

Marca	Descrição	Exemplo
`<font=value>`	Permite que você altere a fonte do texto da marca d'água. O valor é o nome de uma fonte disponível no VDA.	`<font=Courier New>`
`<fontzoom=value>`	Permite que você defina a porcentagem do fator de zoom da fonte. O valor é 200 para zoom de 200% no texto da marca d'água.	`<fontzoom=200>`
`<position=value>`	Permite que você altere a posição do texto da marca d'água. Os valores são `center`, `topleft`, `topright`, `bottomleft` e `bottomright`. Essa marca só é aplicável com um único estilo.	`<position=topright>`
`<rotation=value>`	Permite que você gire o texto da marca d'água. O valor é especificado em graus e o intervalo é de -360 e 360.	`<rotation=45>`
`<style=value>`	Permite que você altere o estilo de exibição. Essa marca substitui a política Session watermark style.	`<style=single>`

Os seguintes estilos de marca d'água estão disponíveis:

- Single style –Um único rótulo de texto de marca d'água aparece no centro da sessão. Você pode usar a marca de posição para alterar a localização.
- xstyle ou multiple –Cinco rótulos de marca d'água aparecem na sessão: um no centro e um em cada canto.
- Tile –Vários rótulos aparecem na sessão. O texto da marca d'água ocupa toda a tela, por igual.

As marcas disponíveis para alterar o texto da marca d'água estão descritas na tabela a seguir:

Marca	Descrição
<clientip>	O endereço IP do ponto de extremidade.
<date>	A data em que a sessão foi estabelecida.
<domain>	O nome de domínio da conta de usuário conectada.
<hostname>	O nome da máquina do VDA.
<newline>	Cria uma linha extra.
<serverip>	O endereço IP do VDA.
<time>	A hora em que a sessão foi estabelecida.
<username>	O nome do usuário.

> **Nota:**
>
> - A política **Watermark custom text** só entra em vigor quando a política **Enable session watermark** está ativada. Seu valor padrão é *Disabled*.
> - Se você usar as marcas para alterar o texto da marca d'água, todas as outras políticas de marca d'água de sessão, exceto **Enable session watermark**, serão ignoradas. Se você usar as marcas para configurações de texto da marca d'água, poderá usar todas as outras políticas de marca d'água.

Watermark transparency

Você pode especificar a opacidade da marca d'água de 0 a 100. Quanto maior o valor especificado, mais opaca a marca d'água.

Por padrão, o valor é 17.

Configurações da política de controle de fuso horário

June 28, 2023

A seção **Time Zone Control** inclui configurações de política relacionadas ao uso da hora local nas sessões.

Estimate local time for legacy clients

Essa configuração ativa ou desativa a estimativa do fuso horário local dos dispositivos do usuário. Esses dispositivos incluem os dispositivos do usuário que enviam informações imprecisas de fuso horário ao servidor.

Por padrão, o servidor estima o fuso horário local quando necessário.

Essa configuração destina-se a ser usada com clientes Citrix Receivers ou ICA legados que não enviam informações detalhadas de fuso horário para o servidor. Considere que essa configuração é usada com Citrix Receivers que enviam informações detalhadas de fuso horário para o servidor. Por exemplo, versões compatíveis do Citrix Receiver para Windows. Nesse caso, essa configuração não tem efeito.

Restore desktop OS time zone on session disconnect or logoff

Considere que o usuário desconecta ou faz logoff de uma sessão. Nesse caso, essa configuração determina se a configuração de fuso horário de um VDA com SO de sessão única é restaurada para o fuso horário original da máquina. Se você ativar 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 a opção **Use local time of client** como **Use client time zone**.

Por padrão, essa configuração está ativada.

Use local time of client

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, é usado o fuso horário da sessão do usuário.

Para que essa configuração entre em vigor, ative a configuração **Allow time zone redirection** no Editor de Política de Grupo. A configurações está em **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Device and Resource Redirection**.

Se você estiver usando o VDA de sessão única (anteriormente conhecido como Workstation VDA) em máquinas que executam um sistema operacional de servidor, configure o usuário local corretamente **Change the time zone** para **Everyone**. Este direito de usuário pode ser encontrado em **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.

> **Nota:**
>
> Em um sistema operacional de sessão única, os **Users** são incluídos na atribuição de direitos de usuário **Change the time zone**, embora não em um SO multissessão. Em um SO multissessão, o fuso horário é sincronizado por meio da seguinte política de grupo: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow timezone redirection. Esta política se aplica quando o Servidor é um Host de Sessão de Área de Trabalho Remota no VDA de SO multissessão (instalado com o comando `/ServerVDI`). Em um SO multissessão, por padrão e por design, os usuários não têm o direito local de alterar o fuso horário.

Configurações da política de dispositivos TWAIN

June 28, 2023

A seção **TWAIN devices** inclui configurações de política relacionadas ao seguinte:

- Mapeamento de dispositivos TWAIN cliente, como câmeras digitais ou scanners
- Transferências de imagens otimizadas do servidor para o cliente

> **Nota:**
>
> O TWAIN 2.0 é compatível com o Citrix Receiver para Windows 4.5.

Client TWAIN device redirection

Os dispositivos TWAIN se comunicam com aplicativos de processamento de imagem hospedados pelo servidor usando o protocolo TWAIN.

Essa configuração permite ou impede que os usuários acessem dispositivos TWAIN no dispositivo do usuário. Por padrão, o redirecionamento do dispositivo TWAIN é permitido.

As seguintes configurações de política são correlatas:

- TWAIN compression level
- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent

TWAIN compression level

Essa configuração especifica o nível de compactação das transferências de imagem do cliente para o servidor. Use Low para melhor qualidade de imagem, Medium para boa qualidade de imagem, ou

High para baixa qualidade de imagem. Por padrão, a compactação Medium é aplicada.

Configurações de política de dispositivos USB

June 28, 2023

A seção **USB devices** inclui configurações de política para gerenciar o redirecionamento de arquivos para dispositivos USB.

Client USB device optimization rules

As regras de otimização do dispositivo 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 de **USB policy** autorizam o dispositivo. Se o dispositivo for permitido, o host verificará as **Client USB device optimization rules** 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 têm desempenho degradado em relação à latência mais alta, os administradores podem habilitar o modo interativo (02). Veja descrições dos modos disponíveis na tabela neste artigo.

É bom saber

- Para o uso de tablets e mesas gráficas para assinatura Wacom, recomendamos que você desative o protetor de tela. Passos sobre como desativar o protetor de tela estão no final desta seção.
- O suporte para a otimização da série de produtos com tablet e mesas gráficas para assinatura Wacom STU foi pré-configurado na instalação das políticas Citrix Virtual Apps and Desktops.
- Os dispositivos de assinatura funcionam nos Citrix Virtual Apps and Desktops e não exigem que um driver seja usado como dispositivo de assinatura. A Wacom tem mais softwares que podem ser instalados para personalizar o dispositivo ainda mais. Veja http://www.wacom.com/.
- Tablets de desenho. Determinados dispositivos de entrada de desenho podem apresentar como um dispositivo HID em barramentos PCI/ACPI e não têm suporte. Conecte esses dispositivos em um controlador de host USB no cliente para que seja redirecionado dentro de uma sessão do Citrix Virtual Desktops.

As regras de política assumem o formato das expressões tag=expressões de valor separadas por espaços em branco. As seguintes marcas têm suporte:

Nome da marca	Descrição
Modo	O modo de otimização é suportado para dispositivos de entrada para class=**03**. Os modos suportados são: Sem otimização - valor **01**. Modo interativo - valor **02**. Recomendado para dispositivos como tablets de caneta e mouses 3D Pro. Modo de captura - valor **04**. Preferido para dispositivos como mesas gráficas para assinatura.
VID	ID do fornecedor do descritor de 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 de dispositivo, como um número hexadecimal de quatro dígitos.
Class	Classe do descritor de dispositivo ou de um descritor de interface.
SubClass	Subclasse do descritor de dispositivo ou de um descritor de interface.
Prot	Protocolo do descritor de dispositivo ou de um descritor de interface

Exemplos

Mode=00000004 VID=067B PID=1230 class=03 #Entrada do dispositivo operando no modo de captação

Mode=00000002 VID=067B PID=1230 class=03 #Entrada dispositivo operando no modo interativo (padrão)

Mode=00000001 VID=067B PID=1230 class=03 #Entrada dispositivo operando sem qualquer otimização

Mode=00000100 VID=067B PID=1230 # Otimização da configuração do dispositivo desabilitada (padrão)

Mode=00000200 VID=067B PID=1230 # Otimização da configuração do dispositivo habilitada

Desativar o protetor de tela para dispositivos com mesa gráfica para assinatura Wacom

Para o uso de tablets e mesas gráficas para assinatura Wacom, a Citrix recomenda que você desative o protetor de tela da seguinte forma:

1. Instale o **Wacom-STU-Driver** depois de redirecionar o dispositivo.
2. Instale o **Wacom-STU-display MSI** para obter acesso ao painel de controle da mesa gráfica para assinatura.
3. Acesse **Painel de controle > Wacom STU Display > STU430** ou **STU530** e selecione a guia do seu modelo.
4. Escolha **Change**, em seguida, selecione **Yes** quando a janela de segurança UAC aparecer.
5. Selecione **Disable slideshow** e, em seguida, **Apply**.

Depois que a configuração é definida para um modelo de mesa gráfica para assinatura, ela é aplicada a todos os modelos.

Client USB device redirection

Esta configuração permite ou impede o redirecionamento de dispositivos USB de e para o dispositivo do usuário.

Por padrão, os dispositivos USB não são redirecionados.

Client USB device redirection rules

Essa configuração especifica as regras de redirecionamento para dispositivos USB.

Por padrão, nenhuma regra é especificada.

Quando um usuário conecta um dispositivo USB, o dispositivo host verifica-o em relação a cada regra de política, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada definitiva. Se a primeira correspondência for uma regra Allow, o dispositivo será remoto para a área de trabalho virtual. Se a primeira correspondência for uma regra Deny, o dispositivo estará disponível apenas para a área de trabalho local. Se nenhuma correspondência for encontrada, serão usadas as regras padrão.

As regras de política assumem o formato {Allow:|Deny:} seguido por um conjunto de expressões tag=expressões de valor separadas por espaço em branco. As seguintes marcas têm suporte:

Nome da marca	Descrição
VID	ID do fornecedor do descritor de dispositivo

Nome da marca	Descrição
PID	ID do produto do descritor do dispositivo
REL	Liberar ID do descritor de dispositivo
Class	Classe do descritor de dispositivo ou de um descritor de interface
SubClass	Subclasse do descritor de dispositivo ou de um descritor de interface
Prot	Protocolo do descritor de dispositivo ou de um descritor de interface

Ao criar regras de política, lembre-se:

- As regras não diferenciam maiúsculas e minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por #.
- As linhas em branco ou puramente de comentários são ignoradas.
- As tags devem usar o operador correspondente = (por exemplo, VID=067B_.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.
- Veja os códigos de classe USB disponíveis no site USB Implementers Forum, Inc.

Exemplos de regras de política USB definidas pelo administrador:

- Allow: VID=067B PID = 0007 # Outra empresas, outra unidade Flash
- Deny: Class=08 subclass=05 # Armazenamento em massa
- Para criar uma regra que negue todos os dispositivos USB, use “DENY:”sem outras tags.

Redirecionamento do dispositivo plug and play USB do cliente

Essa configuração permite ou evita 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 do dispositivo plug-and-play é permitido. Quando definido como Allowed, todos os dispositivos plug-and-play para um usuário ou grupo específico são redirecionados. Quando definido como Prohibited, nenhum dispositivo é redirecionado.

Configurar o redirecionamento automático de dispositivos USB

Os dispositivos USB são redirecionados automaticamente quando o suporte a USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar dispositivos USB automaticamente.

> **Nota:**
>
> No Receiver for Windows 4.2, os dispositivos USB também são redirecionados automaticamente quando operam no modo de dispositivo de área de trabalho. Além disso, a barra de conexão não está presente. Nas versões anteriores do Citrix Receiver for Windows, os dispositivos USB também são redirecionados automaticamente quando operam da seguinte forma:
>
> - Modo de dispositivo de área de trabalho
> - Aplicativos hospedados em máquinas virtuais (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 ponto de extremidade do cliente ou na política DDC. Consulte Guias de Administração para obter mais detalhes.

> **Cuidado:**
>
> Usar o Editor do Registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Configurações de preferências do usuário para redirecionamento automático de dispositivos USB

Política:

1. Abra **Local Group Policy Editor** e vá até **Administrative Templates > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**.
2. Abra **New USB Devices**, selecione **Enabled** e clique em **OK**.
3. Abra **Existing USB Devices**, selecione **Enabled** e clique em **OK**.

Citrix Receiver:

1. Vá para **Citrix Receiver Preferences > Connections**.
2. As seguintes opções devem ser selecionadas:
   - When a session starts, connect devices automatically
   - When a new device is connected while a session is running, connect the device automatically.
3. Clique em **OK**.

Todas as chaves de registro e as alterações de política são aplicadas ao dispositivo cliente Windows.

Redirecionamento de impressoras USB simples

A melhor solução para impressoras USB simples é usar o driver de impressora universal dedicado e o canal virtual para executar a impressão. Por padrão, as impressoras USB simples não são redirecionadas automaticamente.

Impressoras simples são detectadas usando heurística. As impressoras avançadas com funções de digitalização, por exemplo, provavelmente precisarão ser redirecionadas usando o suporte a USB para funcionar completamente.

Use este registro para configurar se as impressoras simples devem ser redirecionadas automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectPrinters

Tipo: DWORD

Dados: 00000000

O valor padrão é 0 (não redireciona automaticamente). Alterar o valor para qualquer número maior que zero permite que o suporte USB redirecione impressoras USB simples.

Você também pode implantar políticas do Active Directory nesta chave de registro e substituir o valor de não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectAudio

Tipo: DWORD

Dados: 00000000

Redirecionamento de dispositivos de áudio simples

Como ocorre com as impressoras simples, o usuário tem mais vantagens se for utilizado o canal virtual de áudio dedicado do ICA para enviar dados de áudio a partir de dispositivos de áudio simples. No entanto, talvez seja necessário redirecionar alguns dispositivos especiais usando o suporte USB. É usada a heurística para determinar quais dispositivos são dispositivos de áudio simples.

Use este registro para configurar se os dispositivos de áudio simples devem ser 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). Se o valor for diferente de zero, os dispositivos de áudio USB simples com suporte USB são direcionados.

Você pode usar as políticas do Active Directory para implantar esse valor na chave do Registro e substituir o valor de 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 por meio do canal virtual dedicado, como o mapeamento da unidade cliente que também executa a otimização. Além de simples leitura ou gravação de arquivos, para executar certas tarefas especiais, como gravar um CD/DVD ou acessar dispositivos de sistemas de arquivos criptografados, o dispositivo ainda pode precisar ser redirecionado por meio do suporte USB genérico.

É usada a heurística para determinar quais dispositivos são dispositivos de armazenamento simples. Use esta chave de registro para configurar se os dispositivos de armazenamento simples são redirecionados automaticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectStorage

Tipo: DWORD

Dados: 00000000

O padrão é definido como 0 (não redireciona automaticamente). Alterando o valor para diferente de zero, redireciona dispositivos de armazenamento USB simples usando suporte USB genérico.

Você também pode usar as políticas do Active Directory para implantar esse valor na seguinte chave do Registro e substituir o valor de 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 genérico de USB, quando for configurável se estiver usando o CDM.

Unidades flash USB com redirecionamento de criptografia de hardware

As unidades flash USB com criptografia de hardware geralmente consistem em uma partição de armazenamento criptografada e uma segunda partição de *utilitário* que contém um utilitário para desbloquear a partição criptografada. No caso dispositivos USB Flash Drive, é possível oferecer a melhor experiência do usuário usando o mapeamento de unidade cliente dedicado/mapeamento dinâmico de unidade de miniatura HDX canal virtual que também executa otimização.

O redirecionamento genérico de USB é necessário para o seguinte:

- Clientes não Windows (por exemplo, clientes Linux)
- Clientes em que o cliente restringiu (bloqueou) o acesso do usuário às funções locais no cliente

O redirecionamento USB genérico pode redirecionar qualquer dispositivo de armazenamento USB sem criptografia de hardware para as sessões de VDA de SO de sessão única e SO multissessão.

Antes do Citrix Virtual Apps and Desktops 7 1808, as unidades flash USB com criptografia de hardware não podiam ser redirecionadas de forma útil para as sessões de VDA de SO de sessão única ou SO multissessão. Um novo aprimoramento de recursos introduzido no Citrix Virtual Apps and Desktops 7 1808 oferece suporte ao redirecionamento USB genérico de drives flash USB com criptografia de hardware em sessões de VDA de SO de sessão única e SO multissessão.
Depois que o dispositivo é reorientado, nenhuma de suas unidades aparece no cliente local. Então, se o desbloqueio da unidade for necessário, execute-o na sessão. Esse recurso requer a atualização do Windows KB4074590.

Dispositivos simples de imagem estática (scanners e câmeras digitais)

Para dispositivos simples de imagem estática, 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. Considere se um dispositivo não está em conformidade ou não está sendo usado de acordo com as intenções originais. Nesse caso, o redirecionamento USB genérico pode ser a única maneira de usar o dispositivo. É usada a heurística para determinar quais dispositivos são dispositivos de imagem estática.

Use esta chave de registro para configurar se os dispositivos de imagem estática simples devem ser 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). Alterando o valor para diferente de zero, redireciona dispositivos de imagem fixa USB simples com USB genérico.

Você também pode usar políticas do Active Directory para implantar esse valor nesta chave do Registro e substituir o valor de não-política se ambos estiverem presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nome: AutoRedirectImage

Tipo: DWORD

Dados: 00000000

Configurações específicas do dispositivo

As heurísticas usadas para selecionar dispositivos otimizáveis Citrix nem sempre correspondem ao que você deseja. Exemplos de dispositivos otimizáveis Citrix são impressoras, dispositivos de áudio, vídeo, armazenamento e imagens estáticas. Talvez você queira controlar o redirecionamento automático de dispositivos que não estão listados acima. Você pode controlar o redirecionamento automático em uma base específica do dispositivo.

Por exemplo, o leitor de código de barras DemoTech 2,000 não precisa ser redirecionado por meio do suporte USB. Ele dispõe de um identificador de fornecedor de 12AB e um identificador de produto de 5678. Estes 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 do fornecedor e do produto.

Você também pode implantar esse valor usando as políticas do Active Directory para essa chave de registro. Ele substitui o valor da 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 específicas do AutoRedirect do dispositivo têm precedência sobre os valores mais gerais do AutoRedirectXXX explicados acima. A heurística padrão para dispositivos otimizados Citrix pode interpretar um dispositivo como genérico erroneamente. Portanto, defina o valor específico do AutoRedirect do dispositivo como 1 para redirecioná-lo automaticamente.

Allow existing USB devices to be automatically connected

Essa configuração permite ou impede a conexão automática dos dispositivos USB existentes que estão conectados ao ponto de extremidade no início de uma sessão com a sessão remota.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- Pergunte antes de redirecionar os dispositivos USB disponíveis.
- Não redirecione automaticamente os dispositivos USB disponíveis.
- Redirecione automaticamente os dispositivos USB disponíveis.

Por padrão, a opção de perguntar antes de redirecionar dispositivos, **Ask before redirecting available USB devices**, já vem selecionada. Com base na política selecionada, a opção selecionada na seção de **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Nota:**
>
> Atualmente, a política **Allow existing USB devices to be automatically connected** é aplicável somente ao aplicativo Citrix Workspace para Windows.

Allow newly arrived USB devices to be automatically connected

Essa configuração permite ou impede a conexão automática dos dispositivos USB que são inseridos no ponto de extremidade durante uma sessão com a sessão remota.

Ao adicionar essa configuração a uma política, selecione uma das seguintes opções:

- Pergunte antes de redirecionar os dispositivos USB disponíveis.
- Não redirecione automaticamente os dispositivos USB disponíveis.
- Redirecione automaticamente os dispositivos USB disponíveis.

Por padrão, a opção de perguntar antes de redirecionar dispositivos, **Ask before redirecting available USB devices**, já vem selecionada. Com base na política selecionada, a opção selecionada na seção de **Preferências** > **Dispositivos** do cliente pode ser substituída.

> **Nota:**
>
> Atualmente, a política **Allow newly arrived USB devices to be automatically connected** é aplicável somente ao aplicativo Citrix Workspace para Windows.

Client USB device redirection rules (Version 2)

Essa configuração especifica regras para filtrar, dividir e conectar automaticamente dispositivos USB a uma sessão remota.

Quando essa configuração é selecionada, o host substitui a configuração das *regras de redirecionamento do dispositivo USB cliente* pelas regras do dispositivo definidas nessa configuração.

Para obter mais informações, consulte Configuração do redirecionamento de dispositivo USB composto.

Configurações de política de lista de permissão de canal virtual

June 28, 2023

A configuração da política **Virtual channel allow list** 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, somente os canais virtuais Citrix são permitidos.

Para usar canais virtuais personalizados ou de terceiros, adicione os canais virtuais à lista. Para adicionar um canal virtual à lista:

1. Digite o nome do canal virtual seguido por uma vírgula.
2. Insira o caminho para o processo que acessa o canal virtual.

Mais caminhos executáveis podem ser listados e os caminhos são separados por vírgulas.

Por exemplo,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```


A partir do Citrix Virtual Apps and Desktops 7 2109, as listas de permissão de canais virtuais são ativadas por padrão.

Se você estiver usando o HDX RealTime Optimization Pack for Skype for Business, adicione o canal virtual à lista de autorizações. Para obter mais informações, consulte a documentação do HDX RealTime Optimization Pack.

> **Importante:**
>
> As máquinas VDA devem ser reiniciadas para que a configuração tenha efeito.

Para obter mais informações sobre canais virtuais, consulte Canais virtuais ICA.

Configurações de política de exibição visual

June 28, 2023

A seção **Visual Display** inclui configurações de política para controlar a qualidade das imagens que são enviadas de áreas de trabalho virtuais para o dispositivo do usuário.

Profundidade de cor preferida para gráficos simples

Essa configuração de política está disponível nas versões 7.6 FP3 do VDA e posteriores. A opção de 8 bits está disponível nas versões 7.12 e posteriores do VDA.

Essa configuração permite reduzir a profundidade de cor com a qual gráficos simples são enviados pela rede. Reduzir para 8 bits ou 16 bits por pixel potencialmente melhora a capacidade de resposta por conexões de baixa largura de banda. No entanto, essa ação pode custar uma pequena degradação na qualidade da imagem. A profundidade de cor de 8 bits não é suportada quando a configuração de política Use video codec for compression é definida como **For the entire screen**.

A profundidade de cor preferida padrão é de 24 bits por pixel.

Os VDAs usam a profundidade de cor de 24 bits (padrão) se a configuração de 8 bits for aplicada na versão 7.11 e anteriores do VDA.

Target frame rate

Essa configuração especifica o número máximo de quadros por segundo enviados da área de trabalho virtual para o dispositivo do usuário.

Por padrão, o máximo é 30 quadros por segundo.

Definir um número elevado 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 mais baixo para melhorar a experiência do usuário.

A taxa de quadros máxima suportada por segundo é 60.

Visual quality

Essa configuração especifica a qualidade visual desejada para as imagens exibidas no dispositivo do usuário.

Por padrão, essa configuração é Medium.

Para especificar a qualidade das imagens, escolha uma das seguintes opções:

- **Low** - Recomendado para redes com restrições de largura de banda onde a qualidade visual pode ser sacrificada por interatividade
- **Medium** - Oferece o melhor desempenho e eficiência de largura de banda na maioria dos casos de uso
- **High** - Recomendado se você precisar de qualidade de imagem visualmente sem perdas
- **Build to lossless** - 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 da rede. Essa configuração melhora o desempenho em relação às conexões de rede com restrições de largura de banda
- **Always lossless** - Quando é essencial preservar dados de imagem, selecione **Always lossless** para garantir que nunca sejam enviados para o dispositivo do usuário dados com redução de qualidade. Por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável.

Configurações de política de imagens em movimento

June 28, 2023

A seção **Moving Images** contém configurações que permitem remover ou alterar a compactação de imagens dinâmicas.

Minimum image quality

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração especifica a qualidade de imagem mínima aceitável para a Adaptive Display. Quanto menor a compressão utilizada, maior a qualidade das imagens exibidas. Escolha entre compressão Ultra High, Very High, High, Normal ou Low

Por padrão, isso é definido como Normal.

Moving image compression

Essa configuração especifica se a Adaptive Display está ativada ou não. A Adaptive Display ajusta automaticamente a qualidade da imagem de vídeos e slides de transição em apresentações de slides com base na largura de banda disponível. Com a Adaptive Display ativada, os usuários devem ver apresentações em execução suave sem redução na qualidade.

Por padrão, a Adaptive Display está ativada.

Para as versões do VDA 7.0 a 7.6, essa configuração se aplica somente quando o modo gráfico legado está ativado. Para as versões 7.6 FP1 do VDA e posteriores, essa configuração se aplica quando o modo gráfico legado está ativado ou quando o modo gráfico legado está desativado e não é usado um codec de vídeo para compactar gráficos.

Quando o modo gráfico legado está ativado, a sessão deve ser reiniciada antes que as alterações de política tenham efeito. A Adaptive Display é mutuamente exclusiva com Progressive Display; ativar a Adaptive Display desativa a Progressive Display e vice-versa. No entanto, tanto a Progressive Display quanto a Adaptive Display podem ser desativados ao mesmo tempo. O Progressive Display, como um recurso herdado, não é recomendado para o XenApp ou XenDesktop. Definir Progressive Threshold Level desabilita a Adaptive Display.

Progressive compression level

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Esta configuração fornece uma exibição inicial de imagens menos detalhada, mas mais rápida.

Por padrão, não é aplicada nenhuma compressão progressiva.

A imagem mais detalhada, definida pela configuração normal de compressão com perdas, aparece quando essa fica disponível. Use compactação Very High ou Ultra High para melhor visualização de gráficos com uso intensivo de largura de banda, como fotografias.

Para que a compactação progressiva seja eficaz, seu nível de compressão deve ser maior do que a configuração do nível de compressão com perdas.

Nota: O aumento do nível de compactação associado à compactação progressiva também aumenta a interatividade de imagens dinâmicas sobre 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 é aplicada configuração normal de compactação com perdas.

As seguintes configurações de política são correlatas:

- Progressive compression threshold value
- Progressive heavyweight compression

Progressive compression threshold value

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual é aplicada a compressão progressiva. Isto é aplicado somente às conexões do cliente sob esta largura de banda.

Por padrão, o valor limite é 2147483647 kilobits por segundo.

As seguintes configurações de política são correlatas:

- Progressive compression threshold value
- Progressive heavyweight compression

Target minimum frame rate

Essa 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 do VDA 7.0 a 7.6, essa configuração se aplica somente quando o modo gráfico legado está ativado. Para as versões 7.6 FP1 do VDA e posteriores, essa configuração se aplica quando o modo gráfico legado é desativado ou ativado.

Configurações de política de imagens estáticas

June 28, 2023

A seção **Still Images** contém configurações que permitem remover ou alterar a compactação de imagens estáticas.

Extra color compression

Essa configuração permite ou desativa o uso de compactação extra de cor em imagens fornecidas através de conexões de clientes limitadas em largura de banda, melhorando a capacidade de resposta, reduzindo a qualidade das imagens exibidas.

Por padrão, a compressão de cor extra está desativada.

Quando ativada, a compressão de cor extra é aplicada somente quando a largura de banda de conexão do cliente está abaixo do valor limite de compressão de cor extra. Quando a largura de banda de conexão do cliente está acima do valor limite ou Desativado estiver selecionada, a compactação de cor extra não é aplicada.

Extra color compression threshold

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração representa a largura de banda máxima em kilobits por segundo para uma conexão abaixo da qual é aplicada a compactação extra de cor. Se a largura de banda da conexão do cliente cair abaixo do valor definido, a compressão de cor extra será aplicada, se estiver ativada.

Por padrão, o valor limite é 8192 kilobits por segundo.

Heavyweight compression

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração permite ou desativa a redução da largura de banda além da compressão progressiva sem perder a qualidade da imagem usando um algoritmo gráfico mais avançado, mas que exige mais da CPU.

Por padrão, a compactação intensa está desativada.

Se ativada, a compactação intensa se aplica a todas as configurações de compactação com perdas. Ele é compatível com o aplicativo Citrix Workspace, mas não tem efeito em outros plug-ins.

As seguintes configurações de política são correlatas:

- Progressive compression level
- Progressive compression threshold value

Lossy compression level

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração controla o grau de compactação com perdas usado em imagens fornecidas através de conexões de cliente que são limitadas em largura de banda. Nesses casos, a exibição de imagens sem compactação pode ser lenta.

Por padrão, é selecionada a compactação média.

Para melhorar a capacidade de resposta com imagens com uso intensivo de largura de banda, use alta compactação. Nos casos em que é essencial preservar dados de imagem, por exemplo, ao exibir imagens de raios-X onde nenhuma perda de qualidade é aceitável, será preferível não usar a compactação com perdas.

Configuração de política correlata: Lossy compression threshold value

Lossy compression threshold value

Nota: no Virtual Delivery Agent 7.x, essa configuração de política se aplica somente quando a configuração Legacy graphics mode estiver ativada.

Essa configuração representa a largura de banda máxima em kilobits por segundo para uma conexão à qual é aplicada a compactação com perdas.

Por padrão, o valor limite é 2147483647 kilobits por segundo.

Adicionar a configuração de nível de compactação com perdas a uma política e incluir nenhum limite especificado pode melhorar a velocidade de exibição de bitmaps de alto detalhe, como fotografias, através de uma LAN.

Configuração de política correlata: Lossy compression level

Configurações da política do WebSockets

June 28, 2023

A seção **WebSockets** inclui configurações de política para acessar áreas de trabalho virtuais e aplicativos hospedados por meio do aplicativo Citrix Workspace para HTML5. O recurso WebSockets aumenta a segurança e reduz a sobrecarga através da realização de comunicação bidirecional entre aplicativos e servidores baseados em navegador. O recurso faz isso sem abrir várias conexões HTTP.

WebSockets connections

Essa configuração permite ou proíbe conexões WebSockets.

Por padrão, as conexões WebSocket são proibidas.

WebSockets port number

Essa configuração identifica a porta para conexões WebSocket de entrada.

Por padrão, o valor é 8008.

WebSockets trusted origin server list

Essa configuração fornece uma lista separada por vírgulas de servidores de origem confiáveis, geralmente o aplicativo Citrix Workspace para Web, expresso como URLs. O servidor aceita apenas conexões WebSockets originadas de um desses endereços.

Por padrão, o curinga * é usado para confiar em todos os aplicativos Citrix Workspace para URLs da Web.

Se você optar por digitar um endereço na lista, use esta sintaxe:

<protocolo>://<Nome do domínio do host totalmente qualificado>:[porta]

O protocolo deve ser HTTP ou HTTPS. Se a porta não for especificada, será usada a porta 80 para HTTP e a porta 443 para HTTPS.

O curinga `*` pode ser usado na URL, exceto como parte de um endereço IP (`10.105.*.*`).

Configurações da política de dispositivos WIA

June 28, 2023

A seção de **dispositivos WIA** inclui configurações de política para gerenciar o redirecionamento do scanner usando a Aquisição de Imagens do Windows (WIA).

Redirecionamento WIA

Dispositivos WIA, como câmeras digitais e scanners, se comunicam com aplicativos de processamento de imagem hospedados pelo servidor usando a estrutura WIA. Essa configuração permite ou proíbe que os usuários acessem dispositivos WIA no dispositivo do usuário. Por padrão, o redirecionamento WIA é proibido.

Para obter informações sobre dispositivos compatíveis com WIA, consulte Dispositivos WIA.

Recursos HDX gerenciados através do registro

June 28, 2023

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

Para abrir o Editor do Registro, execute `regedit.exe` no servidor. Em seguida, navegue até a chave de registro para adicionar ou editar as configurações.

Dispositivos

Teclados Bloomberg

O Citrix Virtual Apps and Desktops são compatíveis com o teclado starboard Bloomberg modelo 4 e modelo 3. Por padrão, o suporte ao teclado avançado Bloomberg é 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 de valor: 0 = Desativado, 1 = Ativado

Para obter mais informações, consulte Teclado Bloomberg.

Unidades cliente mapeadas

Como precaução de segurança, quando um usuário faz logon no Citrix Virtual Apps and Desktops, por padrão, o servidor mapeia as unidades cliente sem a permissão de execução do usuário. Para permitir que os usuários executem arquivos executáveis residentes em unidades cliente mapeadas, substitua esse padrão editando o registro no servidor.

Para permitir o acesso, edite o seguinte valor de registro (crie **CDMSettings** se não existir):

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- Nome do valor: ExecuteFromMappedDrive
- Tipo de valor: DWORD
- Dados de valor: 1 = Permitir permissão, 0 = Negar permissão em unidades mapeadas

A alteração entra em vigor para sessões conectadas após você editar o registro.

Para obter mais informações, consulte Unidades cliente mapeadas.

Canetas Microsoft Surface Pro e Surface Book

O Citrix Virtual Apps and Desktops oferece suporte à funcionalidade de caneta padrão com aplicativos Windows baseados em tinta. Por padrão, esse recurso está ativado.

Para desativar ou ativar esse recurso, defina o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- Nome do valor: DisablePen
- Tipo de valor: DWORD
- Dados de valor: 1 = Desativar, 0 = Ativar

Para obter mais informações, consulte Canetas Microsoft Surface Pro e Surface Book.

Lista de permissões de aplicativos de Aquisição de Imagens do Windows

Esta 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 a Aquisição de Imagens do Windows.

Para ajustar Aquisição de Imagens do Windows para aplicativos no VDA, crie a seguinte configuração de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- Nome do valor: WIAAllowedProcesses

  Selecione e clique com o botão direito em **WIAAllowedProcesses**. Escolha **Novo > Valor de Cadeia de Caracteres Múltipla** e renomeie o novo valor para **AllowProcesses**.
- Dados de valor: insira o caminho completo e o nome do processo para cada aplicativo que pode acessar a Aquisição de Imagens do Windows. Forneça a cada aplicativo em uma nova linha.

Quaisquer alterações nessa configuração entrarão em vigor na próxima vez que você iniciar uma sessão no VDA.

Geral

Configurar o logon automático no VDA

Essa configuração permite ativar ou desativar a configuração de política da Microsoft **Sempre pedir senha** no SO Windows 10 de sessão única e VDAs com SO multissessão.

Se **Sempre pedir senha** estiver ativada, os usuários deverão inserir credenciais no VDA quando iniciarem uma sessão remota. Se a configuração estiver desativada, os usuários se conectam automaticamente à sessão remota sem fornecer credenciais no VDA.

Por padrão, a configuração de política da Microsoft está desativada. Para ativar ou desativar a configuração **Sempre pedir 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 de valor:
  - 1 - Desativa a configuração de política da Microsoft e permite que os usuários façam login automaticamente a uma sessão remota.
  - 0 —Habilita a configuração de política da Microsoft e solicita que os usuários forneçam credenciais ao iniciarem uma sessão remota.

Desativar o aviso de tempo limite

Por padrão, os usuários com sessões inativas ou ociosas recebem uma mensagem de aviso dois minutos antes de a sessão se desconectar automaticamente.

Essa configuração desativa e remove a mensagem de aviso para usuários que atingem o limite de tempo da sessão ociosa em:

- Windows Server 2004
- Windows 10 multissessão 2004 ou SO multissessão posterior

Para remover o aviso, defina o seguinte valor de registro no VDA:

- Chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- Nome do valor: fEnableTimeoutWarning
- Tipo de valor: DWORD
- Dados de valor: 1 = Desativar a mensagem de aviso, 0 = Ativar a mensagem de aviso

Para exibir a mensagem de aviso, exclua o valor de registro ou defina-o como 0.

Descoberta de MTU em EDT

A descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso impede a fragmentação do pacote EDT que possa resultar em degradação de desempenho ou falha para estabelecer uma sessão.

Essa configuração é ativada por padrão. Para desabilitar a descoberta de MTU em EDT, configure o seguinte valor de registro e reinicialize o VDA.

- Chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- Nome do valor: MtuDiscovery
- Tipo de valor: DWORD
- Dados de valor: 0

Essa configuração se aplica a toda a máquina e afeta todas as sessões que se conectam a partir de um cliente suportado.

Redirecionamento geral de conteúdo

Adicionar tipos de URL para redirecionamento de host para 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 de valor: especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade do URL. Por exemplo:
  `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL somente para clientes Windows. Os clientes que não têm essa configuração de registro rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para lidar com os tipos de URL especificados.

Para obter mais informações, consulte Redirecionamento do host para o client.

Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente altera a maneira como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Considere que você ativa o redirecionamento da pasta cliente no servidor e o usuário o configura no dispositivo do usuário. Nesse caso, a parte do volume local especificada pelo usuário é redirecionada.

Para ativar o redirecionamento de pasta do cliente no servidor, defina o seguinte valor do registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- Nome do valor: CFROnlyModeAvailable
- Tipo de valor: DWORD
- Dados de valor: 1

Para obter mais informações, consulte Redirecionamento de pasta do cliente.

Redirecionamento de host para cliente para um conjunto específico de sites

Para habilitar o redirecionamento de host para 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 de valor: especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNS). Digite vários FQDNS em linhas separadas. Inclua somente o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este caractere curinga combina um único nível de domínio, que é consistente com as regras no RFC 6125. Por exemplo:

`www.example.com`


```
*.example.com
```

Para obter mais informações, consulte Redirecionamento do host para o client.

Comportamento do aplicativo local no logoff e na desconexão

Por padrão, os aplicativos locais continuam sendo executados quando um usuário faz logoff ou se desconecta da área de trabalho virtual. Após a reconexão, os aplicativos locais serão reintegrados se estiverem disponíveis na área de trabalho virtual. Para configurar o comportamento do aplicativo local no logoff e na desconexão, defina o seguinte valor de registro na área de trabalho hospedada:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- Nome do valor: Session State
- Tipo de valor: DWORD
- Dados de valor:
  - 1 - Os aplicativos locais continuam sendo 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 ao aplicativo local e redirecionamento de URL.

Remover tipos de URL da lista padrão para redirecionamento de host para cliente

Para remover os tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e os valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD
- Dados de valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados de valor: especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

```
http
https
```


`rtsp`

Para obter mais informações, consulte Redirecionamento do host para o client.

Configuração do navegador padrão de VDA do servidor

Você pode ativar o redirecionamento de host para cliente para substituir qualquer configuração do navegador padrão no VDA do servidor. Se um URL da Web não for redirecionado, o Citrix Launcher passa a URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente.

- Internet Explorer (padrão)
  - Chave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome do valor: Default
  - Tipo de valor: REG_SZ
  - Dados de valor: `"c:\program files\internet explorer\iexplore.exe"" %1"`
  - Chave: HKEY_CLASSES_ROOT\https\shell\open\command_backup‘
  - Nome do valor: Default
  - Tipo de valor: REG_SZ
  - Dados de valor: `"c:\program files\internet explorer\iexplore.exe"" %1"`
- Google Chrome
  - Chave: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - Nome do valor: Default
  - Tipo de valor: REG_SZ
  - Dados de 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 de 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 de 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 de valor: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

O Local App Access para aplicativos publicados

O Local App Access integra perfeitamente os aplicativos do Windows instalados localmente em um ambiente de trabalho hospedado sem mudar de uma área de trabalho para outra. 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 de valor: 1 = Ativar, 0 = Desativar

Para obter mais informações, consulte Acesso ao aplicativo local e redirecionamento de URL.

Gráficos

Aceleração de GPU para aplicações CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL em execução em uma sessão de usuário é desativada por padrão.

Para usar os recursos POC de aceleração CUDA, faça 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 de valor: 00000001

Para usar os recursos POC de aceleração OpenCL, faça 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 de valor: 00000001

Para obter mais informações, consulte Aceleração de GPU para SO multissessão Windows

Modo progressivo

O modo progressivo está desativado por padrão. Você pode alterar o estado do modo progressivo com o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo de valor: REG_DWORD
- Nome do valor: ProgressiveDisplay
- Dados de valor:
  - 0 = Sempre inativo (Desativa o modo progressivo. Este valor é o padrão.)
  - 1 = Automático (Alternar com base nas condições de rede.)
  - 2 = Sempre ativo

Para obter mais informações, consulte Modo progressivo.

Renderização do Windows Presentation Foundation (WPF)

O HDX 3D Pro permite que aplicativos com muitos gráficos em execução em sessões de SO multissessão Windows para renderizar na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização do Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não diminui a velocidade de processamento da CPU do servidor.

Para permitir a renderização de aplicativos WPF usando a GPU do servidor, crie a seguinte configuração no registro do servidor executando o SO multisessão do Windows:

1. Abra o Editor do Registro no VDA e navegue até a seguinte chave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Crie ou edite os seguintes valores de registro:

   - [REG_DWORD] AdapterHandle = 0x00000001

- [REG_DWORD] DevicePath = 0x00000001
- [REG_DWORD] Flag = 0x00000412
- [REG_DWORD] WPF = 0x00000001

3. Crie uma subchave com o nome executável do seu aplicativo WPF. Por exemplo, se seu aplicativo for chamado de "mywpfapp.exe", crie a seguinte chave:

   ```
   HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
   ```

4. Reinicialize o servidor para que a configuração entre em vigor.

Para obter mais informações, consulte Aceleração da GPU para SO Windows multissessão e o blog sobre Getting the best out of WPF apps on Windows multi-session OS.

Multimídia

Evitar eco durante conferências multimídia

O Citrix Virtual Apps and Desktops oferece uma opção de cancelamento de eco que minimiza o eco. Esse recurso é ativado por padrão. Para desativar o cancelamento de eco, você pode alterar uma das seguintes configurações do registro:

- Chave:
  - 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Module
  - 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Ad
- Nome do valor: EchoCancellation
- Tipo de valor: DWORD
- Dados de valor: False

Para obter mais informações, consulte Recursos de áudio.

Limitação de áudio

Depois de instalar um dispositivo de áudio em seu cliente, ativar o redirecionamento de áudio e iniciar uma sessão do RDS, os arquivos de áudio podem não reproduzir o áudio. Como solução alternativa, adicione a seguinte chave de registro à máquina RDS e reinicie o computador:

- Chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- Nome do valor: EnableSvchostMitigationPolicy
- Tipo de valor: DWORD
- Dados de 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 algum 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 da GPU de 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 de 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 de valor:
  - 0 = Desativar a transmissão de webcam de alta definição
  - 1 = Ativar a transmissão de webcam de alta definição

Resolução de webcam de alta definição

Se a negociação de tipo de mídia falhar, o HDX cai de volta à resolução padrão de 352x288 CIF. Você pode usar chaves de registro no cliente para configurar a resolução padrão. Antes de definir as seguintes chaves de registro, verifique se a câmera suporta a resolução especificada.

- Chave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Largura
  - Nome do valor: DefaultWidth
  - Tipo de valor: DWORD
  - Dados de valor: largura desejada em decimal (por exemplo, 1280)

- Altura
  - Nome do valor: DefaultHeight
  - Tipo de valor: DWORD
  - Dados de valor: altura desejada em decimal (por exemplo 720)

Largura de banda de webcam de alta definição

A compactação de vídeo de webcam HDX usa menos largura de banda em comparação com o redirecionamento USB genérico plug-and-play e funciona bem em conexões WAN. Para ajustar a largura de banda, configure o seguinte valor de registro no cliente:

- Chave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Nome do valor: TargetBitrate
- Tipo de valor: DWORD
- Dados de valor: 350000

Digite um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usam 350000 bps por padrão.

Para obter mais informações, consulte Compactação de vídeo de webcam HDX.

Modo de fallback do Microsoft Teams

Se o Microsoft Teams não carregar no modo VDI otimizado (“Citrix HDX Not Connected”em Teams/-Sobre/Versãp), o VDA volta às tecnologias HDX herdadas, como o redirecionamento da webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando um sistema operacional de versão/plataforma do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não serão aplicadas.

Para controlar o mecanismo de fallback, defina um dos seguintes valores de registro no VDA:

- Chave (apenas uma é necessária):
  - **Configuração do computador:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - **Configuração do usuário:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- Nome do valor: DisableFallback
- Tipo de valor: DWORD
- Dados de valor: 1 = Desativar o modo de fallback, 2 = Ativar somente áudio

Se o valor não estiver presente ou estiver definido como 0, o modo de fallback será ativado. Esse 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 do VDA e do Microsoft Teams em camadas diferentes, crie uma chave de registro vazia chamada **PortICA** no Windows antes de instalar o Microsoft Teams com o sinalizador ALLUSER=1 da linha de comando. Deixe o nome do valor, o tipo e os dados padrão.

- Chave para a versão de 32 bits do Editor do Registro: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cit
- 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

Esta configuração fornece logon único para um servidor Web configurado com a 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 de valor: 1

Para obter mais informações, consulte Logon único com autenticação integrada do Windows.

Cabeçalho de solicitação do agente do usuário

O cabeçalho usuário-agente ajuda a identificar solicitações HTTP enviadas pelo redirecionamento de conteúdo do navegador. Essa configuração pode ser útil quando você configura as regras de proxy e firewall. Por exemplo, se o servidor bloquear as solicitações enviadas do redirecionamento de conteúdo do navegador, você poderá criar uma regra que contenha o cabeçalho usuário-agente para ignorar determinados requisitos. Somente dispositivos Windows suportam o cabeçalho de solicitação de agente-usuário.

Por padrão, a string de cabeçalho de solicitação agente-usuário está desabilitada. Para habilitar o cabeçalho agente-usuário para conteúdo renderizado pelo cliente, use o Editor do Registro.

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 de 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.

Compactação de software de webcam

Se uma webcam suportar codificação de hardware, a compactação de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compactação de software, adicione o seguinte valor ao cliente:

- Chave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- Nome do valor: DeepCompress_ForceSWEncode
- Tipo de valor: DWORD
- Dados de valor: 1

Para obter mais informações, consulte Compactação de vídeo de webcam HDX.

Compactação de vídeo de webcam

A compactação, ou compressão, de vídeo de 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 de webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Esse recurso é ativado por padrão.

Para desativar o streaming direto de vídeo 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 de valor: 0

Para obter mais informações, consulte Compactação de vídeo de webcam HDX.

Taxa de quadros de compressão de vídeo da webcam

Para ajustar a taxa de quadros de vídeo preferida, edite o seguinte valor de registro no cliente:

- Chave: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Nome do valor: FramesPerSecond
- Tipo de valor: DWORD
- Dados de valor: 15

Se a webcam não suportar a taxa de quadros especificada, o aplicativo usará 15 FPS por padrão.

Para obter mais informações, consulte Compactação de vídeo de webcam HDX.

Configurações da política de gerenciamento de carga

June 28, 2023

A seção de **Gerenciamento de Carga** inclui configurações de política para habilitar e configurar o gerenciamento de carga entre servidores que fornecem máquinas do sistema operacional Windows multissessão.

Para obter informações sobre o cálculo do índice do avaliador de carga, consulte CTX202150.

Concurrent logon tolerance

Essa configuração especifica o número máximo de logons simultâneos que um servidor pode aceitar.

Por padrão, esse valor é definido como 2.

Quando essa configuração está ativada, 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 aplicado. Para impor o limite (e fazer com que os logons simultâneos que excedam o número especificado falhem), crie a seguinte chave de registro:

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> Type: DWORD
> Value: 1

Uso de CPU

Essa configuração especifica o nível de uso da CPU, como uma porcentagem, no qual o servidor relata uma carga total. Quando ativada, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, essa configuração está desativada e o uso da CPU é excluído dos cálculos de carga.

CPU usage excluded process priority

> **Nota:**
>
> Em cenários em que o Workspace Environment Management gerencia as máquinas, o uso dessa configuração com as configurações CPU Priority pode ter resultados indesejados. Recomendamos que você desative essa configuração se optar por usar as configurações de CPU Priority.

Essa configuração especifica o nível de prioridade no qual o uso da CPU de um processo é excluído do índice de carga de uso da CPU.

Por padrão, esse valor é definido como **Below Normal** ou **Low**.

Disk usage

Essa configuração especifica o comprimento da fila de disco no qual o servidor relata uma carga total de 75%. Quando ativado, o valor padrão para o comprimento da fila de disco é 8.

Por padrão, essa configuração está desativada e o uso do disco é excluído dos cálculos de carga.

Maximum number of sessions

Essa configuração especifica o número máximo de sessões que um servidor pode hospedar. Quando ativada, a configuração padrão para o número máximo de sessões que um servidor pode hospedar é 250.

Por padrão, essa configuração está ativada.

Uso de memória

Essa configuração especifica o nível de uso da memória, como uma porcentagem, no qual o servidor relata uma carga total. Quando ativada, o valor padrão no qual o servidor relata uma carga total é 90%.

Por padrão, essa configuração está desativada e o uso de memória é excluído dos cálculos de carga.

Memory usage base load

Essa configuração especifica uma aproximação do uso de memória do sistema operacional base. Além disso, define, em MB, o uso de memória abaixo do qual um servidor é considerado com carga zero.

Por padrão, esse valor é definido como 768 MB.

Configurações da política de gerenciamento de perfis

June 28, 2023

Esta seção contém configurações de política para ativar e configurar o Profile Management.

Para obter outras informações, como as seguintes, consulte as Políticas do Profile Management:

- Nomes da configuração do arquivo .ini equivalente
- Qual versão do Profile Management é necessária para a configuração de uma política

Configurações avançadas de política

June 28, 2023

Number of retries when accessing locked files

Define o número de novas tentativas ao acessar arquivos bloqueados.

Se esta política estiver desativada, será usado o valor padrão de cinco novas tentativas. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, será usado o valor padrão.

Process Internet cookie files on logoff

Algumas implantações deixam cookies extras da Internet que `Index.dat` não faz referência. Os cookies extras deixados no sistema de arquivos após a navegação sustentada podem levar à sobrecarga do perfil. Essa política permite que você ative o Profile Management para forçar o processamento do Index.dat e remover os cookies extras. A política aumenta os tempos de logoff, portanto, habilite-a apenas depois de ter esse problema.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, não ocorrerá nenhum processamento do Index.dat.

Disable automatic configuration

O Profile Management examina qualquer ambiente do Citrix Virtual Desktops, por exemplo, quanto à presença de vDisks pessoais, e configura a Política de Grupo de modo correspondente. Somente as políticas de Profile Management no estado Not Configured são ajustadas, portanto, todas as personalizações feitas são preservadas.

Essa política permite acelerar a implantação e simplificar a otimização. Você não precisa configurar essa política. No entanto, você pode desativar a configuração automática ao fazer o seguinte:

- Atualização para manter as configurações de versões anteriores
- Solução de problemas

Você pode considerar a configuração automática como um verificador de configuração dinâmico que configura automaticamente as configurações de política padrão de acordo com os ambientes em tempo de execução. Isso elimina a necessidade de configurar as configurações manualmente. Os ambientes de tempo execução incluem:

- Sistema operacional 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 for alterado:

- Active write-back
- Always cache
- Delete locally cached profiles on logoff
- Delay before deleting cached profiles
- Profile streaming

Consulte a tabela a seguir para ver o status padrão das políticas em sistemas operacionais diferentes:

	SO multissessão	SO de sessão única
Active write back	Enabled	*Disabled* se o Personal vDisk estiver em uso; caso contrário, ativado.
Always cache	Disabled	*Disabled* se o Personal vDisk estiver em uso; caso contrário, ativado.
Delete locally cached profiles on logoff	Enabled	*Disabled* se ocorrer uma das seguintes situações: o Personal vDisk está em uso, o Citrix Virtual Desktops está atribuído ou o Citrix Virtual Desktops não está instalado; caso contrário, ativado.
Delay before deleting cached profiles	0 segundos	60 segundos se as alterações do usuário não forem persistentes; caso contrário, 0 segundos.
Profile streaming	Enabled	*Disabled* se o Personal vDisk estiver em uso; caso contrário, ativado.

No entanto, com a configuração automática desabilitada, todas as políticas acima do padrão para **Disabled**.

> **Importante:**
>
> Personal vDisk está obsoleto. Para obter detalhes, consulte Remover PVD, AppDisks e hosts não suportados.

Começando com o Profile Management 1909, você pode ter uma experiência melhorada com o menu Iniciar no Windows 10 (versão 1607 e posteriores) e Windows Server 2016 e posteriores. Essa melhoria é alcançada através da configuração automática das seguintes políticas:

- Adicione `Appdata\Local\Microsoft\Windows\Caches` e `Appdata\Local\Packages` a **Folders to Mirror**.
- Adicione `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` a **Files to synchronize**.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver configurada aqui nem no arquivo .ini, a configuração automática será ativada. Nesse caso, as configurações do Profile Management podem mudar se o ambiente mudar.

Log off user if a problem is encountered

Permite especificar se o Profile Management faz logoff dos usuários se um problema for encontrado.

Se essa política estiver desabilitada ou não estiver configurada, o Profile Management fornece um perfil temporário aos usuários se um problema for encontrado. Por exemplo, o armazenamento do usuário não está disponível.

Se estiver ativada, uma mensagem de erro será exibida e os usuários serão desativados. Esta configuração pode simplificar a solução do problema.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, será fornecido um perfil temporário.

Programa de Aperfeiçoamento da Experiência do Usuário

Por padrão, o Programa de Aperfeiçoamento da Experiência do Usuário está ativado para ajudar a melhorar a qualidade e o desempenho dos produtos Citrix coletando estatísticas anônimas e dados de uso.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Enable search index roaming for Outlook

Permitir experiência de pesquisa do Outlook baseada no usuário roaming automaticamente dados de pesquisa do Outlook juntamente com o perfil do usuário. Esse recurso requer espaços extras no armazenamento do usuário para armazenar os índices de pesquisa para o Outlook.

Faça logoff e, em seguida, faça logon novamente para que esta política tenha efeito.

Outlook search index database –backup and restore

Permite especificar o que o Profile Management faz durante o logon quando a política Enable search index roaming for Outlook policy está ativada.

Se essa política estiver ativada, o Profile Management faz um backup do banco de dados de índice de pesquisa sempre que o banco de dados for montado com êxito no logon. O Profile Management

trata o backup como a cópia boa do banco de dados de 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 válida conhecida.

> Nota:
>
> O Profile Management exclui o backup salvo anteriormente depois que um backup novo é salvo com sucesso. O backup consome o armazenamento VHDX disponível.

Enable concurrent session support for Outlook search data roaming

Permite que o Profile Management forneça uma experiência de pesquisa nativa do Outlook em sessões simultâneas do mesmo usuário. Use essa política com a política Search index roaming for Outlook.

Com essa política habilitada, cada sessão simultânea usa um arquivo OST do Outlook separado.

Por padrão, apenas dois discos VHDX podem ser usados para armazenar arquivos OST do Outlook (um arquivo por disco). Se o usuário iniciar mais sessões, seus arquivos OST do Outlook serão armazenados no perfil de usuário local. Você pode especificar o número máximo de discos VHDX para armazenar arquivos OST do Outlook.

Enable OneDrive container

Permite que as pastas do OneDrive façam roaming com os usuários.

O contêiner do OneDrive é uma solução de roaming de pastas baseada em VHDX. O Profile Management cria um arquivo VHDX por usuário em um compartilhamento de arquivos e armazena as pastas do OneDrive dos usuários nos arquivos VHDX. Os arquivos VHDX são anexados quando os usuários fazem logon e desanexados quando os usuários fazem logoff.

Enable asynchronous processing for user Group Policy on logon

O Windows fornece dois modos de processamento para a Política de Grupo do usuário: síncrono e assíncrono. O Windows usa um valor de registro para determinar o modo de processamento para o próximo logon do usuário. Se o valor do registro não existir, o modo síncrono é aplicado. O valor do registro é uma configuração no nível da máquina e não faz roaming com os usuários. Assim, o modo assíncrono não é aplicado conforme o esperado se os usuários:

- Fazem logon em máquinas diferentes.
- Fazem logon na mesma máquina em que a política Delete locally cached profiles on logoff está ativada.

Com essa política ativada, o valor do registro faz roaming com os usuários. Como resultado, o modo de processamento é aplicado sempre que os usuários fazem logon.

Proporção de espaço livre para acionar a compactação do disco VHD

Aplicável quando a opção Enable VHD disk compaction está ativada. Permite especificar a proporção de espaço livre para acionar a compactação do disco VHD. Quando a proporção de espaço livre excede o valor especificado no logoff do usuário, a compactação do disco é acionada.

Proporção de espaço livre = (tamanho atual do arquivo VHD —tamanho mínimo de arquivo VHD necessário*) ÷ tamanho do arquivo VHD atual

* Obtido usando o método GetSupportedSize da classe `MSFT_Partition` do sistema operacional Microsoft Windows.

Número de logoffs para acionar a compactação do disco VHD

Aplicável quando a opção Enable VHD disk compaction está ativada. Permite que você especifique o número de logoffs do usuário para acionar a compactação do disco VHD.

Quando o número de logoffs desde a última compactação atinge o valor especificado, a compactação do disco é acionada novamente.

Desativar a desfragmentação para compactação de disco VHD

Aplicável quando a opção Enable VHD disk compaction está ativada. Permite que você especifique se a desfragmentação de arquivos deve ser desativada para compactação de disco VHD.

Quando a compactação de disco VHD está ativada, o arquivo de disco VHD é, primeiro, desfragmentado automaticamente usando a ferramenta `defrag` interna do Windows e depois compactado. A desfragmentação do disco VHD produz melhores resultados de compactação, enquanto sua desativação pode economizar recursos do sistema.

Enable multi-session write-back for profile containers

Permite write-back para contêineres de perfis em cenários multissessão. Se ativado, as alterações em todas as sessões serão gravadas de volta em contêineres de perfis. Caso contrário, somente as alterações na primeira sessão serão salvas porque somente a primeira sessão está no modo de leitura/-gravação em contêineres de perfil. Os contêineres de perfil Citrix Profile Management são suportados a partir do Citrix Profile Management 2103. O FSLogix Profile Container é suportado a partir do Citrix Profile Management 2003.

Para usar essa política para o FSLogix Profile Container, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O recurso FSLogix Profile Container está instalado e ativado.
- O tipo de perfil é definido como **Try for read-write profile and fallback to read-only** no FSLogix.

Replicate user stores

Permite replicar o armazenamento de perfis de usuário remoto em vários caminhos em cada logon e logoff. Isso permite que o Profile Management forneça redundância de perfil para logons de usuários.

A ativação da política aumenta a E/S do sistema e pode prolongar os logoffs.

Nota:

> - Esse recurso está disponível tanto para armazenamento do usuário quanto para o contêiner de perfil completo.
> - Os contêineres de perfil replicados fornecem redundância de perfil para logons de usuários, mas não para failover na sessão.

Enable credential-based access to user stores

Por padrão, o Citrix Profile Management personifica o usuário atual para acessar o armazenamento do usuário. Ative esse recurso se você não quiser que o Profile Management personifique o usuário atual ao acessar o armazenamento do usuário. Você pode colocar armazenamentos de usuários em repositórios de armazenamento (por exemplo, arquivos do Azure) que o usuário atual não tem permissão para acessar.

Para garantir que o Profile Management possa acessar os armazenamentos de usuários, salve as credenciais do servidor de armazenamento de perfil no Workspace Environment Management (WEM) ou no Gerenciador de Credenciais do Windows. Recomendamos que você use o Workspace Environment Management para eliminar a necessidade de configurar as mesmas credenciais para cada máquina em que o Profile Management é executado. Se você usar o Gerenciador de Credenciais do Windows, use a conta do Sistema Local para salvar as credenciais com segurança.

> **Nota:**
>
> Essa política está disponível tanto para armazenamentos de usuário baseados em arquivos quanto em VHDX. Para versões do Profile Management anteriores à 2212, essa política está disponível somente para armazenamentos de usuário baseados em VHDX.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini. Se essa configuração não estiver definida aqui nem no arquivo .ini, ela será desativada por padrão.

Customize storage path for VHDX files

O Profile Management fornece as seguintes políticas baseadas em VHDX: Profile container, Search index roaming for Outlook e Accelerate folder mirroring. Por padrão, os arquivos VHDX são armazenados no armazenamento do usuário. Essa política permite especificar um caminho separado para armazená-los.

Automatically reattach VHDX disks in sessions

Com essa política ativada, o Profile Management garante um alto nível de estabilidade das políticas baseadas em VHDX. Por padrão, essa política está ativada.

Quando essa política está desativada, o Profile Management monitora os discos VHDX que estão em uso por políticas baseadas em VHDX. Se algum dos discos for desanexado, o Profile Management reconectará o disco automaticamente.

Configurações básicas de política

June 28, 2023

Esta seção contém configurações de política relacionadas à configuração básica do Profile Management.

Enable Profile Management

Por padrão, para facilitar a implantação, o Profile Management não processa logons ou logoffs. Ative o Profile Management somente depois de executar todas as outras tarefas de configuração e testar como os perfis de usuário Citrix funcionam em seu ambiente.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, o Profile Management não processará perfis de usuário do Windows de forma alguma.

Processed groups

Podem ser utilizados grupos de computadores locais e grupos de domínios (local, global e universal). Os grupos de domínio devem ser especificados no formato: NOME DE DOMÍNIO\NOME DE GRUPO

Se esta política estiver configurada aqui, o Profile Management processará somente membros desses grupos de usuários. Se esta política estiver desativada, o Profile Management processa todos os usuários. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, os membros de todos os grupos de usuários serão processados.

Excluded groups

Você pode usar grupos locais de computador e grupos de domínio (local, global e universal) para evitar que sejam processados perfis de usuário específicos. Especifique grupos de domínio no formato NOME DE DOMÍNIO\NOME DE GRUPO

Se esta configuração estiver configurada aqui, o Profile Management exclui membros desses grupos de usuários. Se essa configuração estiver desativada, o Profile Management não excluirá nenhum usuário. Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini. Se essa configuração não estiver definida aqui nem no arquivo .ini, nenhum membro de nenhum grupo será excluído.

Process logons of local administrators

Especifica se os logons de membros do grupo BUILTIN\Administrators são processados. Considere que esta política está desativada ou não está configurada em sistemas operacionais multissessão, como ambientes Citrix Virtual Apps. Nesse caso, o Profile Management pressupõe 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. Essa política permite aos usuários de domínio com direitos de administrador local, geralmente usuários do Citrix Virtual Desktops com áreas de trabalho virtuais atribuídas:

- Ignorar qualquer processamento
- Fazer logon
- Solucionar problemas de área de trabalho com o Profile Management

Observação: os logons dos usuários de domínio podem estar sujeitos a restrições impostas pela associação ao grupo, geralmente para garantir a conformidade com o licenciamento do produto.
Se esta política estiver desativada, o Profile Management não processará logons por administradores locais. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, os administradores não serão processados.

Path to user store

Define o caminho para o diretório (o armazenamento do usuário) no qual são armazenadas as configurações do usuário (alterações do registro e arquivos sincronizados).

O caminho pode ser:

- Um caminho relativo. Deve ser relativo ao diretório home (que é normalmente configurado como o atributo #homeDirectory# para um usuário no Active Directory).
- Um caminho UNC. Normalmente, ele especifica um compartilhamento de servidor ou um namespace DFS.
- Desativado ou não configurado. Nesse caso, é assumido um valor de #homeDirectory#\ Windows.

Os seguintes tipos de variáveis podem ser usados para esta política:

- Variáveis de ambiente do sistema incluídas em 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 símbolos de cerquilha (por exemplo, #sAMAccountName#).
- Variáveis de Profile Management. Para obter mais informações, consulte o documento do produto de variáveis de Profile Management.

As variáveis de ambiente do usuário não podem ser usadas, exceto para %username% e %userdomain%. Você também pode criar atributos personalizados para definir totalmente variáveis organizacionais, como localização ou usuários. Os atributos diferenciam maiúsculas e minúsculas.

Exemplos:

- \server\share#sAMAccountName# armazena as configurações do usuário para o caminho UNC \server\share\JohnSmith (se #sAMAccountName# resolve para JohnSmith para o usuário atual)
- \server\profiles$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! pode se expandir para \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Importante: qualquer que sejam os atributos ou variáveis que você usar, verifique se esta política se expande para a pasta um nível superior à pasta que contém NTUSER.DAT. Por exemplo, se esse 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 como usar variáveis ao especificar o caminho para o armazenamento do usuário, consulte os seguintes tópicos:

- Share Citrix user profiles on multiple file servers
- Administer profiles within and across OUs

- High availability and disaster recovery with Profile Management

Se o Caminho para o armazenamento do usuário estiver desativado, as configurações do usuário serão salvas no subdiretório Windows do diretório inicial.

Se esta política estiver desativada, as configurações do usuário serão salvas no subdiretório Windows do diretório inicial. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, o diretório do Windows na unidade inicial será usado.

Migrate user store

Especifica o caminho para a pasta onde as configurações do usuário (alterações do registro e arquivos sincronizados) foram salvas anteriormente (o caminho de armazenamento do usuário que você usou anteriormente).

Se essa opção estiver configurada, as configurações do usuário armazenadas no repositório de usuários anterior são migradas para o armazenamento de usuário atual especificado na política "Path to user store".

O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório home.

Nos dois casos, você pode usar os seguintes tipos de variáveis:

- Variáveis do ambiente do sistema entre símbolos de porcentagem
- Atributos do objeto de usuário do Active Directory entre símbolos de cerquilha

Exemplos:

- A pasta `Windows\\%ProfileVer%` armazena as configurações do usuário em uma subpasta chamada `Windows\W2K3` do repositório do usuário (se %ProfileVer% for uma variável de ambiente do sistema que resolve para W2K3).
- `\\server\share\\#SAMAccountName#` armazena as configurações do usuário no caminho UNC `\\server\share\<JohnSmith>` (se `#SAMAccountName#` for resolvido para JohnSmith em relação ao usuário atual).

No caminho, você pode usar variáveis de ambiente de usuário exceto `%username%` e `%userdomain%`.

Se essa configuração estiver desativada, as configurações do usuário serão salvas no repositório de usuários atual.

Se essa configuração não estiver definida aqui, será usada a configuração correspondente do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, as configurações do usuário serão salvas no armazenamento do usuário atual.

Active write back

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 estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, ela estará ativada.

Offline profile support

Esta política permite que os perfis sincronizem com o armazenamento do usuário o mais cedo possível. Destina-se a usuários de laptop ou dispositivos móveis em roaming. 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. Posteriormente, são sincronizados com o armazenamento do usuário quando a conexão de rede for restabelecida.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, os perfis offline serão desativados.

Active write back registry

Use esta política junto com "Active write back". As entradas de registro que são modificadas podem ser sincronizadas com o armazenamento do usuário no meio de uma sessão.

Se você não definir essa configuração aqui, será usado o valor do arquivo .ini.

Se você não definir essa configuração aqui ou no arquivo .ini, o registro de gravação ativa será desativado.

Gravação ativa no bloqueio e desconexão da sessão

Com essa política e a política **Active write back** ativadas, os arquivos e pastas de perfil são gravados somente quando uma sessão é bloqueada ou desconectada.

Com essa política e as políticas **Active write back** e **Active write back registry** ativadas, as entradas do registro são gravadas somente quando uma sessão é bloqueada ou desconectada.

Offline profile support

Ativa o recurso de perfis off-line. Este recurso destina-se a computadores que são normalmente removidos de redes. Por exemplo, laptops ou dispositivos móveis, não servidores ou desktops.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, o suporte ao perfil offline será desativado.

Configurações de política entre plataformas

June 28, 2023

Esta seção contém configurações de política relacionadas à configuração do recurso de definições **multiplataforma do Profile Management**.

Enable cross-platform settings

Por padrão, para facilitar a implantação, as configurações multi- plataforma são desativadas. Ative o processamento habilitando esta política, mas somente após um planejamento completo e teste desse recurso.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, não será aplicada nenhuma configuração multi-plataforma.

Cross-platform settings user groups

Insira um ou mais grupos de usuários do Windows. Por exemplo, você pode usar essa política para processar apenas os perfis de um grupo de usuários de teste. Se esta política for configurada, o recurso de configurações multi-plataforma do Profile Management processa somente membros desses grupos de usuários. Se esta política estiver desativada, o recurso processa todos os usuários especificados pela política Processed groups.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, todos os grupos de usuários serão processados.

Path to cross-platform definitions

Identifica a localização da 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 esse 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, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, não será aplicada nenhuma configuração multiplataforma.

Path to cross-platform settings store

Define o caminho para o armazenamento de configurações entre plataformas, a pasta na qual as configurações entre plataformas dos usuários são salvas. Os usuários devem ter acesso de gravação a essa área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório home.

Esta área é a área comum do armazenamento do usuário onde os dados de perfil compartilhados por várias plataformas estão localizados. Os usuários devem ter acesso de gravação a essa área. O caminho pode ser um caminho UNC absoluto ou um caminho relativo ao diretório home. Você pode usar as mesmas variáveis usadas em **Path to user store**.

Se esta política estiver desativada, é usado o caminho Windows\PM_CP. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, será usado o valor padrão.

Source for creating cross-platform settings

Especifica uma plataforma como plataforma base se essa política estiver habilitada na UO dessa plataforma. Essa política migra dados dos perfis da plataforma base para o armazenamento de configurações entre plataformas.

O próprio conjunto de perfis de cada plataforma é armazenado em uma UO separada. Você deve decidir quais dados de perfil da plataforma usar para propagar o armazenamento de configurações multiplataformas. É conhecida como a plataforma base. Considere que o armazenamento de configurações entre plataformas contém um arquivo de definição sem dados ou que os dados armazenados em cache em um perfil de plataforma única são mais recentes do que os dados da definição no armazenamento. Nesse caso, o Profile Management migra os dados do perfil de plataforma única para o armazenamento, a menos que você desative essa política.

> **Importante:**
>
> Se essa política estiver habilitada em várias unidades organizacionais, ou em vários objetos de usuário ou de máquina, a plataforma em que o primeiro usuário faz logon se tornará o perfil base.
> Por padrão, esta política é Enabled.

Configurações da política do sistema de arquivos

June 28, 2023

Esta seção contém políticas que definem o seguinte:

- Quais arquivos em um perfil de usuário são sincronizados entre o sistema em que o perfil está instalado e o armazenamento do usuário
- Quais diretórios em um perfil de usuário são sincronizados entre o sistema em que o perfil está instalado e o armazenamento do usuário

Configurações de política de exclusões

June 28, 2023

Esta seção descreve configurações de política para configurar quais arquivos e diretórios em um perfil de usuário são excluídos do processo de sincronização.

Exclusion list - files

Lista de arquivos que são ignorados durante a sincronização. Os nomes dos arquivos devem ser caminhos relativos ao perfil do usuário (%USERPROFILE%). Os caracteres curinga são suportados em nomes de arquivos e em nomes de pastas, mas somente os 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 desativada, nenhum arquivo será excluído. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhum arquivo será excluído.

Enable Default Exclusion List - directories

Lista padrão de diretórios ignorados durante a sincronização. Use esta política para especificar diretórios de exclusão de GPO sem ter de 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 exclui nenhum diretório por padrão.

Exclusion list - directories

Lista de pastas que são ignoradas durante a sincronização. Os nomes das pastas devem ser especificados como caminhos relativos ao perfil do usuário (%USERPROFILE%). Os caracteres curinga nos nomes das pastas são suportados, mas não são aplicados recursivamente.

Exemplo:

- `Desktop` ignora a pasta `Desktop` no perfil do usuário

Se esta política estiver desativada, nenhuma pasta será excluída. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será excluída.

Logon Exclusion Check

Essa configuração define o que o Profile Management faz se um perfil no armazenamento do usuário contiver arquivos ou pastas excluídos. As configurações de política possíveis e as ações correspondentes estão listadas na tabela a seguir:

Configuração da política	Ação
A configuração está desativada ou o valor de "Synchronize excluded files or folders on logon" está definido como padrão	O Profile Management sincroniza os arquivos ou pastas excluídos do armazenamento do usuário com o perfil local quando um usuário faz logon.
A configuração está definida como "Ignore excluded files or folders on logon"	O Profile Management ignora os arquivos ou pastas excluídos no armazenamento do usuário quando um usuário faz logon.
A configuração está definida como "Delete excluded files or folder on logon"	O Profile Management apaga os arquivos ou pastas excluídos no armazenamento do usuário quando um usuário faz logon.

Configuração da política	Ação
A configuração não está definida no Web Studio	O valor do arquivo .ini é usado
A configuração não está definida no Web Studio ou no arquivo .ini	Os arquivos ou pastas excluídos são sincronizados do armazenamento do usuário para um perfil local quando um usuário faz logon.

Manipulação de arquivos grandes - Arquivos que devem ser criados como links simbólicos

Para melhorar o desempenho de logon e processar arquivos de tamanho grande, 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 off-line (`*.ost`) do Microsoft Outlook, verifique se a pasta do **Outlook** não está excluída para Profile Management.

Esses arquivos não podem ser acessados em várias sessões simultaneamente.

Configurações da política de sincronização

June 28, 2023

A seção de **sincronização** descreve as configurações de política para especificar quais arquivos e pastas em um perfil de usuário são sincronizados entre o sistema em que o perfil está instalado e o armazenamento do usuário.

Directories to synchronize

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema em que está instalado e o armazenamento do usuário. Se você excluir uma pasta da sincronização, essa política permitirá incluir as subpastas da pasta excluída de volta à sincronização.

Os caminhos desta lista devem ser relativos ao perfil do usuário. Os caracteres curinga nos nomes das pastas são suportados, mas não são aplicados recursivamente.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, somente pastas não excluídas no perfil de usuário serão sincronizadas.

Files to synchronize

Por padrão, o Profile Management sincroniza o perfil do usuário entre o sistema em que está instalado e o armazenamento do usuário. Se você excluir uma pasta da sincronização, essa política permitirá incluir os arquivos dentro da pasta excluída de volta à sincronização.

Os caminhos desta lista devem ser relativos ao perfil do usuário. Os caracteres curinga são suportados em nomes de arquivos e em nomes de pastas, mas somente os curingas em nomes de arquivos são aplicados recursivamente. Os 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 essa política tem o mesmo efeito que ativá-la e configurar uma lista vazia.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, somente os arquivos não excluídos no perfil do usuário serão sincronizados.

Folders to mirror

Essa política permite a você resolver problemas que envolvam qualquer pasta transacional (também conhecida como pasta referencial). Essa pasta contém arquivos interdependentes, onde um arquivo faz referência ao outro.

O espelhamento de pastas habilita o Profile Management para processar uma pasta transacional e seu conteúdo como uma única entidade, evitando o inchaço do perfil. Por exemplo, você pode espelhar a pasta de **cookies do Internet Explorer** para que Index.dat seja sincronizado com os cookies indexados. Nestas situações, a "última gravação prevalece". Assim, os arquivos em pastas espelhadas que foram modificados em mais de uma sessão são substituídos pela última atualização, resultando em perda de alterações de perfil.

Por exemplo, a tabela a seguir descreve como o Index.dat faz referência a cookies enquanto um usuário navega na Internet:

Cenário	Como o Index.dat faz referência a cookies
—	—
Um usuário tem duas sessões do Internet Explorer, cada uma em um servidor diferente, e visita sites diferentes em cada sessão. |Os cookies de cada site são adicionados ao servidor apropriado.| Os cookies de cada site são adicionados ao servidor apropriado.
O usuário faz logoff da primeira sessão ou no meio de uma sessão (se o recurso de gravação ativa estiver configurado)	Os cookies da segunda sessão devem substituir os cookies da primeira sessão.
A primeira e a segunda sessões são mescladas e as referências aos cookies no Index.dat ficam desatualizadas	Navegação adicional em novas sessões resulta em mesclagem repetida e uma pasta de cookies sobrecarregada

Espelhar a pasta de cookies resolve o problema. Nesse caso, os cookies são substituídos pelos cookies da última sessão cada vez que o usuário faz logoff. Assim, o Index.dat permanece atualizado.

Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui ou no arquivo .ini, nenhuma pasta será espelhada.

Accelerate folder mirroring

Com essa política e a política **Folders to mirror** habilitadas, o **Profile Management** armazena pastas espelhadas em um disco virtual baseado em VHDX. Ele conecta o disco virtual durante os logons e o desconecta durante os logoffs. A ativação dessa 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

June 28, 2023

Esta seção contém configurações de política que especificam se deseja redirecionar pastas que geralmente aparecem em perfis para um local de rede compartilhada.

Grant administrator access

Essa configuração permite que um administrador acesse o conteúdo das pastas redirecionadas de um usuário.

> **Nota:**
>
> Essa configuração concede permissões a administradores que têm acesso completo e irrestrito ao domínio.

Por padrão, essa configuração está desativada e os usuários recebem acesso exclusivo ao conteúdo de suas pastas redirecionadas.

Include domain name

Essa configuração permite a inclusão da variável de ambiente `%userdomain%` como parte do caminho UNC. Esse caminho UNC é especificado para pastas redirecionadas.

Por padrão, essa configuração está desativada. E a variável de ambiente `%userdomain%` não está incluída como parte do caminho UNC especificado para pastas redirecionadas.

Configurações de política AppData (Roaming)

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **AppData (Roaming)** para um local de rede compartilhada.

AppData(Roaming) path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **AppData (Roaming)** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for AppData(Roaming)

Essa configuração especifica como redirecionar o conteúdo da pasta **AppData (Roaming)**.

Por padrão, os conteúdos são redirecionados para um caminho UNC. Para obter mais informações, consulte a seção Path to user store.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de contatos

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Contatos** para um local de rede compartilhada.

Contacts path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Contatos** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Contacts

Essa configuração especifica como redirecionar o conteúdo da pasta **Contatos**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de Desktop

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta `Desktop` para um local de rede compartilhada.

Desktop path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Desktop** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Desktop

Essa configuração especifica como redirecionar o conteúdo da pasta **Desktop**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de documentos

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Documentos** para um local de rede compartilhada.

Documents path

Essa configuração especifica o local de rede para o qual os arquivos na pasta **Documentos** são redirecionados.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

A configuração **Documents path** deve estar ativada não apenas para redirecionar arquivos para a pasta **Documentos**, mas também direcionar arquivos para as pastas **Música**, **Imagens** e **Vídeos**.

Redirection settings for Documents

Essa configuração especifica como redirecionar o conteúdo da pasta **Documentos**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Documentos**, escolha uma das seguintes opções:

- Redirect to the following UNC path. Redireciona o conteúdo para o caminho UNC especificado na configuração de política de caminho Documentos.
- Redirect to the users home directory. Redireciona o conteúdo para o diretório home dos usuários, normalmente configurado como o atributo #homeDirectory# para um usuário no Active Directory.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de downloads

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Downloads** para um local de rede compartilhada.

Downloads path

Essa configuração especifica o local de rede para o qual os arquivos na pasta **Downloads** são redirecionados.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Downloads

Essa configuração especifica como redirecionar o conteúdo da pasta **Downloads**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de favoritos

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Favoritos** para um local de rede compartilhada.

Favorites path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Favoritos** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Favorites

Essa configuração especifica como redirecionar o conteúdo da pasta **Favoritos**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de links

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Links** para um local de rede compartilhada.

Links path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Links** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Links

Essa configuração especifica como redirecionar o conteúdo da pasta **Links**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de música

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Música** para um local de rede compartilhada.

Music path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Música** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Music

Esta configuração especifica como redirecionar o conteúdo da pasta **Música**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Música**, escolha uma das seguintes opções:

- Redirect to the following UNC path. Redireciona o conteúdo para o caminho UNC especificado na configuração de política Caminho de música.
- Redirect relative to Documents folder. Redireciona o conteúdo para uma pasta relativa à pasta Documentos.

Para redirecionar o conteúdo para uma pasta relativa à pasta **Documentos**, a configuração de **Documents path** deve estar ativada.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de fotos

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Imagens** para um local de rede compartilhada.

Pictures path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Imagens** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Redirection settings for Pictures

Esta configuração especifica como redirecionar o conteúdo da pasta **Imagens**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Imagens**, escolha uma das seguintes opções:

- Redirect to the following UNC path. Redireciona o conteúdo para o caminho UNC especificado na configuração de política de caminho Imagens.
- Redirect relative to Documents folder. Redireciona o conteúdo para uma pasta relativa à pasta Documentos.

Para redirecionar o conteúdo para uma pasta relativa à pasta **Documentos**, a configuração de **Documents path** deve estar ativada.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de Jogos Salvos

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Jogos Salvos** para um local de rede compartilhada.

Redirection settings for Saved Games

Essa configuração especifica como redirecionar o conteúdo da pasta **Jogos Salvos**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Saved Games path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Jogos Salvos** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política do menu Iniciar

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Menu Iniciar** para um local de rede compartilhada.

Redirection settings for Start Menu

Esta configuração especifica como redirecionar o conteúdo da pasta **Menu Iniciar**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Start Menu path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Menu Iniciar** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de pesquisa

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Pesquisas** para um local de rede compartilhada.

Redirection settings for Searches

Essa configuração especifica como redirecionar o conteúdo da pasta **Pesquisas**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Searches path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Pesquisas** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações da política de vídeo

June 28, 2023

Esta seção contém configurações de política para redirecionar o conteúdo da pasta **Vídeo** para um local de rede compartilhada.

Redirection settings for Video

Essa configuração especifica como redirecionar o conteúdo da pasta **Vídeo**.

Por padrão, os conteúdos são redirecionados para um caminho UNC.

Para controlar como redirecionar o conteúdo da pasta **Vídeo**, escolha uma das seguintes opções:

- Redirect to the following UNC path. Redireciona o conteúdo para o caminho UNC especificado na configuração de política de caminho de Vídeo.
- Redirect relative to Documents folder. Redireciona o conteúdo para uma pasta relativa à pasta Documentos.

Para redirecionar o conteúdo para uma pasta relativa à pasta **Documentos**, a configuração de **Documents path** deve estar ativada.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Video path

Essa configuração especifica o local de rede para o qual o conteúdo da pasta **Vídeo** é redirecionado.

Por padrão, essa configuração está desativada e não é especificado nenhum local.

Se essa configuração não estiver definida aqui, o Profile Management não redirecionará a pasta especificada.

Configurações de política de registro em log

June 28, 2023

Esta seção contém configurações de política que configuram o registro em log do Profile Management.

Active Directory actions

Essa configuração ativa ou desativa o registro detalhado das ações realizadas no Active Directory.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida no Web Studio, o valor do arquivo .ini será usado.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Common information

Essa configuração ativa ou desativa o registro detalhado de informações comuns.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Common warnings

Essa configuração ativa ou desativa o registro detalhado de avisos comuns.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Enable logging

Essa configuração ativa ou desativa o registro em log do Profile Management no modo de depuração (log detalhado). No modo de depuração, são registradas informações detalhadas de status nos arquivos de log localizados em "%SystemRoot%\System32\Logfiles\UserProfileManager".

Por padrão, essa configuração está desabilitada e somente os erros são registrados.

A Citrix recomenda ativar essa configuração somente se você estiver solucionando problemas do Profile Management.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, somente os erros serão registrados.

File system actions

Essa configuração ativa ou desativa o registro detalhado das ações realizadas no sistema de arquivos.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

File system notifications

Essa configuração ativa ou desativa o registro detalhado de notificações de sistemas de arquivos.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Logoff

Essa configuração ativa ou desativa o registro detalhado de logoffs de usuários.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Logon

Essa configuração ativa ou desativa o registro detalhado de logons de usuários.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Maximum size of the log file

Essa configuração especifica o tamanho máximo permitido para o arquivo de log do Profile Management, em bytes.

Por padrão, esse valor é definido como 1048576 bytes (1 MB).

A Citrix recomenda aumentar o tamanho desse arquivo para 5 MB ou mais, se você tiver espaço em disco suficiente. Se o arquivo de log ultrapassar o tamanho máximo:

- Um backup existente do arquivo (.bak) é excluído
- O arquivo de log é renomeado para .bak
- Um novo arquivo de log é criado

O arquivo de log é criado em %SystemRoot%\System32\Logfiles\UserProfileManager.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, será usado o valor padrão.

Path to log file

Essa configuração especifica um caminho alternativo para salvar o arquivo de log do Profile Management.

Por padrão, essa configuração está desativada 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 remota baseada em rede (caminho UNC). Os caminhos remotos podem ser úteis em grandes ambientes distribuídos, mas podem gerar uma intensidade significativa de tráfego de rede, o que pode ser inapropriado para arquivos de log. Para máquinas virtuais provisionadas com um disco rígido persistente, defina um caminho local para essa unidade. Essa configuração garante que os arquivos de log sejam preservados quando a máquina é reiniciada. Para máquinas virtuais sem um disco rígido persistente, definir um caminho

UNC permite que você retenha os arquivos de log. No entanto, a conta do sistema para as máquinas deve ter acesso de gravação ao compartilhamento UNC. Use um caminho local para todos os laptops gerenciados pelo recurso perfis off-line.

Se um caminho UNC for usado para arquivos de log, a Citrix recomenda que uma lista de controle de acesso apropriada seja aplicada à pasta do arquivo de log. Essa configuração garante que somente contas de usuário ou computador autorizadas possam acessar os arquivos armazenados.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo.ini, será usado o local padrão %SystemRoot%\System32\Logfiles\UserProfileManager.

Personalized user information

Essa configuração ativa ou desativa o registro detalhado de informações personalizadas do usuário.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Policy values at logon and logoff

Essa configuração ativa ou desativa o registro detalhado dos valores da política quando um usuário faz logon e logoff.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Registry actions

Essa configuração ativa ou desativa o registro detalhado das ações realizadas no registro.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Registry differences at logoff

Essa configuração ativa ou desativa o registro detalhado de eventuais diferenças no registro quando um usuário faz logoff.

Por padrão, essa configuração está desativada.

Ao habilitar essa configuração, verifique se a configuração **Enable logging** também está ativada.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida no Web Studio ou no arquivo .ini, o seguinte log será registrado:

- Erros
- Informações gerais

Configurações de política de tratamento de perfis

June 28, 2023

Esta seção inclui configurações de política que especificam como o Profile Management lida com perfis de usuário.

Delay before deleting cached profiles

Essa configuração especifica uma extensão opcional para o atraso, em minutos, antes que o Profile Management exclua perfis armazenados localmente em cache no logoff.

Um valor de 0 exclui os perfis imediatamente no final do processo de logoff. O Profile Management verifica se há logoffs a cada minuto. Como resultado, um valor de 60 garante que os perfis sejam excluídos entre um e dois minutos após o logoff dos usuários. Essa ação depende de quando a última verificação ocorreu. Estender o atraso é útil se você souber que um processo mantém os arquivos ou a colmeia do registro do usuário aberta durante o logoff. Com perfis grandes, esse processo também pode acelerar o logoff.

Por padrão, esse valor é definido como 0 e o Profile Management exclui perfis armazenados localmente em cache imediatamente.

Ao habilitar essa configuração, verifique se a opção Excluir perfis armazenados em cache local no logoff também está habilitado.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, os perfis serão excluídos imediatamente.

Delete locally cached profiles on logoff

Essa configuração especifica se os perfis armazenados em cache local são excluídos depois que um usuário faz logoff.

Quando essa configuração está ativada, o cache de perfil local de um usuário é excluído depois que ele tiver feito logoff. A Citrix recomenda ativar essa configuração para servidores de terminal.

Por padrão, essa configuração é desabilitada e um cache de perfil local de usuários é retido depois que eles fazem logoff.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, os perfis armazenados em cache não serão excluídos.

Local profile conflict handling

Essa configuração define como o Profile Management se comporta se um perfil de usuário existir nos dois itens a seguir:

- Armazenamento do usuário
- Perfil do usuário Windows local (não é um perfil do 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 o perfil local. O Profile Management usa o perfil local, mas não o altera de nenhum modo.
- Excluir o perfil local. O Profile Management exclui o perfil de usuário local do Windows e, em seguida, importa o perfil de usuário Citrix do armazenamento do usuário.
- Renomear o 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 do usuário.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, os perfis locais existentes serão usados.

Migration of existing profiles

Essa configuração especifica os tipos de perfil migrados para o armazenamento do usuário durante o logon se um usuário não tiver nenhum perfil atual no armazenamento do usuário.

O Profile Management pode migrar perfis existentes diretamente durante o logon se um usuário não tiver perfil no armazenamento do usuário. Depois disso, o perfil do armazenamento do usuário é usado pelo Profile Management nos dois itens a seguir:

- Sessão atual
- Qualquer outra sessão configurada com o caminho para o mesmo armazenamento do usuário

Por padrão, os perfis locais e de roaming são migrados para o armazenamento de usuários durante o logon.

Para especificar os tipos de perfil migrados para o armazenamento de usuários durante o logon, escolha uma das seguintes opções:

- Local and roaming profiles
- Local
- Roaming
- None (desativado)

Se você selecionar **None**, o sistema usará o mecanismo existente do Windows para criar perfis, como se estivesse em um ambiente em que o Profile Management não esteja instalado.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, os perfis locais e de roaming existentes serão migrados.

Automatic migration of existing application profiles

Essa configuração ativa ou desativa a migração automática de perfis de aplicativos existentes em diferentes sistemas operacionais. Os perfis do aplicativo incluem os dados do aplicativo na pasta `AppData` e as entradas do registro em `HKEY_CURRENT_USER\SOFTWARE`. Essa configuração pode ser útil nos casos em que você deseja migrar seus perfis de aplicativos entre diferentes sistemas operacionais.

Por exemplo, suponha que você atualize seu sistema operacional (OS) do Windows 10 versão 1803 para o Windows 10 versão 1809. Se essa configuração estiver ativada, o Profile Management migrará automaticamente as configurações do aplicativo existentes para o Windows 10 versão 1809 na primeira vez que cada usuário fizer logon. Como resultado, os dados do aplicativo na pasta `AppData` e as entradas de registro em HKEY_CURRENT_USER\SOFTWARE são migrados.

Se houver vários perfis de aplicativo existentes, o Profile Management executará 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 multissessão para SO multissessão).
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 sistema operacional; por exemplo, Windows 7 para Windows 10, ou Windows Server 2012 para Windows 2016.
4. Perfis do sistema operacional mais próximo.

Nota: Você deve especificar o nome abreviado do sistema operacional, incluindo a variável "!CTX_OSNAME!"no caminho do armazenamento do usuário. Isso permite que o Profile Management localize os perfis de aplicativos existentes.

Se essa configuração não estiver definida aqui, será usada a configuração do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, ela será desativada por padrão.

Path to the template profile

Essa configuração especifica o caminho para o perfil que você deseja que o Profile Management use como modelo para criar perfis de usuário.

O caminho especificado deve ser o caminho completo para a pasta que contém o arquivo de registro NTUSER.DAT e quaisquer outras pastas e arquivos necessários para o perfil do modelo.

Nota: Não inclua NTUSER.DAT no caminho. Por exemplo, com o arquivo \\myservername\myprofiles\template\ntu
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.

Observação: essa configuração não oferece suporte à expansão de atributos do Active Directory, variáveis de ambiente do sistema ou variáveis %USERDOMAIN% e %USERNAME%.

Por padrão, essa configuração é desativada e são criados novos perfis de usuário a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, nenhum modelo será usado.

Template profile overrides local profile

Essa configuração permite que o perfil do modelo substitua o perfil local ao criar perfis de usuário.

Considere que um usuário não tenha um perfil de usuário Citrix, mas tenha um perfil de usuário local do Windows. Nesse caso, por padrão, o perfil local é usado e migrado para o armazenamento do usuário, se esse valor estiver habilitado. A ativação dessa configuração de política permite que o perfil do modelo substitua o perfil local usado ao criar perfis de usuário.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, nenhum modelo será usado.

Template profile overrides roaming profile

Essa configuração permite que o perfil de modelo substitua um perfil de roaming ao criar perfis de usuário.

Considere que um usuário não tenha um perfil de usuário Citrix, mas tenha um perfil de usuário de roaming do Windows. Nesse caso, por padrão, o perfil de roaming é usado e migrado para o armazenamento do usuário, se esse valor estiver habilitado. Habilitar essa configuração de política permite que o perfil de modelo substitua o perfil de roaming usado ao criar perfis de usuário.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, nenhum modelo será usado.

Template profile used as a Citrix mandatory profile for all logons

Essa configuração permite que o Profile Management use o perfil de modelo como o perfil padrão para criar todos os perfis de usuário.

Por padrão, essa configuração é desativada e são criados novos perfis de usuário a partir do perfil de usuário padrão no dispositivo onde um usuário faz logon pela primeira vez.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, nenhum modelo será usado.

Configurações de política de registro

June 28, 2023

Esta seção contém configurações de política que especificam quais chaves de registro estão incluídas ou excluídas do processamento do Profile Management.

Exclusion list

Lista de chaves de registro no hive HKCU que são ignoradas durante o logoff.

Exemplo: Software\Policies

Se esta política estiver desativada, nenhuma chave de registro será excluída. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui nem no arquivo .ini, nenhuma chave de registro será excluída.

Inclusion list

Lista de chaves de registro no hive HKCU que são processadas durante o logoff.

Exemplo: Software\Adobe.

Se esta política estiver habilitada, somente as chaves nesta lista serão processadas. Se esta política é desabilitada, será processado o hive HKCU completo. Se esta política não estiver configurada aqui, será usado o valor do arquivo .ini. Se esta política não estiver configurada aqui nem no arquivo .ini, todo o HKCU está processado.

Ativar lista de exclusão padrão - Profile Management 5.5

Lista padrão de chaves de registro no hive HKCU que não são sincronizadas com o perfil do usuário. Use esta política para especificar arquivos de exclusão de GPO sem ter que preenchê-los manualmente.

Se você desabilitar esta política, o Profile Management não excluirá nenhuma chave de registro por padrão. Se você não configurar esta política aqui, o Profile Management usará o valor do arquivo .ini. Se você não configurar esta política aqui ou no arquivo.ini, o Profile Management não excluirá nenhuma chave de registro por padrão.

NTUSER.DAT backup

Permite um backup da última cópia boa conhecida do NTUSER.DAT e reversão se corrompido.

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 fará backup de NTUSER.DAT.

Configurações de política de perfis de usuário transmitidos

June 28, 2023

Esta seção contém configurações de política que especificam como o Profile Management processa os perfis de usuário transmitidos.

Always cache

Essa configuração especifica se o Profile Management armazena em cache os arquivos transmitidos o mais rápido possível após o logon do usuário. O cache de arquivos depois que um usuário faz logon salva a largura de banda da rede, melhorando a experiência do usuário.

Use essa configuração com a configuração **Profile streaming**.

Por padrão, essa configuração está desabilitada e os arquivos transmitidos não são armazenados em cache assim que possível após o logon do usuário.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, ela está desativada.

Always cache size

Essa configuração especifica um limite inferior, em MB, sobre o tamanho dos arquivos que são transmitidos. O Profile Management armazena em cache todos os arquivos desse tamanho ou maior o mais rápido possível após um usuário efetuar logon.

Por padrão, o valor é definido como 0 (zero) e o recurso de perfil inteiro do cache é usado. Quando o recurso de perfil inteiro do cache é ativado, o Profile Management busca todo o conteúdo do perfil no armazenamento do usuário, depois que um usuário faz logon, como uma tarefa em segundo plano.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, ela está desativada.

Profile streaming

Essa configuração ativa e desativa o recurso de perfis de usuário transmitidos do Citrix. Quando ativado, os arquivos e pastas de perfil são obtidos do armazenamento do usuário para o computador local somente quando os usuários os acessam após o logon. As entradas de registro e arquivos na área pendente são buscados imediatamente.

Por padrão, o fluxo de perfil é desativado.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, ela está desativada.

Streamed user profile groups

Essa configuração especifica quais perfis de usuário dentro de uma unidade organizacional são transmitidos, com base em grupos de usuários do Windows.

Quando ativado, somente os perfis de usuário dentro dos grupos de usuários especificados são transmitidos. Todos os outros perfis de usuário são processados normalmente.

Por padrão, essa configuração está desativada e todos os perfis de usuário dentro de uma unidade organizacional são processados normalmente.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, todos os perfis de usuário serão processados.

Enable profile streaming exclusion

Quando a exclusão de streaming de perfil estiver ativada:

- O Profile Management não transmite pastas na lista de exclusão
- Todas as pastas são obtidas imediatamente do armazenamento do usuário para o computador local quando um usuário faz logon

Para obter mais informações, consulte Stream user profiles.

Timeout for pending area lock files

Essa configuração especifica o número de dias após os quais os arquivos dos usuários são gravados de volta no armazenamento de usuários a partir da área pendente, caso o armazenamento do usuário permaneça bloqueado quando um servidor de armazenamento ficar sem resposta. Esse comportamento evita a sobrecarga na área pendente e garante que o armazenamento do usuário sempre contenha os arquivos mais atualizados.

Por padrão, essa configuração é definida como 1 (um) dia.

Se essa configuração não estiver definida aqui, será usado o valor do arquivo .ini.

Se essa configuração não estiver definida aqui nem no arquivo .ini, será usado o valor padrão.

Enable profile streaming for pending area

Permite ativar o recurso de streaming de perfil para arquivos e pastas na área pendente.

A área pendente é usada para garantir a consistência do perfil enquanto o streaming de perfis está ativado. Ela armazena temporariamente pastas e arquivos de perfil alterados em sessões simultâneas.

Por padrão, essa política está desativada e todos os arquivos e pastas na área pendente são obtidos do perfil local no logon. Com essa política ativada, os arquivos na área pendente são obtidos do perfil local somente quando solicitados. Use a política com a política de streaming de perfis para garantir uma experiência de logon ideal em cenários de sessões simultâneas.

A política se aplica a pastas na área pendente quando a política Enable profile streaming for folders está ativada.

Configurações da política da camada de personalização do usuário

June 28, 2023

Para habilitar a montagem de camadas de usuário em Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Em que ponto da rede acessar as camadas do usuário.
- O quanto os discos novos de camada de usuário pode crescer.

Para fazer isso, estas duas políticas aparecem na lista de políticas disponíveis:

- Caminho do Repositório da Camada de Usuário - Insira um caminho no formato ‘\nome do servidor ou endereço\nome da pasta’ no campo Value.

- User Layer Size GB - O tamanho padrão da camada de usuário de 10 GB é o mínimo que a Citrix recomenda. Uma camada de usuário é um disco com provisionamento dinâmico que se expande para o tamanho definido à medida que o espaço é usado. As camadas do usuário nunca diminuem de tamanho.

> **Nota:**
>
> O aumento do tamanho da camada de usuário afeta novas camadas de usuário e expande as existentes. A diminuição do 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

June 28, 2023

A seção Virtual Delivery Agent (VDA) contém configurações de política que controlam a comunicação entre o VDA e os controladores de um site.

Importante: o VDA requer informações fornecidas por essas configurações para se registrar com 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:

- Controller registration IPv6 netmask
- Controller registration port
- Controller SIDs
- Controllers
- Only use IPv6 controller registration
- Site GUID

Controller registration IPv6 netmask

Essa configuração de política permite que os administradores restrinjam o VDA a apenas uma sub-rede preferencial (em vez de um IP global, se houver uma já registrada). Essa configuração especifica o endereço IPv6 e a rede em que o VDA se registra. O VDA se registra somente no primeiro endereço que corresponde com a máscara de rede especificada. Esta configuração é válida somente se a configuração da política Only use IPv6 controller registration estiver ativada.

Por padrão, esta configuração está em branco.

Controller registration port

Use essa configuração somente se a configuração **Enable auto update of controllers** estiver desativada.

Essa configuração especifica o número da porta TCP/IP que o VDA usa para se registrar em um Controller ao usar o registro baseado no registro do sistema.

Por padrão, o número da porta é definido como 80.

Controller SIDs

Use essa configuração somente se a configuração **Enable auto update of controllers** estiver desativada.

Essa configuração especifica uma lista separada por espaço de identificadores de segurança (SIDs) do controlador que o VDA usa para registrar com um controlador ao usar o registro baseado no registro do sistema. Esta configuração é opcional e pode ser usada com a configuração **Controllers** para restringir a lista de controladores usados para registro.

Por padrão, essa configuração está em branco.

Controllers

Use essa configuração somente se a configuração **Enable auto update of controllers** estiver desativada.

Essa configuração especifica uma lista separada por espaço de nomes de domínio totalmente qualificados (FQDNs) do controlador que o VDA usa para registrar com um controlador ao usar o registro baseado no registro do sistema. Essa configuração é opcional e pode ser usada com a configuração dos **SIDs do controlador**.

Por padrão, essa configuração está em branco.

Enable auto update of controllers

Essa configuração permite que o VDA se registre com um controlador automaticamente após a instalação.

Depois que o VDA registra, o controlador com o qual se registrou envia uma lista do controlador atual FQDNS e SIDs ao VDA. O VDA grava esta lista no armazenamento persistente. Cada controlador também verifica o banco de dados do site a cada 90 minutos para obter informações sobre o Controller. O controlador envia listas atualizadas para seus VDAs registrados se ocorrer uma das seguintes situações:

- Um controlador foi adicionado ou removido desde a última verificação
- Ocorreu uma mudança de política

O VDA aceita conexões de todos os controladores na lista mais recente que recebeu.

Por padrão, essa configuração está ativada.

Only use IPv6 controller registration

Esta configuração controla qual a forma de endereço que o VDA usa para se registrar com o controlador:

- Quando ativado, o VDA registra com o controlador usando o endereço IPv6 da máquina. Quando o VDA se comunica com o controlador, ele usa a seguinte ordem de endereços: endereço IP global, Unique Local Address (ULA), endereço local de link (se nenhum outro endereço IPv6 estiver disponível).
- Quando desativado, o VDA registra e se comunica com o Controlador usando o endereço IPv4 da máquina.

Por padrão, essa configuração está desativada.

Site GUID

Use essa configuração somente se a configuração **Enable auto update of controllers** estiver desativada.

Essa configuração especifica o Globally Unique Identifier (GUID) do site que o VDA usa para se registrar em um Controller ao usar o registro baseado no Active Directory.

Por padrão, essa configuração está em branco.

Configurações da política HDX 3D Pro

June 28, 2023

A seção HDX 3D Pro inclui configurações de política para habilitar e configurar a ferramenta de configuração de qualidade de imagem para os usuários. Essa ferramenta permite que os usuários otimizem o uso da largura de banda disponível. Para essa otimização, o equilíbrio entre qualidade de imagem e capacidade de resposta é ajustado em tempo real.

Enable lossless

Essa configuração especifica se os usuários podem ativar e desativar a compactação sem perdas usando a ferramenta de configuração de qualidade de imagem. Por padrão, os usuários não têm a opção de ativar a compactação sem perdas.

Considere que um usuário habilita a compactação sem perdas. Nesse caso, 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 em função dos recursos do dispositivo do usuário e do computador host.

HDX 3D Pro quality settings

Essa configuração especifica os valores mínimo e máximo disponíveis para os usuários na ferramenta de configuração de qualidade de imagem. Usando esses valores, os usuários podem definir a faixa de ajuste de qualidade de imagem na ferramenta de configuração de qualidade de imagem.

Especifique valores de qualidade de imagem entre 0 e 100, inclusive. O valor máximo deve ser maior ou igual ao valor mínimo.

Configurações da política de monitoramento

June 28, 2023

A seção **Monitoring** inclui configurações de política para monitoramento de processos, monitoramento de recursos e monitoramento de falhas de aplicativos.

O escopo dessas políticas pode ser definido com base no seguinte:

- Site
- Grupo de entrega
- Tipo de grupo de entrega
- Unidade organizacional
- Marcas

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 armazená-los consome espaço considerável no banco de dados de monitoramento. Considere

que você não deseja monitorar dados de recursos ou dados de processo ou ambos para um escopo específico. Por exemplo, um grupo de entrega ou unidade organizacional específicos. Nesse caso, é recomendável desativar a política.

Enable process monitoring

Ative essa configuração para permitir o monitoramento de processos em execução em máquinas com VDAs. Estatísticas como CPU e uso de 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 essa configuração é Disabled.

Enable resource monitoring

Ative essa configuração para permitir o monitoramento de contadores de desempenho críticos em máquinas com VDAs. Estatísticas (como CPU e uso de 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 essa configuração é Enabled.

Escalabilidade

Os dados da CPU e da memória são enviados para o banco de dados de cada VDA em intervalos de 5 minutos. Os dados do processo (se ativado) 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 uma hora.

CPU and memory data

A opção CPU and memory data está **ativada** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

Granularidade de dados	Número de dias
Dados de 5 minutos	1 dia
Dados de 10 minutos	7 dias
Dados horários	30 dias
Dados diários	90 dias

IOPS and disk latency data

A opção IOPS and disk latency data está **ativada** por padrão. Os valores de retenção de dados são os seguintes (licença Platinum):

Granularidade de dados	Número de dias
Dados horários	3 dias
Dados diários	90 dias

Com as configurações de retenção de dados, aproximadamente 276 KB de espaço em disco são necessários para armazenar o seguinte para um VDA durante um período de um ano:

- CPU
- Memória
- IOPS
- Dados de latência de disco

Número de máquinas	Armazenamento aproximado necessário
1	276 KB
1.000	270 MB
40.000	10,6 GB

Process data

A opção Process data está **desativada** por padrão. Recomenda-se ativar os dados de processo em um subconjunto de máquinas conforme a necessidade. As configurações padrão de retenção de dados para os dados do processo são as seguintes:

Granularidade de dados	Número de dias
Dados de 10 minutos	1 dia
Dados horários	7 dias

Se os dados do processo estiverem ativados com as configurações de retenção padrão, os dados do processo consumiriam aproximadamente 1,5 MB por VDA e 3 MB por VDA dos Serviços de Terminal (TS VDA) durante um período de um ano.

Número de máquinas	Armazenamento aproximado necessário VDA	Armazenamento aproximado necessário TS VDA
1	1,5 MB	3 MB
1.000	1,5 GB	3 GB

> **Nota:**
>
> Os números fornecidos anteriormente não incluem o espaço de Índice. Todos os cálculos são aproximados e variam dependendo da implantação.

Configurações opcionais

Você pode modificar as configurações de retenção padrão para atender às suas necessidades. No entanto, essa configuração consome armazenamento extra. Ao ativar as configurações abaixo, você pode obter mais precisão nos dados de utilização do processo. As configurações que podem ser ativadas são:

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

Estas configurações podem ser ativadas a partir do cmdlet Monitoring PowerShell: Set-MonitorConfiguration

Políticas para monitoramento de falhas de aplicativos

A guia **Application Failure**, por padrão, exibe apenas falhas de aplicativo de VDAs de SO multissessão. As configurações do monitoramento de falhas de aplicativo podem ser modificadas com as seguintes políticas de monitoramento:

Enable monitoring of application failures

Use essa configuração para configurar o monitoramento de falhas do aplicativo para monitorar erros ou falhas do aplicativo (falhas e exceções não processadas) ou ambas.
Desative o monitoramento de falha do aplicativo definindo o **Value** como **None**.
O padrão para essa configuração é Application faults only.

Enable monitoring of application failures on Single-session OS VDAs

Por padrão, as falhas somente de aplicativos hospedados nos VDAs de SO multissessão são monitoradas. Para monitorar VDAs de SO de sessão única, defina a política como **Allowed**.
O padrão para essa configuração é **Prohibited**.

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 de coleta de dados do Performance Analytics

Coleta de dados de VDA do Performance Analytics

Use a política para habilitar ou desabilitar o serviço Monitor de coletar métricas relacionadas ao desempenho dos VDAs para o Performance Analytics. Por padrão, a política é **Allowed**. Defina a política como **Prohibited** 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 recursos ou dados do processo, qualquer um deles ou ambos podem ser desativados usando a política de grupo. Para obter mais informações, consulte a seção **Group Policy** em Criar políticas.

Limpeza de dados. As configurações padrão de retenção de dados podem ser modificadas para limpar os dados antecipadamente e liberar espaço de armazenamento. Para obter mais informações sobre configurações de limpeza, consulte Granularidade e retenção de dados em Acesso a dados usando a API.

Configurações da política de IP virtual

June 28, 2023

> **Importante:**
>
> O Windows 10 Enterprise multissessão não suporta Virtualização IP de Área de Trabalho Remota

> (IP Virtual) e não oferecemos suporte a IP virtual nem loopback virtual em Windows 10 Enterprise multissessão.

A seção **IP virtual** inclui configurações de política que controlam se as sessões têm seu próprio endereço de loopback virtual.

Virtual IP loopback support

Quando essa configuração está ativada, cada sessão tem seu próprio endereço de loopback virtual. Quando desativadas, as sessões não têm endereços de loopback separados.

Por padrão, essa configuração está desativada.

Virtual IP virtual loopback programs list

Essa configuração especifica os executáveis do aplicativo que podem usar endereços de loopback virtuais. Ao adicionar programas à lista, especifique apenas o nome do executável. Você não precisa especificar o caminho todo.

Por padrão, não é especificado nenhum executável.

Definições da configuração de redirecionamento da Porta COM e Porta LPT usando o registro

June 28, 2023

Nas versões de VDA 7.0 a 7.8, as configurações da **porta COM e porta LPT** são configuráveis somente usando o registro. Para versões VDA anteriores a 7.0 e para VDA versões 7.9 e posteriores, essas configurações são configuráveis no Web Studio. Para obter mais informações, consulte Configurações de política de redirecionamento de porta e Configurações da política de largura de banda.

As configurações de política para porta COM e redirecionamento de porta LPT estão localizadas em HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated na imagem ou na máquina VDA.

Para habilitar a porta COM e o redirecionamento de porta LPT, adicione novas chaves de registro do tipo REG_DWORD, da seguinte forma:

Cuidado: editar o registro incorretamente pode causar sérios problemas que poderão exigir que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Chave do registro	Descrição	Valores permitidos
AllowComPortRedirection	Permitir ou proibir o redirecionamento da porta COM	1 (Permitir) ou 0 (Proibir)
LimitComBw	Limite de largura de banda para 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
AutoConnectClientComPorts	Conectar automaticamente as portas COM do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)
AllowLptPortRedirection	Permitir ou proibir o redirecionamento da porta LPT	1 (Permitir) ou 0 (Proibir)
LimitLptBw	Limite de largura de banda para o canal de redirecionamento 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	Conecte automaticamente portas LPT a partir do dispositivo do usuário	1 (Permitir) ou 0 (Proibir)

Depois de definir essas configurações, altere os catálogos de máquinas para usar a nova imagem mestre ou a máquina física atualizada. As áreas de trabalho são atualizadas com as novas configurações na próxima vez que os usuários efetuarem logoff.

Configurações da política do Connector for Configuration Manager 2012

June 28, 2023

A seção Connector for Configuration Manager 2012 contém configurações de política para configurar o agente Citrix Connector 7.5.

> **Importante:**
>
> As políticas de aviso, logoff e mensagem de reinicialização se aplicam apenas a implantações em catálogos de máquinas com SO multissessão gerenciados manualmente ou pelos Provisioning Services. Para esses catálogos de máquinas, o serviço Connector alerta os usuários quando há instalações pendentes de aplicativos ou atualizações de software.

Para catálogos gerenciados pelo MCS, use o Web Studio para notificar os usuários. Para catálogos de SO de sessão única gerenciados manualmente, use o Configuration Manager para notificar os usuários. Para catálogos de SO de sessão única gerenciados pelos Provisioning Services, use os Provisioning Services para notificar os usuários.

Intervalo de frequência de advertência

Esta configuração define o intervalo entre as aparências da mensagem de aviso para os usuários.

Os intervalos são definidos usando o formato ddd.hh:mm:ss, onde:

- ddd representa dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh representa horas com um intervalo de 0-23.
- mm representa minutos com um intervalo de 0-59.
- ss representa segundos com um intervalo de 0-59.

Por padrão, a configuração de intervalo é de 1 hora (01:00:00).

Texto corpo da caixa de mensagem de aviso

Esta configuração contém o texto editável da mensagem aos usuários notificando-os das próximas atualizações de software ou manutenção que exigem que eles façam logoff.

Por padrão, a mensagem é: {TIMESTAMP} Save your work. The server goes offline for maintenance in {TIMELEFT}.

Warning message box title

Essa configuração contém o texto editável da barra de título da mensagem de aviso aos usuários.

Por padrão, o título é: Upcoming Maintenance

Warning time period

Essa configuração define até que ponto antes da manutenção a mensagem de aviso aparece pela primeira vez.

A hora é definida usando o formato ddd.hh:mm:ss, onde:

- ddd representa dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh representa horas com um intervalo de 0-23.
- mm representa minutos com um intervalo de 0-59.
- ss representa segundos com um intervalo de 0-59.

Por padrão, a configuração é de 16 horas (16:00:00), o que indica que a primeira mensagem de aviso aparece aproximadamente 16 horas antes da manutenção.

Final force logoff message box body text

Essa configuração contém o texto editável da mensagem que alerta os usuários que começou um logoff forçado.

Por padrão, a mensagem é: The server is currently going offline for maintenance

Final force logoff message box title

Essa configuração contém o texto editável da barra de título da mensagem final de logoff forçado.

Por padrão, o título é: Notification From IT Staff

Force logoff grace period

Essa configuração define o período entre notificar os usuários a fazer logoff e a implementação do logoff forçado para processar a manutenção pendente.

A hora é definida usando o formato ddd.hh:mm:ss, onde:

- ddd representa dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh representa horas com um intervalo de 0-23.
- mm representa minutos com um intervalo de 0-59.
- ss representa segundos com um intervalo de 0-59.

Por padrão, a configuração de período de tolerância de logoff forçado é de 5 minutos (00:05:00).

Forçar texto do corpo da caixa de mensagem de logoff

Essa configuração contém o texto editável da mensagem que avisa aos usuários para que salvem seus trabalhos e façam logoff antes de começar um logoff forçado.

Por padrão, a mensagem contém o seguinte: {TIMESTAMP} Save your work and log off. The server goes offline for maintenance in {TIMELEFT}.

Force logoff message box title

Essa configuração contém o texto editável da barra de título da mensagem de logoff forçado.

Por padrão, o título é: Notification From IT Staff

Modo gerenciado por imagem

O agente Connector detecta automaticamente se ele está sendo executado em um clone de máquina gerenciado pelos Provisioning Services ou MCS. O agente bloqueia as atualizações do Configuration Manager em clones gerenciados por imagem e instala automaticamente as atualizações na imagem mestre do catálogo.

Depois que uma imagem mestre é atualizada, use o Web Studio para orquestrar a reinicialização dos clones de catálogo MCS. O Connector Agent orquestra automaticamente a reinicialização dos clones de catálogo PVS durante as janelas de manutenção do Configuration Manager. Para substituir esse comportamento para que o software seja instalado em clones de catálogo pelo Configuration Manager, mude o modo gerenciado por imagem para Desativado.

Reboot message box body text

Essa configuração contém o texto editável da mensagem notificando os usuários quando o servidor está prestes a ser reiniciado.

Por padrão, a mensagem é: The server is currently going offline for maintenance.

Intervalo de tempo regular no qual a tarefa do agente deve ser executada

Essa configuração determina com que frequência a tarefa do agente Citrix Connector é executada.

A hora é definida usando o formato ddd.hh:mm:ss, onde:

- ddd representa dias, um parâmetro opcional, com um intervalo de 0 a 999.
- hh representa horas com um intervalo de 0-23.

- mm representa minutos com um intervalo de 0-59.
- ss representa segundos com um intervalo de 0-59.

Por padrão, a configuração de intervalo de tempo regular é de 5 minutos (00:05:00).

Gerenciar

June 28, 2023

O gerenciamento de um site Citrix Virtual Apps and Desktops abrange vários itens e tarefas.

Licenciamento

Uma conexão válida com o Citrix License Server é necessária quando você cria um site. Posteriormente, você pode concluir várias tarefas de licenciamento do Studio, incluindo a adição de licenças, a alteração de tipos ou modelos de licença, e o gerenciamento de administradores de licenças. Você também pode acessar o License Administration Console do Studio.

Aplicativos

Gerencie aplicativos em Grupos de entrega e, opcionalmente, Grupos de aplicativos.

Zonas

Em uma implantação geograficamente dispersa, você pode usar zonas para manter aplicativos e áreas de trabalho mais próximos dos usuários finais, o que pode melhorar o desempenho. Quando você instala e configura um site, todos os Controllers, catálogos de máquinas e conexões de host ficam em uma zona primária. Mais tarde, você pode usar o Studio para criar zonas satélites contendo esses itens. Depois que o seu site tiver mais de uma zona, você poderá indicar em qual zona os catálogos de máquina recém-criados, conexões de host e Controllers adicionados serão colocados. Você também pode mover itens entre zonas.

Conexões e recursos

Se estiver usando um hipervisor ou outro serviço para hospedar máquinas que entregam aplicativos e áreas de trabalho aos usuários, você cria sua primeira conexão com esse hipervisor ou com outro serviço ao criar um site. Os detalhes de armazenamento e rede da conexão formam os seus recursos. Mais tarde, você pode alterar essa conexão e seus recursos e criar mais conexões. Você também pode gerenciar as máquinas que usam uma conexão configurada.

Cache do host local

O cache de host local permite que as operações de troca de conexão em um site continuem quando a conexão entre um Delivery Controller e o banco de dados do site falhar.

IP virtual e loopback virtual

O recurso de endereço IP virtual da Microsoft fornece um aplicativo publicado com um endereço IP atribuído dinamicamente e exclusivo para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem das comunicações com o localhost para usar um endereço de loopback virtual exclusivo no intervalo do localhost.

Delivery Controllers

Este artigo contém considerações e procedimentos ao adicionar e remover Controllers de um site. Ele também descreve como mover Controllers para outra zona ou site e como mover um VDA para outro site.

Registro de VDA em Controllers

Antes que um VDA possa ajudar a entregar aplicativos e áreas de trabalho, ele deve se registrar (estabelecer comunicação) em 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 do site.

Sessões

Manter a atividade da sessão é fundamental para oferecer a melhor experiência de usuário. Vários recursos podem otimizar a confiabilidade das sessões e reduzir transtornos, tempo de inatividade e perda de produtividade.

- Confiabilidade da sessão
- Reconexão automática de cliente
- ICA Keep-Alive
- Controle do espaço de trabalho
- Roaming de sessão

Utilizar a pesquisa no Studio

Para exibir informações sobre computadores, sessões, catálogos de máquinas, aplicativos ou grupos de entrega no Studio, use o recurso de pesquisa flexível.

Marcas

Use marcas para identificar itens como computadores, aplicativos, grupos e políticas. Dessa forma, você pode adaptar certas operações para aplicar a itens com uma marca específica.

IPv4/IPv6

O Citrix Virtual Apps and Desktops oferece suporte a implantações de IPv4 puro, IPv6 puro e pilha dupla que usam redes IPv4 e IPv6 sobrepostas. Este artigo descreve e ilustra essas implantações. Ele também descreve as configurações da política da Citrix que controlam o uso de IPv4 ou IPv6.

Perfis de usuário

Por padrão, o Citrix Profile Management é instalado automaticamente quando você instala um VDA. Se você usa essa solução de perfil, leia este artigo para obter informações gerais. Consulte a documentação do Profile Management para obter detalhes.

Coletar rastreamento Citrix Diagnostic Facility (CDF) na inicialização do sistema

O utilitário CDFControl é um controlador de rastreamento de eventos ou consumidores que captura mensagens de rastreamento Citrix Diagnostic Facility (CDF) exibidas de vários provedores de rastreamento da Citrix. Ele é feito para solucionar problemas complexos relacionados à Citrix, analisar o suporte ao filtro 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 na implantação do Citrix Virtual Apps and Desktops. A Citrix oferece uma análise abrangente e automatizada das coletas de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com as orientações do suporte da Citrix.

Aplicativos

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Se a implantação usa apenas grupos de entrega (e não grupos de aplicativos), você adicionará aplicativos aos grupos de entrega. Se você também tiver grupos de aplicativos, geralmente você adiciona aplicativos aos grupos de aplicativos. Essa orientação possibilita uma administração mais fácil. Um aplicativo deve sempre pertencer a pelo menos um grupo de entrega ou grupo de aplicativos.

No assistente para 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 grupos de um aplicativo (por exemplo, mover um aplicativo de um grupo de aplicativos para um grupo de entrega), a prática recomendada desencoraja a adição dessa complexidade. Mantenha seus aplicativos em um 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 exibir o aplicativo em todos os grupos. Nesses casos, consulte um administrador com mais permissões ou estenda o seu escopo para incluir todos os grupos aos quais o aplicativo foi associado.

Se você publicar dois aplicativos com o mesmo nome (talvez de grupos diferentes) para os mesmos usuários, altere a propriedade `Application name (for user)` no Web Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Você também pode alterar a pasta do aplicativo em que o aplicativo é colocado, quando você adiciona o aplicativo ou mais tarde.

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 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:

- Não é possível adicionar aplicativos a grupos de entrega de acesso ao PC remoto.
- Você não pode usar o assistente para adicionar aplicativos para remover aplicativos de grupos de entrega ou grupos de aplicativos. Essa é uma operação separada.

Para adicionar um ou mais aplicativos:

1. Selecione **Applications** no painel esquerdo e, em seguida, selecione **Add Applications** na barra de ações.
2. O assistente de aplicativos é iniciado em uma página **Introduction**, que você pode remover das futuras inicializações do assistente.
3. O assistente orienta você pelas páginas **Groups**, **Applications** e **Summary** . Quando terminar cada página, clique em **Next** até chegar à página **Summary**.

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 **Delivery Groups** no painel esquerdo do Web Studio, selecione um grupo de entrega no painel central e, em seguida, selecione **Add Applications** na barra de ações. O assistente não exibe a página **Groups** .
- **Para adicionar aplicativos a apenas um grupo de aplicativos:** na etapa 1, selecione **Applications** no painel esquerdo do Web Studio, selecione um grupo de aplicativos no painel central e, em seguida, selecione a entrada **Add Applications** sob o nome do grupo de aplicativos na barra de ações. O assistente não exibe a página **Groups** .

Página Groups

Esta página lista todos os grupos de entrega no site. Se você também criou grupos de aplicativos, a página listará os grupos de aplicativos e os grupos de entrega. Você pode escolher entre qualquer um dos grupos, mas não de ambos os grupos. Em outras palavras, você não pode adicionar aplicativos a um grupo de aplicativos e a um grupo de entrega ao mesmo tempo. Geralmente, se você estiver usando grupos de aplicativos, adicione aplicativos a grupos de aplicativos, em vez de grupos de entrega.

Ao adicionar um aplicativo, marque a caixa de seleção ao lado de pelo menos um grupo de entrega (ou grupo de aplicativos, se disponível). Cada aplicativo deve sempre estar associado a pelo menos um grupo.

Página de aplicativos

Clique em **Add** para exibir as origens do aplicativo.

- **From Start menu:** aplicativos que são detectados em uma máquina nos grupos de entrega selecionados. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se você (1) tiver selecionado grupos de aplicativos sem grupos de entrega associados, (2) grupos de aplicativos selecionados com grupos de entrega associados que não contêm máquinas ou (3) tiver selecionado um grupo de entrega sem máquinas.
- **Manually:** aplicativos localizados em um VDA no grupo de entrega ou em outro lugar na sua rede. Selecionar essa fonte abre uma nova página na qual você especifica um aplicativo a ser adicionado das seguintes formas:

  - Digite o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Browse**, insira as credenciais para acessar o VDA, aguarde até ser conectado ao VDA e selecione um aplicativo no VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.

- **Existing:** aplicativos adicionados anteriormente ao site. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de aplicativos detectados. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Essa origem não pode ser selecionada se o site não tiver aplicativos.

- **App-V:** aplicativos em pacotes App-V. Quando você seleciona essa origem, uma nova página é iniciada na qual 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 clique em **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V.

  Esta origem não pode ser selecionada se o App-V não estiver configurado para o site.

- **Application Group**: Grupos de aplicativos. Quando você seleciona essa origem, uma nova página é iniciada com uma lista de grupos de aplicativos. (Embora a exibição também liste os aplicativos em cada grupo, você pode selecionar somente o grupo, não aplicativos individuais.) Todos os aplicativos atuais e futuros nos grupos selecionados são adicionados. Marque as caixas de seleção dos grupos de aplicativos para adicionar e clique em **OK**.

  Essa 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 fontes na lista **Add** não podem ser selecionadas se não houver uma origem válida desse tipo. Origens incompatíveis (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos) não estão incluídas na lista. Os aplicativos que já foram adicionados aos grupos que você escolheu não podem ser selecionados.

Você pode alterar as propriedades (configurações) de um aplicativo nesta página ou posteriormente.

Por padrão, os aplicativos adicionados são colocados na pasta do aplicativo de nome `Applications`. Você pode alterar o aplicativo nesta página ou posterior. Se você tentar adicionar um aplicativo e já existir outro com o mesmo nome na mesma pasta, você será solicitado a renomear o aplicativo que está adicionando. Você pode aceitar o novo nome oferecido ou recusar e renomear o aplicativo ou selecionar uma pasta diferente. Por exemplo, se `app` já existir na pasta **Applications** e você tentar adicionar outro aplicativo de nome `app` a essa pasta, o novo nome `app_1` será oferecido.

Página Summary

Se você estiver adicionando 10 ou menos aplicativos, seus nomes serão listados em **Applications to add**. Se você estiver adicionando mais de 10 aplicativos, o número total será especificado.

Revise as informações de resumo e clique em **Finish**.

Alterar a associação de grupos de um aplicativo

Depois de adicionar um aplicativo, você pode alterar os grupos de entrega e os grupos de aplicativos aos quais o aplicativo está associado.

Você pode arrastar um aplicativo para um grupo adicional. Essa é uma alternativa ao uso de comandos na barra de ações.

Se um aplicativo estiver associado a mais de uma entrega ou grupo de aplicativos, a prioridade de grupo poderá ser usada para especificar a ordem na qual vários grupos são verificados para localizar aplicativos. Por padrão, todos os grupos são prioridade 0 (a mais alta). Grupos com a mesma prioridade são balanceados de 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 áreas de trabalho somente, se (1) o grupo de entrega contiver máquinas compartilhadas e tiver sido criado com uma versão do XenDesktop 7.x anterior à 7.9 e (2) você tiver permissão de `Edit delivery group`. O tipo de grupo de entrega é convertido automaticamente para `desktops and applications` quando a caixa de diálogo de propriedades é confirmada.

1. Entre no Web Studio, selecione **Applications** no painel esquerdo e selecione o aplicativo.
2. Selecione **Properties** na barra de ações.
3. Selecione a página **Groups** .

    - Para adicionar um grupo, clique em **Add** e selecione **Application Groups** ou **Delivery Groups**. (Se você não criou nenhum grupo de aplicativos, a única entrada será **Delivery Groups**.) Em seguida, selecione um ou mais grupos disponíveis. Grupos 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 **Remove**. Se a remoção da associação de grupo resultar em que o aplicativo não esteja mais associado a nenhum grupo, você será alertado de que o aplicativo será excluído.
    - Para alterar a prioridade de um grupo, selecione o grupo e clique em **Edit Priority**. Selecione um valor de prioridade e clique em **OK**.

4. Quando terminar, clique em **Apply** para aplicar as alterações e manter a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Duplicar, ativar ou desativar, renomear ou excluir um aplicativo

As seguintes ações estão disponíveis:

- **Duplicate:** Talvez você queira duplicar um aplicativo para criar uma versão diferente com parâmetros ou propriedades diferentes. Quando você duplica um aplicativo, ele é renomeado automaticamente com um sufixo exclusivo e colocado ao lado do original. Você também pode querer duplicar um aplicativo e adicioná-lo a um grupo diferente. (Após a duplicação, a maneira mais fácil de mover um aplicativo é arrastá-lo.)
- **Enable or disable:** Ativar e desativar um aplicativo é uma ação diferente da ativação e desativação de um grupo de entrega ou grupo de aplicativos.
- **Rename:** Você pode renomear apenas um aplicativo por vez. Se você tentar renomear um aplicativo e um com o mesmo nome existir na mesma pasta ou grupo, será solicitado que você especifique um nome diferente.
- **Delete:** Excluir um aplicativo o remove dos grupos de entrega e dos grupos de aplicativos aos quais ele foi associado, mas não da origem usada para adicionar o aplicativo originalmente. Excluir um aplicativo é uma ação diferente da remoção de um grupo de entrega ou de um grupo de aplicativos.

Para duplicar, habilitar, desabilitar, renomear ou excluir um aplicativo:

1. Selecione **Applications** no painel esquerdo.
2. Selecione um ou mais aplicativos no painel do meio e, em seguida, selecione a tarefa apropriada na barra de ações.
3. Confirme a ação, quando solicitado.

Remover aplicativos de um grupo de entrega

Um aplicativo deve estar associado (pertencer) a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de entrega que remova a associação desse aplicativo com qualquer grupo de entrega ou grupo de aplicativos, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente a partir de uma origem válida.

1. Selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo de entrega. No painel central inferior, na guia **Applications**, selecione o aplicativo que você deseja remover.
3. Selecione **Remove Application** na barra de ações.
4. Confirme a remoção.

Remover aplicativos de um grupo de aplicativos

Um aplicativo deve pertencer a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de aplicativos que resultará em que esse aplicativo não pertença mais a nenhum grupo, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontecer, se você quiser entregar esse aplicativo, deverá adicioná-lo novamente a partir de uma origem válida.

1. Selecione **Applications** no painel esquerdo.
2. Selecione o grupo de aplicativos no painel do meio e selecione um ou mais aplicativos.
3. Selecione **Remove from Application Group** na barra de ações.
4. Confirme a remoção.

Alterar propriedades do aplicativo

Você pode alterar as propriedades de apenas um aplicativo por vez.

Para alterar as propriedades de um aplicativo:

1. Selecione **Applications** no painel esquerdo.
2. Selecione um aplicativo e, em seguida, selecione **Edit Application Properties** na barra de ações.
3. Selecione a página que contém a propriedade que você deseja alterar.
4. Quando terminar, clique em **Apply** 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	Delivery
Argumentos de linha de comando; consulte Passar parâmetros para aplicativos publicados	Localização
Grupos de entrega e grupos de aplicativos em que o aplicativo está disponível	Groups
Descrição	Identification
Extensões de nome de arquivo e associação de tipo de arquivo: as extensões que o aplicativo abre automaticamente	File Type Association
Ícone	Delivery

Propriedade	Página
Palavras-chaves para StoreFront	Identification
Limites; consulte Configurar limites de aplicativos	Delivery
Nome: Nomes vistos pelo usuário e pelo administrador	Identification
Caminho para executável; consulte Passar parâmetros para aplicativos publicados	Localização
Atalho na área de trabalho do usuário: ativar ou desativar	Delivery
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.	Limit Visibility
Working directory	Localização

As alterações no aplicativo podem não entrar em vigor para os usuários atuais do aplicativo até que eles façam logoff de suas sessões.

Configurar limites de aplicativos

Configure os limites de aplicativos para ajudar a gerenciar o uso do aplicativo. Por exemplo, você pode usar limites de aplicativos para gerenciar o número de usuários que acessam um aplicativo simultaneamente. Da mesma forma, os limites de aplicativos podem ser usados para gerenciar o número de instâncias simultâneas de aplicativos com uso intenso de recursos. Esse limite pode ajudar a manter o desempenho do servidor e evitar a perda de qualidade do serviço.

Esse recurso limita o número de lançamentos de aplicativos que são intermediados pelo Controlador (por exemplo, do aplicativo Citrix Workspace e StoreFront), e não o número de aplicativos em execução que podem ser iniciados por outros métodos. Isso significa que os limites de aplicativos ajudam os administradores ao gerenciar o uso simultâneo, mas não fornecem imposição em todos os cenários. Por exemplo, limites de aplicativos não podem ser aplicados quando o Controlador está no modo de interrupção.

Por padrão, não há limite para quantas instâncias de aplicativos podem ser executadas ao mesmo tempo. Existem várias configurações de limite de aplicativos. Você pode configurar alguns deles ou todos eles.

- 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 executar 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 usando limites de aplicativos:

- **Maximum number of simultaneous instances limit:** Em um grupo de entrega, você configura o número máximo de instâncias simultâneas de aplicativo `Alpha` para 15. Posteriormente, os usuários desse grupo de entrega têm 15 instâncias desse aplicativo em execução ao mesmo tempo. Se algum usuário nesse grupo de entrega agora tentar iniciar `Alpha`, uma mensagem de erro será gerada. O `Alpha` não é iniciado porque excederia o limite de instância de aplicativo simultâneo configurado (15).
- **Limite de aplicativo de uma instância por usuário:** Em outro grupo de entrega, você habilita a opção de uma instância por usuário para aplicativo `Beta`. O usuário Tony inicia o aplicativo `Beta` com sucesso. No final do dia, enquanto esse aplicativo ainda está sendo executado na sessão de Tony, ele tenta executar outra instância do `Beta`. Uma mensagem de erro é gerada e `Beta` não é iniciado porque excederia o limite de uma instância por usuário.
- **Maximum number of simultaneous instances and one-instance-per-user limits:** 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`. Posteriormente, quando 10 usuários desse grupo de entrega tiverem uma instância do `Delta` em execução, qualquer outro usuário nesse grupo de entrega que tentar iniciar o `Delta` receberá uma mensagem de erro. O `Delta` não é iniciado. Se algum dos 10 usuários atuais do `Delta` tentar executar uma segunda instância desse aplicativo, eles receberão uma mensagem de erro e a segunda instância não será iniciada.
- **Maximum number of simultaneous instances per machine, and using tag restrictions:** O aplicativo `Charlie` tem requisitos de licenciamento e desempenho que determinam quantas instâncias podem estar sendo executadas ao mesmo tempo em um servidor específico. Esses requisitos também determinam quantas instâncias podem ser executadas simultaneamente em todos os servidores do site.

  O limite de instâncias por máquina do aplicativo 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 as instâncias do aplicativo por limite de máquina para 2. Portanto, não mais do que seis instâncias de aplicativos `Charlie` têm permissão para executar todo o site. (Esse é um limite de duas instâncias de Charlie em cada um dos três servidores.)

Para restringir o uso de um aplicativo a apenas algumas máquinas dentro de um grupo de entrega (além de limitar as instâncias em todas as máquinas em todo o site):

- Use a funcionalidade de marcação para essas máquinas.
- Configure o número máximo de instâncias por limite de máquina para esse aplicativo.

Se os aplicativos forem executados por métodos diferentes de intermediação de controlador (por exemplo, enquanto um controlador estiver no modo de interrupção) e os limites configurados forem excedidos, os usuários não poderão executar 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 poderão continuar até que seus usuários as fechem.

Se você desativar o roaming da sessão, desative o limite de aplicativo de uma instância por usuário. Se você ativar o limite do aplicativo de uma instância por usuário 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 **Applications** no painel esquerdo e, em seguida, selecione um aplicativo.
2. Selecione **Edit Application Properties** na barra de ações.
3. Na página **Delivery**, escolha uma das seguintes opções.
   - **Allow unlimited use of the application**. Não há limite para o número de instâncias em execução ao mesmo tempo. Esse é o padrão.
   - **Set limits for the application**. Existem dois tipos de limite; especifique um ou ambos.
     - Especifique o número máximo de instâncias que podem ser executadas simultaneamente por máquina
     - Limite a uma instância do aplicativo por usuário
4. Clique em **OK** para aplicar a alteração e fechar a caixa de diálogo, ou **Apply** 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 PowerShell SDK 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 **Location** das propriedades de um aplicativo para inserir a linha de comando e passar parâmetros para aplicativos publicados.

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos `"%*"` (percentual e símbolos de estrela entre aspas duplas) são acrescidos ao final da linha de comando do aplicativo. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos do usuário.

Se um aplicativo publicado não for iniciado quando esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos do usuário são validados quando os símbolos `"%*"` são acrescentados. Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo do usuário, os símbolos `"%**"` são acrescentados à linha de comando para deixar de lado a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como `"C:\Program Files"`), inclua a linha de comando do aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Para fazer isso, adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos `%*`. Tenha o cuidado de incluir um espaço entre as aspas de fechamento para o caminho e a aspas de abertura para os símbolos `%*`.

Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é:

```
"C:\Program Files\Windows Media Player\mplayer1.exe""%*"
```

> **Nota:**
>
> O número máximo de caracteres, incluindo argumentos, na linha de comando para iniciar aplicativos publicados é 203.

Gerenciar pastas de aplicativos

Por padrão, os novos aplicativos adicionados a grupos de entrega são colocados em uma pasta chamada **Applications**. Você pode especificar uma pasta diferente ao criar o grupo de entrega, ao adicionar um aplicativo ou posterior.

É bom saber:

- Você não pode renomear ou excluir a pasta Applications, mas você pode mover todos os aplicativos que ela contém para outras pastas criadas.
- O nome de uma pasta pode conter de 1 a 64 caracteres. É permitido o uso de espaços.
- As pastas podem ser aninhadas em até cinco níveis.
- As pastas não precisam conter aplicativos. São permitidas pastas vazias.

- As pastas são listadas em ordem alfabética no Web Studio, a menos que você as mova ou especifique um local diferente ao criá-las.
- Você pode ter mais de uma pasta com o mesmo nome, desde que cada uma tenha uma pasta pai diferente. Da mesma forma, você pode ter mais de um aplicativo com o mesmo nome, desde que cada um esteja em uma pasta diferente.
- Você deve ter permissão de `View Applications` para ver os aplicativos em pastas e você deve ter permissão de `Edit Application Properties` para todos os aplicativos na pasta para remover, renomear ou excluir uma pasta que contenha aplicativos.
- A maioria dos procedimentos a seguir solicita ações usando as barra de ações no Web Studio. Como alternativa, você pode usar menus com o botão direito do mouse ou arrastar o item. Por exemplo, se você criar ou mover uma pasta em um local que não pretendia, poderá arrastar/soltá-la no local correto.

Para gerenciar pastas de aplicativos, selecione **Applications** no painel esquerdo. Use a lista a seguir para obter orientação.

- **Para exibir todas as pastas (excluindo pastas aninhadas):** Clique em **Show all** acima da lista de pastas.
- **Para criar uma pasta no nível mais alto (não aninhada):** Selecione a pasta **Applications** . Para colocar a nova pasta em uma pasta existente diferente de **Applications**, selecione essa pasta. Em seguida, selecione **Create Folder** na barra de ações. Digite um nome.
- **Para mover uma pasta:** selecione a pasta e, em seguida, selecione **Move Folder** na barra de ações. Você pode mover apenas uma pasta por vez, a menos que a pasta contenha pastas aninhadas. (A maneira mais fácil de mover uma pasta é arrastá-la.)
- **Para renomear uma pasta:** selecione a pasta e selecione **Rename Folder** na barra de ações. Digite um nome.
- **Para excluir uma pasta:** selecione a pasta e, em seguida, selecione **Delete Folder** na barra de ações. Quando você exclui 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. O Tt não o remove da máquina.
- **Para mover aplicativos para uma pasta:** Selecione um ou mais aplicativos. Em seguida, selecione **Move Application** na barra de ações. Selecione a pasta.

Você também pode colocar aplicativos que você está adicionando em uma pasta na página **Application** ao criar um grupo de entrega ou um grupo de aplicativos. Por padrão, aplicativos adicionados vão para a pasta **Applications** . Clique em **Change** para selecionar ou criar uma pasta.

Controle o início local de aplicativos em áreas de trabalho publicadas

Quando os usuários iniciam um aplicativo publicado de dentro de uma área de trabalho publicada, você pode controlar se o aplicativo é iniciado nessa sessão de área de trabalho 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 será iniciada. Se você iniciar um aplicativo que não esteja instalado no VDA, o aplicativo hospedado será iniciado. Para obter mais informações, consulte vPrefer launch.

No PowerShell (usando o SDK do PowerShell remoto em implantações do Citrix Cloud ou o PowerShell SDK em implantações locais), você pode alterar essa ação.

No aplicativo `New-Broker` ou cmdlet `Set-BrokerApplication`, use a opção `LocalLaunchDisabled`. Por exemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Por padrão, o valor dessa opção é false (`-LocalLaunchDisabled $false`). Ao iniciar um aplicativo publicado de dentro de uma área de trabalho publicada, o aplicativo é iniciado nessa sessão da área de trabalho.

Se você definir o valor da opção como true (`-LocalLaunchDisabled $true`), o aplicativo publicado será iniciado. Isso cria uma sessão separada e adicional da área de trabalho publicada (usando o aplicativo Citrix Workspace para Windows) para o aplicativo publicado.

Requisitos e limites:

- O valor do aplicativo `ApplicationType` deve ser `HostedOnDesktop`.
- Essa opção está disponível somente por meio do SDK do PowerShell apropriado. No momento, ela não está disponível na interface gráfica do Web Studio.
- Essa opção requer o mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 e Delivery Controller 7.17.

Pacotes de aplicativos

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

A Microsoft fornece três tecnologias de empacotamento para entregar aplicativos aos usuários: App-V, MSIX e anexação de aplicativo MSIX. Este artigo explica como implantar e entregar esses pacotes de aplicativos usando **Web Studio > App Packages**:

- Implementar e entregar aplicativos App-V
- Implementar e entregar aplicativos MSIX e de anexação de aplicativo MSIX

Implementar e entregar aplicativos App-V

Esta seção aborda as seguintes informações:

- Visão geral. Descreve os métodos de gerenciamento para entregar e gerenciar os pacotes do App-V.
- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

Esta seção descreve os métodos de gerenciamento para entregar e gerenciar os pacotes do App-V. Para obter mais informações sobre os componentes e conceitos com os quais você interage ao entregar aplicativos empacotados do App-V, consulte a documentação da Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Você pode usar os seguintes métodos para entregar e gerenciar pacotes do App-V:

- **Administração dupla**. Os pacotes de aplicativos são configurados e gerenciados em servidores App-V. Os servidores Citrix Virtual Apps and Desktops e App-V trabalham em conjunto para entregar e gerenciar pacotes.

  Esse método exige que o Citrix Virtual Apps and Desktops atualize periodicamente a exibição do instantâneo do estado do servidor App-V. Isso resulta na sobrecarga de hardware, infraestrutura e administração. Os servidores Citrix Virtual Apps and Desktops e App-V devem permanecer sincronizados, especialmente as permissões de usuário.

  A Administração dupla funciona melhor nas implantações em que o App-V e o seu ambiente estão estreitamente ligados:

  - **Servidor de gerenciamento App-V**. Publica e gerencia o ciclo de vida dos pacotes App-V e os arquivos de configuração dinâmica.
  - **Componente Citrix Personalization** instalado em máquinas VDA. Gerencie o registro do servidor de publicação App-V apropriado necessário para inicializações de aplicativos.

  Esse método garante que o servidor de publicação App-V seja sincronizado para o usuário no momento apropriado. O servidor de publicação mantém outros aspectos do ciclo de vida do pacote, como atualizar no login e grupos de conexão.

- **Administração simples**. Os pacotes de aplicativos são armazenados em compartilhamentos de rede. O Citrix Virtual Apps and Desktops entrega e gerencia pacotes de forma independente.

Esse método reduz a sobrecarga porque os servidores App-V e a infraestrutura de banco de dados não são necessários na implantação.

Nesse método, você armazena os pacotes App-V em um compartilhamento de rede e carrega seus metadados desse local para o seu ambiente. O componente Citrix Personalization instalado nas máquinas VDA gerencia e entrega os aplicativos da seguinte forma:

- Processam os arquivos de configuração de implantação e os arquivos de configuração do usuário quando um aplicativo for iniciado.
- Gerenciam todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Você pode usar os dois métodos de gerenciamento simultaneamente. Em outras palavras, quando você adiciona aplicativos aos grupos de entrega, os aplicativos podem vir de pacotes App-V presentes em servidores App-V ou em compartilhamentos de rede.

> **Nota:**
>
> Se você estiver usando os dois métodos de gerenciamento simultaneamente, e o pacote App-V tiver um arquivo de configuração dinâmica nos dois locais, o arquivo no servidor App-V (administração dupla) será usado.

Procedimentos

Para dar suporte à entrega dos aplicativos App-V, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization em máquinas VDA para obter detalhes.

Para fornecer aplicativos empacotados do App-V para seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Faça upload de pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.
4. Para habilitar a entrega automática de pacotes App-V interdependentes, crie grupos de isolamento.

Para que o Citrix Virtual Apps and Desktops reconheça e aplique os arquivos de configuração dinâmica do App-V no método de Administração simples, consulte este blog da Citrix.

Implementar e entregar aplicativos MSIX e de anexação de aplicativo MSIX

Esta seção aborda as seguintes informações:

- Visão geral. Descreve como os pacotes de anexação de aplicativo MSIX e MSIX são entregues e gerenciados.

- Procedimentos. Fornece procedimentos para implantar e entregar esses pacotes.

Visão geral

O Citrix Virtual Apps and Desktops entrega aplicativos MSIX e de anexação de aplicativo MSIX aos usuários por meio do componente Citrix Personalization instalado em máquinas VDA. Este componente gerencia todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Para obter mais informações sobre MSIX e anexação de aplicativo MSIX, consulte a documentação da Microsoft: https://docs.microsoft.com/en-us/windows/msix/ e https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach, respectivamente.

Procedimentos

Para dar suporte à entrega dos pacotes MSIX e de conexão de aplicativo MSIX, você deve instalar o componente Citrix Personalization nas máquinas VDA. Consulte Instalar o componente Citrix Personalization em máquinas VDA para obter detalhes.

Para entregar aplicativos empacotados MSIX e de anexação de aplicativo MSIX aos seus usuários, siga estas etapas:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Faça upload de pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.

Instalar o componente Citrix Personalization em máquinas VDA

O componente Citrix Personalization gerencia o processo de publicação de pacotes de aplicativos nos formatos App-V, MSIX e de anexação de aplicativo MSIX. Este componente não é instalado por padrão quando você instala um VDA. Você pode instalar o componente durante ou após a instalação do VDA.

Para instalar o componente durante a instalação do VDA, use uma das seguintes formas:

- No assistente de instalação, vá para a página **Additional Components** e marque a caixa de seleção **Citrix Personalization for App-V - VDA**.
- Na interface da linha de comando, use a opção **/includeadditional "Citrix Personalization for App-V –VDA"**.

Para instalar o componente após a instalação do VDA, siga estas etapas:

1. Na máquina VDA, vá para **Painel de controle > Programas > Programas e recursos**, clique com o botão direito do mouse em **Citrix Virtual Delivery Agent** e selecione **Alterar**.

2. No assistente exibido, vá para a página **Additional Components** e marque a caixa de seleção **Citrix Personalization for App-V - VDA**.

> **Nota:**
>
> O cliente Desktop Microsoft App-V é o componente que executa os aplicativos virtuais dos pacotes App-V nos dispositivos do usuário. O Windows 10 (1607 ou posterior), o Windows Server 2016 e o Windows Server 2019 já incluem esse software cliente App-V. Você só precisa habilitá-lo nas máquinas VDA. Para obter mais informações, consulte este artigo da documentação da Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

Armazenar pacotes de aplicativos em compartilhamentos de rede

Depois de configurar a infraestrutura, gere os pacotes de aplicativos e armazene-os em um local de rede, como um compartilhamento de rede UNC ou SMB, ou em um compartilhamento de arquivos do Azure.

As etapas detalhadas são as seguintes:

1. Gere pacotes de aplicativos. Consulte a documentação da Microsoft para obter detalhes.
2. Armazene pacotes de aplicativos em um local de rede:
   - Para **administração simples de App-V**: armazene os pacotes e os Arquivos de Configuração Dinâmica (App-V) correspondentes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
   - Para **administração dupla de App-V**: publique os pacotes no servidor de gerenciamento App-V a partir de um caminho UNC. (A publicação a partir de URLs HTTP não é suportada.)
   - Para **MSIX ou anexação de aplicativo MSIX**: armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um compartilhamento de arquivos do Azure.
3. Certifique-se de que o VDA tenha permissão de leitura no caminho de armazenamento do pacote:
   - Se você armazenar pacotes em um compartilhamento de rede UNC ou SMB no domínio do AD, conceda à máquina VDA permissão de leitura ao caminho de armazenamento. Para isso, você pode conceder a permissão de leitura da conta do AD da máquina para o compartilhamento explicitamente ou incluir a conta em um grupo do AD que tenha essa permissão.
   - Se você armazenar pacotes em um Compartilhamento de Arquivos do Azure, primeiro conceda uma permissão de leitura de conta de usuário para o caminho de armazenamento no

Azure. Em seguida, configure o `ctxAppVService` em execução na máquina VDA para usar essa conta de usuário para acessar o caminho de armazenamento do pacote. Consulte a seção a seguir para ver as etapas detalhadas.

Alterar a conta de logon do usuário

O VDA chama `ctxAppVService` para acessar os caminhos de armazenamento do pacote. Por padrão, `ctxAppVService` acessa os caminhos de armazenamento de pacotes usando a **conta do Sistema Local** da máquina. Esse tipo de autenticação de máquina funciona em domínios do AD. No entanto, não funciona nos cenários de integração do AD e do Azure AD, que exigem autenticação baseada em conta de usuário.

Se você armazenar pacotes em um Compartilhamento de Arquivos do Azure, altere a conta de logon de `ctxAppVService` para uma conta de usuário que tenha permissão de leitura no caminho de armazenamento do pacote. As etapas detalhadas são as seguintes:

1. Inicie o **Services**, clique com o botão direito do mouse em **ctxAppVService** e selecione **Properties**.
2. Na guia **Log on**, selecione **This account**, insira uma conta de usuário que tenha permissão de leitura para o caminho de armazenamento do pacote e, em seguida, digite a senha do usuário duas vezes.
3. Clique em **OK**.

Upload de pacotes de aplicativos para o seu ambiente

Depois de armazenar os pacotes de aplicativos em um local de rede conforme necessário, carregue-os no seu ambiente para entrega. Use um dos seguintes métodos, conforme necessário:

- Carregar em massa
- Carregar um por um

Preparação

O Citrix Virtual Apps and Desktops usa uma máquina VDA para configurar a conexão com o local de rede para a descoberta de pacotes. Portanto, crie um grupo de entrega previamente e certifique-se de que pelo menos um VDA no grupo atenda aos seguintes requisitos:

- Versão VDA:
  - Para descobrir pacotes do App-V: 2203 ou posterior
  - Para descobrir os pacotes MSIX e de anexação de aplicativo MSIX: 2209 ou posterior

- Componente do Citrix Personalization for App-V: instalado
- Permissão ao local do pacote: Leitura (veja a Etapa 2: Armazenar pacotes de aplicativos em compartilhamentos de rede para obter detalhes.)
- Alimentação: ligado
- Estado: registrado

Carregar pacotes de aplicativos em massa

Faça upload de pacotes em um local de rede para o seu ambiente. Certifique-se de ter os seguintes itens prontos antes do carregamento:

- Um grupo de entrega que atenda aos requisitos de Preparação
- O caminho da localização da rede

Para carregar pacotes em massa, siga estas etapas:

1. No painel esquerdo, selecione **App Packages**.
2. Na guia **Sources**, clique no botão **Add Source**. A página **Add Source** é exibida.
3. No campo **Name**, insira um nome descritivo para a origem do pacote.
4. No campo **Delivery group**, clique em **Select a delivery group**. Em seguida, selecione um grupo de entrega que atenda aos requisitos descritos na Preparação e clique em **OK**.
5. No campo **Location type**, selecione **Microsoft App-V server** ou **Network share** com base em onde você armazena os pacotes e, em seguida, preencha as configurações correspondentes:
    - Se você selecionar o **Microsoft App-V server**, insira as seguintes informações:
        - URL do servidor de gerenciamento. Exemplo: `http://appv-server.example.com`
        - Credenciais de login do administrador do servidor de gerenciamento.
        - URL e número da porta do servidor de publicação. Exemplo: `http://appv-server.example.com:3330`
    - Se você selecionou **Network share**, especifique as seguintes informações:
        - Insira o caminho UNC do compartilhamento de rede. Exemplo: `\\Package-Server\apps\`
        - Selecione os tipos de pacotes que deseja carregar. As opções incluem App-V, MSIX e anexação de aplicativo MSIX.
        - Especifique se deseja pesquisar pacotes nas subpastas.
6. Clique em **Add Source**.

    A página Add Source é fechada e a origem recém-adicionada aparece na lista de origens. O Citrix Virtual Apps and Desktops carrega os pacotes para o seu ambiente usando um VDA no grupo

de entrega. Após a conclusão do carregamento, o campo Status mostra *Import successful*. Os pacotes correspondentes aparecem na guia **Packages**.

> **Nota:**
>
> Para verificar se há atualizações de pacotes em um local de origem e importá-las para o seu ambiente, selecione o local na lista de origem e clique em **Check for Package Updates**.

Carregar pacotes de aplicativos um por um

Carregue um pacote de aplicativos de um compartilhamento de rede para o seu ambiente. Antes do carregamento, verifique se você tem os seguintes itens prontos:

- Um grupo de entrega que atenda aos requisitos descritos em Preparação
- O caminho do local da rede.

Para carregar um pacote para o seu ambiente, siga estas etapas:

1. No painel esquerdo, selecione **App Packages**.
2. Na guia **Packages**, clique no botão **Add Package**. A página **Add Package** é exibida.
3. No campo **Delivery group**, clique em **Select a delivery group**. Em seguida, selecione um grupo de entrega que atenda aos requisitos descritos na Preparação e clique em **OK**.
4. No campo **Package full path**, insira um caminho conforme necessário:
   - Para fazer upload de vários pacotes ao mesmo tempo, insira seus caminhos completos, separados por ponto e vírgula (`;`). Exemplo: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Para carregar todos os pacotes presentes em um compartilhamento de rede, insira o caminho de armazenamento. Exemplo: \package-Server\apps\
5. Clique em **Add Package**.

   O pacote do aplicativo aparece na guia **Packages**.

Adicionar aplicativos a grupos de entrega

Depois que um pacote de aplicativos for totalmente carregado, adicione seus aplicativos a um ou mais grupos de entrega, conforme necessário. Como resultado, os usuários associados a esses grupos de entrega podem acessar os aplicativos.

Para adicionar um ou mais aplicativos em um pacote a vários grupos de entrega, siga estas etapas:

1. No painel esquerdo, selecione **App Packages**.
2. Na guia **Packages**, selecione um pacote conforme necessário.
3. Na barra de ações clique em **Add Delivery Groups**. A página Add Delivery Groups é exibida.
4. Selecione um ou mais aplicativos no pacote, conforme necessário, e clique em **Next**. Os grupos de entrega com o tipo de entrega de *Applications* são exibidos.
5. Na lista de grupos de entrega, selecione os grupos aos quais você deseja atribuir os aplicativos e clique em **Next**.
   Nota: Se você selecionou um pacote MSIX ou de anexação de aplicativo MSIX, somente grupos de entrega cujo nível funcional seja 2106 ou posterior serão mostrados na lista.
6. Clique em **Finish**.

Você também pode adicionar aplicativos empacotados a um grupo de entrega quando:

- Criar um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.
- Editar grupos de entrega ou grupos de aplicativos existentes. Para obter mais informações, consulte Add applications.

(Opcional) Criar grupos de isolamento para pacotes App-V

Você pode criar grupos de isolamento para permitir a entrega automática de pacotes App-V interdependentes.

> **Nota:**
>
> Grupos de isolamento são compatíveis com o método de administração simples de App-V. Se estiver usando o método de administração dupla App-V, você pode atingir o mesmo objetivo criando *grupos de conexão* na infraestrutura do Microsoft App-V. Para obter mais informações, consulte este artigo da documentação da Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

Sobre grupos de isolamento

Um grupo de isolamento é uma coleção de pacotes de aplicativos interdependentes que devem ser executados na mesma Windows Sandbox para criar um ambiente virtual. Os grupos de isolamento do Citrix App-V são semelhantes, mas não são idênticos aos grupos de conexão App-V. Um grupo de isolamento inclui dois tipos de pacotes:

- Pacotes de aplicativos **explícitos**. Aplicativos com requisitos específicos de licenciamento. Você pode restringir esses aplicativos a um intervalo específico de usuários adicionando-os a grupos de entrega.
- Pacotes de aplicativos **automáticos**. Aplicativos que estão sempre disponíveis para todos os usuários, independentemente de serem ou não adicionados aos grupos de entrega.

Por exemplo, o aplicativo app-a requer JRE 1.7 para ser executado. Você pode criar um grupo de isolamento que contenha app-a (marcado como *Explícito*) e JRE 1.7 (marcado como *Automático*). Em seguida, adicionar o pacote App-V de app-a a um ou mais grupos de entrega. Quando um usuário inicia o app-a, o JRE 1.7 é implantado automaticamente com ele.

Quando um usuário inicia um aplicativo App-V marcado como *Explícito* em um grupo de isolamento, o Citrix Virtual Apps and Desktops verifica a permissão de acesso do usuário ao aplicativo em grupos de entrega. Se o usuário tiver permissão para acessar o aplicativo, todos os pacotes de aplicativos *automáticos* no mesmo grupo de isolamento são disponibilizados para o usuário.

Você não precisa adicionar os pacotes *automáticos* a nenhum grupo de entrega. Se houver outro pacote de aplicativo *explícito* no grupo de isolamento, esse pacote será disponibilizado para o usuário somente se estiver no mesmo grupo de entrega.

Para obter mais informações sobre grupos isolados, consulte este blog da Citrix.

Criar um grupo de isolamento App-V Crie um grupo de isolamento e adicione pacotes de aplicativos interdependentes a ele. As etapas detalhadas são as seguintes:

1. Na guia **Isolation Groups**, clique em **Add Isolation Group**.
2. Insira um nome e uma descrição para o grupo de isolamento. Todos os pacotes de aplicativos no seu ambiente aparecem na lista **Available Packages**.
3. Na lista **Available Packages**, selecione um aplicativo, conforme necessário, e clique na seta para a direita. O aplicativo selecionado aparece na lista **Packages in Isolation Group**.
4. No campo **Deployment**, selecione **Explicit** ou **Automatic** para o aplicativo.
5. Repita as etapas 2—3 para adicionar mais pacotes.
6. Para ajustar a ordem dos pacotes na lista, clique na seta para cima ou para baixo.
7. Clique em **Salvar**.

> **Nota:**
>
> As configurações do grupo de isolamento resultam na criação de grupos de conexão App-V no VDA. Os cenários de implantação podem se tornar complexos e o cliente App-V suporta pacotes que estão apenas em um grupo de conexão ativo por vez. Recomendamos que você evite adicionar o mesmo pacote a dois grupos de isolamento diferentes que estão adicionados ao mesmo grupo de entrega.

Aplicativos da Plataforma Universal do Windows

June 28, 2023

Para obter informações sobre aplicativos da Plataforma Universal do Windows (UWP), consulte a seguinte documentação da Microsoft:

- O que é um aplicativo Universal Windows Platform (UWP, Plataforma Universal do Windows)?
- Gerenciador de Pacotes do Windows

Requisitos e limitações

O Citrix Virtual Apps and Desktops suporta o uso de aplicativos UWP com VDAs nas seguintes máquinas Windows:

- Windows 10 e versões posteriores
- Windows Server 2016 e versões posteriores

Os VDAs devem ter a versão mínima 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 sobrepõem, a visualização mostrará o ícone padrão. As APIs Win32 usadas para a visualização dinâmica não são suportadas em aplicativos UWP.
- Uso remoto do Centro de Ação: os aplicativos UWP podem usar o Centro de Ação para exibir as mensagens na sessão. No momento, essas mensagens não são redirecionadas para o ponto de extremidade para serem exibidas ao usuário.

Não há suporte para iniciar aplicativos UWP e aplicativos não UWP do mesmo servidor. Em vez disso, coloque aplicativos UWP e aplicativos não UWP em grupos de entrega ou grupos de aplicativos separados.

Como todos os aplicativos UWP instalados na máquina são enumerados, a Citrix recomenda desativar o acesso do usuário à Windows Store. Isso impede que os aplicativos UWP instalados por um usuário sejam acessados por outro usuário.

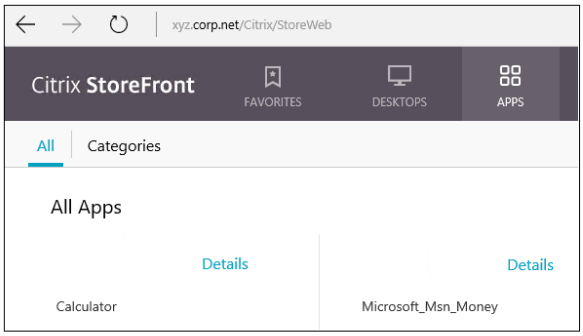
Durante o sideload, o aplicativo UWP é instalado na máquina e está disponível para uso por outros usuários. Quando outro usuário inicia o aplicativo, ele é instalado e o sistema operacional atualiza o seu banco de dados AppX para indicar "como instalado"por esse usuário.

Um logoff normal iniciado a partir de um aplicativo UWP publicado que foi iniciado em uma janela fixa ou contínua pode impedir que a sessão do VDA seja fechada e desconecte o usuário à força. Quando isso ocorre, vários processos restantes na sessão do VDA impedem que ela seja fechada corretamente. Para resolver isso, descubra qual processo está impedindo a sessão do VDA de fechar e adicione-o ao valor da chave de registro "LogoffCheckSysModules"seguindo as orientações em CTX891671.

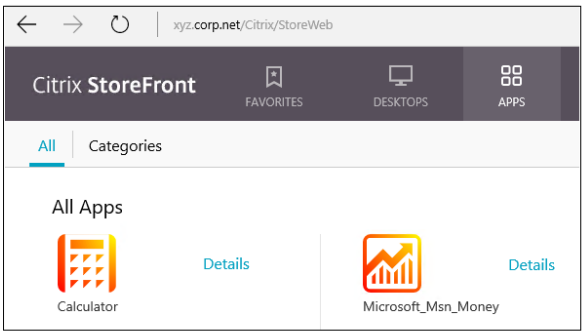
Os nomes de exibição e descrições de aplicativos UWP podem não ter nomes corretos. Edite e corrija essas propriedades ao adicionar os aplicativos ao grupo de entrega.

Marque Problemas conhecidos para quaisquer problemas adicionais.

Atualmente, vários aplicativos UWP têm ícones brancos com transparência ativada, o que resulta em um ícone invisível contra o fundo branco da tela 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 depois deste exemplo.



Before



After

No Windows Server 2016 e versões posteriores, o Gerenciador de Servidores também pode ser iniciado quando um aplicativo UWP é iniciado. Para evitar que isso ocorra, você pode desativar o Gerenciador de Servidores de inicialização automática 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 está habilitado por padrão.

Para instalar um ou mais aplicativos UWP em VDAs (ou uma imagem mestre), use um dos seguintes métodos:

- Conclua uma instalação off-line da Windows Store for Business, usando uma ferramenta como o DISM (Deployment Image Servicing and Management) para implantar os aplicativos na imagem da área de trabalho. Para obter mais informações, consulte Gerenciador de Pacotes do Windows.
- Faça sideload os aplicativos. Para obter mais informações, consulte Sideload line of business (LOB) apps in Windows client devices.

- Instale os aplicativos UWP para cada usuário pretendido diretamente do Windows Store para Empresas.

Para adicionar (publicar) um ou mais aplicativos UWP no Citrix Virtual Apps ou Citrix Virtual Desktops:

1. Depois que os aplicativos UWP estiverem 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 **Applications**, no menu **Add**, selecione **From Start menu**.
2. Quando a lista de aplicativos for exibida, selecione os aplicativos UWP que você deseja publicar.
3. Continue com o assistente ou feche a caixa de diálogo de edição.

Para desativar o uso de Aplicativos Universais em um VDA, adicione a configuração do Registro **EnableUWASeamlessSupport** em `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` e defina como **0**.

Desinstalar aplicativos UWP

Quando você desinstala um aplicativo UWP com um comando como `Remove-AppXPackage`, o item é desinstalado somente dos 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 comando.

Citrix Insight Services

June 28, 2023

O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios. Seus recursos de instrumentação e telemetria permitem que usuários técnicos (clientes, parceiros e técnicos) autodiagnostiquem e corrijam problemas e otimizem seus ambientes. Para obter detalhes e as informações mais recentes sobre o CIS e como ele funciona, consulte https://cis.citrix.com (são necessárias credenciais de conta Citrix).

Todas as informações enviadas para a Citrix são usadas para fins de solução de problemas e diagnóstico, além de melhorar a qualidade, a confiabilidade e o desempenho dos produtos, sujeito a:

- Política de Citrix Insight Services em https://cis.citrix.com/legal
- Política de privacidade da Citrix em https://www.citrix.com/about/legal/privacy.html

Esta versão do Citrix Virtual Apps and Desktops oferece suporte às seguintes tecnologias:

- Análise de instalação e atualização do Citrix Virtual Apps and Desktops
- Citrix Customer Experience Improvement Program (CEIP)
- Citrix Call Home
- Citrix Scout

Além do (e separado do) CIS e do Citrix Analytics: os dados do Google Analytics são coletados (e depois carregados) automaticamente quando você instala (ou atualiza) o Studio. Depois de instalar o Studio, você pode alterar essa configuração com a chave de registro HKLM\Software\Citrix\DesktopStudio\GAEnabled. O valor 1 ativa a coleta e o carregamento, 0 desativa a coleta e o carregamento.

Análise de instalação e atualização

Quando você usa o instalador do produto completo para implantar ou atualizar os componentes do Citrix Virtual Apps and Desktops, informações anônimas sobre o processo de instalação são coletadas e armazenadas na máquina em que 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 do Registro antes de instalar/atualizar, esse valor será usado quando você usar o instalador do produto completo.
- Você pode substituir a configuração padrão se instalar/atualizar com a interface de linha de comando especificando uma opção com o comando.

Controle os uploads automáticos:

- Configuração do registro que controla o upload automático da análise de instalação/atualização (padrão = 1):
  - Localização: HKLM:\Software\Citrix\MetaInstall
  - Nome: SendExperienceMetrics
  - Valor: 0 = desativado, 1 = ativado
- Usando o PowerShell, o seguinte cmdlet desabilita o upload automático da análise de instalação/atualização:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
```



```
<!--NeedCopy-->
```

- 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`.

Citrix Customer Experience Improvement Program

Quando você participa do Citrix Customer Experience Improvement Program (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 **Settings** no painel esquerdo do Web Studio (na guia **Product Support**) e desative a configuração **Citrix Customer Experience Improvement Program**.

Quando você atualiza uma implantação do Citrix Virtual Apps and Desktops:

- Se você atualizar de uma versão que não dava suporte a CEIP, você será consultado se deseja participar.
- Se você atualizar de uma versão que dava suporte ao CEIP e a participação estiver ativada, o CEIP será ativado no Site atualizado.
- Se você atualizar de uma versão que dava suporte ao CEIP e a participação estiver desativada, o CEIP será desativado no Site atualizado.
- Se você atualizar de uma versão que dava suporte ao CEIP e a participação for desconhecida, você será consultado se deseja participar.

As informações coletadas são anônimas, portanto, não podem ser visualizadas após serem carregadas para o Citrix Insight Services.

Inscrição ao instalar um VDA

Por padrão, você é automaticamente inscrito no CEIP quando instala um VDA do Windows. Você pode alterar esse padrão em uma configuração do registro. Se você alterar a configuração do Registro antes de instalar o VDA, esse valor será usado.

Configuração do Registro que controla o registro automático no CEIP (padrão = 1):

Localização: HKLM: \Software\Citrix\Telemetry\CEIP
Name: Enabled
Valor: 0 = desativado, 1 = ativado

Por padrão, a propriedade `Enabled` está oculta no registro. Quando ele permanece não especificado, o recurso de upload automático é ativado.

Usando o PowerShell, o seguinte cmdlet desabilita o registro no CEIP:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

Os datapoints 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 correlatos, como Citrix Provisioning, AppDNA, Citrix License Server, Citrix Workspace app para Windows, Universal Print Server e Session Recording. Consulte a documentação para obter detalhes sobre os valores padrão de instalação e participação.

Citrix Call Home

Quando você instala 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 que contêm 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 com o nome Citrix Telemetry Service. Para obter mais informações, consulte https://more.citrix.com/XD-CALLHOME.

A funcionalidade de agendamento do Call Home também está disponível no Citrix Scout. Para obter detalhes, consulte Citrix Scout.

O que é coletado

O rastreamento do Citrix Diagnostic Facility (CDF) registra informações que podem ser úteis para solução de problemas. O Call Home coleta um subconjunto de rastreamentos de CDF que pode ser

útil ao solucionar problemas de falhas comuns, por exemplo, registros VDA e lançamentos de aplicativo/desktop. Essa tecnologia é conhecida como rastreio sempre ativo (AOT). Os registros AOT são salvos no 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 isso.

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) em Citrix namespace.
- Lista de processos em execução.
- Despejos de memória de processos Citrix que são armazenados em %PROGRAM DATA%\Citrix\CDF.
- Informações de instalação e atualização. Isso pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront, registros de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

As informações de rastreamento são compactadas à medida que são coletadas. O Citrix Telemetry Service retém um máximo de 10 MB de informações de rastreamento recentes compactadas, com um limite de tempo máximo de oito dias.

- A compactação de dados permite que o Call Home ocupe pouco espaço no VDA.
- Os rastreamentos são mantidos na memória para evitar IOPs em máquinas provisionadas.
- O buffer de rastreamento usa um mecanismo circular para reter rastreamentos na memória.

O Call Home coleta os principais datapoints listados em Principais pontos de dados do Call Home.

Configurar e gerenciar o resumo

Você pode se inscrever no Call Home ao usar o assistente de instalação do produto completo ou posteriormente, usando cmdlets do PowerShell. Quando você se inscreve, por padrão, os diagnósticos são coletados e enviados para a Citrix todos os domingos aproximadamente às 3:00 da manhã, horário local. O upload é randomizado com um intervalo de duas horas a partir do horário especificado. Isso significa que um upload usando o cronograma padrão ocorre entre 3:00 e 5:00 da manhã.

Se você não quiser fazer upload de informações de diagnóstico agendadas (ou se quiser alterar um cronograma), poderá usar cmdlets do PowerShell para coletar e carregar diagnósticos manualmente ou armazená-los localmente.

Quando você se inscreve 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 usado para identificar o cliente e fazer upload dos dados. As credenciais não são salvas.

Quando ocorre um upload, é enviada uma notificação por e-mail para o endereço associado à conta Citrix.

Se você ativar o Call Home ao instalar um componente, poderá desativá-lo posteriormente.

Pré-requisitos

- A máquina deve estar executando o PowerShell 3.0 ou posterior.
- O Citrix Telemetry Service deve estar em execução na máquina.
- A variável do sistema `PSModulePath` deve ser definida como caminho de instalação da Telemetria, por exemplo, C:\Program Files\Citrix\Telemetry Service\.

Ativar o Call Home durante a instalação

Durante a instalação ou atualização do VDA: Quando você instala ou atualiza um Virtual Delivery Agent usando a interface gráfica no instalador completo do produto, você é consultado 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 estiver inscrito anteriormente no Call Home, essa página do assistente não será exibida.

Durante a instalação ou atualização do Controller: Quando você instala ou atualiza um Delivery Controller usando a interface gráfica, você é perguntado se deseja participar do Call Home. Existem três opções:

Quando você estiver instalando um Controlador, não será possível configurar informações na página Call Home no assistente de instalação se esse servidor tiver um GPO do Active Directory com a configuração de política "Log on as a service"aplicada. Para obter detalhes, consulte CTX218094.

Se você estiver atualizando um Controller e já estiver inscrito no Call Home, não será consultado quanto à participação.

Cmdlets PowerShell

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Para usar um servidor proxy para uploads, consulte Configurar um servidor proxy.

- **Ativar uploads agendados:** As coletas de diagnóstico são carregadas automaticamente para a Citrix. Se você não inserir cmdlets adicionais para um agendamento personalizado, será usado o agendamento padrão.

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
<!--NeedCopy-->
```

  Para confirmar se os uploads agendados estão ativados, digite `Get-CitrixCallHomeGet-CitrixCallHome`. Se ativados, são fornecidos os valores `IsEnabled=True` e `IsMasterImage=False`.

- **Ativar uploads agendados para máquinas criadas a partir de uma imagem mestre:** Ativar 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 ativados, digite **Get-CitrixCallHome**. Se estiver ativado, são fornecidos os valores `IsEnabled=True` e `IsMasterImage=True`.

- **Criar uma programação personalizada:** Crie uma programação diária ou semanal para coleções de diagnóstico e uploads.

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
   -UploadFrequency {
Daily|Weekly }

<!--NeedCopy-->
```

Exemplos:

O cmdlet a seguir cria um agendamento para agrupar e fazer upload de dados às 22:20 todas as noites. O parâmetro Hours usa um relógio de 24 horas. Quando o valor do parâmetro `UploadFrequency` é Daily, o parâmetro `DayOfWeek` é ignorado, se estiver especificado.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
<!--NeedCopy-->
```

Para confirmar a programação, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, o valor fornecido é `StartTime=22:20:00, DayOfWeek=Sunday (ignored), UploadFrequency=Daily`.

O cmdlet a seguir cria uma programação para agrupar e carregar dados às 20:20 todas as quartas-feiras.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
```



```
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek Wed -
    UploadFrequency Weekly
<!--NeedCopy-->
```

Para confirmar a programação, digite `Get-CitrixCallHomeSchedule`. No exemplo anterior, o valor fornecido é `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency =Weekly`.

Desativar o Call Home

Você pode desativar o Call Home usando um cmdlet do PowerShell ou por meio do Citrix Scout.

Os registros AOT são coletados e salvos em disco, mesmo quando os uploads agendados do Call Home estão desativados. (Quando os uploads agendados são desativados, os logs AOT não são carregados automaticamente para a Citrix.) Você pode desativar a coleta e o armazenamento local de logs AOT.

Desativar o Call Home com o PowerShell Depois de executar o seguinte cmdlet, os dados de diagnóstico não serão carregados para a Citrix automaticamente. (Você ainda pode fazer upload de dados de diagnóstico usando cmdlets Citrix Scout ou telemetria PowerShell.)

```
Disable-CitrixCallHome
```

Para confirmar se o Call Home está desativado, digite `Get-CitrixCallHome`. Se estiver desativado, os valores fornecidos são `IsEnabled=False` e `IsMasterImage=False`.

Desative um cronograma de coleta usando o Citrix Scout Para desativar um cronograma de coleta de diagnóstico usando o Citrix Scout, siga as orientações em Agendar coletas. Na etapa 3, clique em **Off** para cancelar a programação das máquinas selecionadas.

Desativar a coleta de logs AOT Depois de executar o seguinte cmdlet (com o campo `Enabled` definido como **`false`**), os logs de 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 de Call Home

Conclua as seguintes tarefas na máquina em que o Call Home está ativado. Os diagramas de exemplo no procedimento a seguir contêm endereço do servidor e porta 10.158.139.37:3128. Suas informações serão diferentes.

1. Adicione informações do servidor proxy em seu navegador. No Internet Explorer, selecione **Opções da Internet > Conexões > Configurações de LAN**. Selecione **Usar um servidor proxy para sua LAN** e insira o endereço do servidor proxy e o número da porta.
2. No PowerShell, execute `netsh winhttp import proxy source=ie`.

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

3. Usando um editor de texto, edite o arquivo de configuração TelemetryService.exe, localizado em C:\Program Files\Citrix\Telemetry Service. Adicione as informações mostradas na caixa vermelha.

```
TelemetryService.exe - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
            <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
    </startup>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
          <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
        </dependentAssembly>
        <probing privatePath="TelemetryModule" />
      </assemblyBinding>
    </runtime>
<system.net>
<defaultProxy>
<proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
</defaultProxy>
</system.net>

</configuration>
```

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 fazer upload de 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 fazer upload de um pacote usando o site do CIS:

1. Faça logon no Citrix Insight Services usando as credenciais da sua conta Citrix.
2. Selecione **My Workspace**.
3. Selecione **Healthcheck** e navegue até o local dos dados.

O CIS oferece suporte a vários cmdlets do PowerShell que gerenciam uploads de dados. Esta documentação abrange os cmdlets para dois casos comuns:

- Use o 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. Posteriormente, use o cmdlet `Send-CitrixCallHomeBundle` para carregar manualmente uma cópia desse pacote para o CIS. (Os dados que você salvou originalmente permanecem salvos localmente.)

A ajuda do PowerShell fornece sintaxe abrangente, incluindo descrições de cmdlets e parâmetros que não são usados nesses casos de uso comuns.

Quando você 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 executando um upload.

Coletar dados e carregar o pacote para o CIS:

```
1 Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
     string] [-Description string] [-IncidentTime string] [-SRNumber
     string] [-Name string] [-UploadHeader string] [-AppendHeaders string
     ] [-Collect string] [<CommonParameters>]
2 <!--NeedCopy-->
```

Coletar dados e salvá-los localmente:

```
1 Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
     Description string] [-IncidentTime string] [-SRNumber string] [-Name
      string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
     strings] [<CommonParameters>]
2 <!--NeedCopy-->
```

Os seguintes parâmetros são válidos:

- **Credential:** Direciona o upload para o CIS.
- **InputPath:** Localização do arquivo zip a ser incluído no pacote. Esse pode ser um arquivo adicional solicitado pelo Citrix Support. Lembre-se de incluir a extensão.zip.
- **OutputPath:** Local onde as informações de diagnóstico são salvas. Esse parâmetro é necessário ao salvar os dados do Call Home localmente.
- **Description and Incident Time:** Informações em formulário de formato livre sobre o upload.
- **SRNumber:** número de incidente do Suporte Técnico da Citrix.
- **Name:** Nome que identifica o pacote.

- **UploadHeader:** String formatada em JSON que especifica os cabeçalhos de upload carregados para o CIS.
- **AppendHeaders:** String formatada em JSON que especifica os cabeçalhos anexados carregados para o CIS.
- **Collect:** String formatada em JSON especificando quais dados coletar ou omitir, na forma { 'collector':{'enabled':Boolean}}, onde o booleano é verdadeiro ou falso.
  Os valores de coletor válidos são:
  - 'wmi'
  - 'process'
  - 'registry
  - 'crashreport'
  - 'trace'
  - 'file'
  - 'msi'
  - 'localdata'
  - 'sitedata'
  - 'sfb'

  Por padrão, todos os coletores, exceto 'sfb', estão ativados.

  O coletor 'sfb'foi concebido para ser usado sob demanda para diagnosticar problemas do Skype for Business. Além do parâmetro 'enabled', o coletor 'sfb'suporta os parâmetros account'e 'accounts'para especificar usuários de destino. Use um dos formulários:
  - "-Collect "{'sfb':{'account':'domain\\user1'}}"
  - "-Collect "{'sfb':{'accounts':['domain\\\user1', 'domain\\\user2']}}"
- **Parâmetros comuns:** Consulte a ajuda do PowerShell.

Carregar dados que foram salvos anteriormente localmente:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

O parâmetro `Path` especifica a localização do pacote salvo anteriormente.

Exemplos:

O cmdlet a seguir solicita um upload de dados do Call Home (excluindo dados do coletor WMI) para o CIS. Esses dados são relacionados a falhas de registro do Citrix Provisioning VDAs, que foram detectadas às 14:30 em relação ao caso do Citrix Support 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' }
 "
<!--NeedCopy-->
```

O cmdlet a seguir salva os dados do Call Home relacionados ao caso do Citrix Support 223344, detectado às 8:15. Os dados foram 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
<!--NeedCopy-->
```

O cmdlet a seguir carrega o pacote de dados que você salvou anteriormente.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  – Credential $cred -Path \mynetwork\
    myshare\mydata.zip
<!--NeedCopy-->
```

Citrix Scout

June 28, 2023

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 uma análise abrangente e automatizada das coletas de diagnósticos por meio do Citrix Insight Services. Você também pode usar o Scout para solucionar problemas, por conta própria ou com as orientações do suporte da Citrix.

Você pode fazer upload de arquivos de coleção para a Citrix para análise e orientação do suporte da Citrix. Ou, você pode salvar uma coleta localmente para sua própria análise e depois fazer upload do arquivo de coleta para a Citrix para análise.

O Scout oferece os seguintes procedimentos:

- **Colect:** Executa uma única coleta de diagnósticos em máquinas selecionadas em um site. Em seguida, você pode carregar o arquivo para o Citrix ou salvá-lo localmente.
- **Trace & Reproduce:** Inicia um rastreamento manual nas máquinas selecionadas. Em seguida, você recria problemas nessas máquinas. Depois de recriar o problema, o rastreamento é interrompido. Em seguida, o Scout coleta outros diagnósticos e carrega o arquivo para o Citrix ou salva o arquivo localmente.
- **Schedule:** agenda as coletas de diagnósticos para que ocorram diariamente ou semanalmente em um horário especificado nas máquinas selecionadas. O arquivo é carregado automaticamente para a Citrix.
- **Health Check:** executa verificações que avaliam a integridade e a disponibilidade do site e de seus componentes. Você pode executar verificações de integridade para controladores de entrega, agentes de entrega virtuais (VDAs), servidores StoreFront e Servidores de licença Citrix. Se forem encontrados problemas durante as verificações, o Scout fornecerá um relatório detalhado. Cada vez que o Scout inicia, ele verifica se há scripts de verificação de integridade atualizados. Se novas versões estiverem disponíveis, o Scout as baixará automaticamente, para uso na próxima vez que as verificações de integridade forem executadas.

> **Nota:**
>
> Os procedimentos **Trace & Reproduce**, **Schedule** e **Health Check** atualmente não estão disponíveis para Linux VDA.

A interface gráfica descrita neste artigo é a principal maneira de usar o Scout. Como alternativa, você pode usar o PowerShell para configurar coleções 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 servidores de licença. 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 Citrix Virtual Apps and Desktops Service), execute o Scout a partir de um VDA para coletar diagnósticos locais.

O registro do aplicativo Scout é armazenado em `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Esse arquivo pode ser usado para solução de problemas.

O que é coletado

Os diagnósticos coletados pelo Scout incluem arquivos de log de rastreamento do Citrix Diagnostic Facility (CDF). Um subconjunto de rastreamentos de CDF chamado AOT (Always-On Tracing) também está incluído. As informações de AOT podem ser úteis ao solucionar problemas comuns, como registros VDA e lançamentos de aplicativos/desktops. Nenhuma outra informação de Rastreamento de Eventos para 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) sob **Citrix namespace**.
- Processos que estão em execução.
- Despejos de memória de processos Citrix que são armazenados em %PROGRAMDATA%\Citrix\CDF.
- Informações sobre políticas Citrix, em formato CSV.
- Informações de instalação e atualização. A coleta pode incluir o log completo do metainstalador do produto, logs MSI com falha, saída do analisador de log MSI, logs do StoreFront, registros de verificação de compatibilidade de licenciamento e resultados de testes preliminares de atualização do site.

Sobre informações de rastreamento:

- As informações de rastreamento são compactadas à medida que são coletadas, o que reduz o uso de recursos da máquina.
- Em cada máquina, o Citrix Telemetry Service mantém as informações de rastreamento recentes compactadas por no máximo 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 traços eram mantidos na memória.) Caminho padrão = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partir do Citrix Virtual Apps and Desktops 7 1811, os rastreamentos AOT salvos em compartilhamentos de rede são coletados com outros diagnósticos.
- Você pode modificar o tamanho máximo (padrão = 10 MB) e a duração da fatia, usando o cmdlet `Enable-CitrixTrace` ou a string de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Os rastreamentos são anexados ao arquivo até que o arquivo atinja 10% de `MaxSize`.

Para obter uma lista dos datapoints que o Scout coleta, consulte Datapoints chave do Call Home.

Configuração do Scout

O Scout pode ser configurado para funcionar em VDAs Linux. Para obter mais informações sobre Linux VDA e telemetria, consulte Integração com o Citrix Telemetry Service

O Linux VDA pode alterar automaticamente a porta do soquete `ctxtelemetry` ou a porta do serviço de telemetria. Em caso afirmativo, você deve configurar a porta manualmente.

1. Navegue 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 Linux VDA:

- `<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 da 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 Environment Test Service, que fornece uma avaliação abrangente dos serviços FlexCast Management Architecture (FMA). Além de verificar a disponibilidade do serviço, essas verificações buscam outros indicadores de integridade, como conexões de banco de dados.

As verificações de integridade do site são executadas em Controladores de entrega. Dependendo do tamanho do seu site, essas verificações podem levar até uma hora para que sejam 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 de Virtual Apps and Desktops:

- Um ou mais Delivery Controllers estão apresentando falha.
- Há apenas um Delivery Controller no site.
- Os Delivery Controllers são de versões diferentes.

Além do respeito às permissões e requisitos de verificações de integridade, as verificações de configuração do Delivery Controller exigem:

- Pelo menos um controlador ligado.
- O serviço Broker em execução em um controlador.
- Uma conexão de trabalho do controlador com o banco de dados do site.

Verificações de integridade VDA

As verificações de integridade do VDA identificam possíveis causas para problemas comuns de registro VDA, lançamento de sessão e redirecionamento de fuso horário.

Para registro no VDA, o Scout verifica:

- Instalação do software VDA
- Associação ao domínio da máquina VDA
- Disponibilidade da porta de comunicação VDA
- Status do serviço VDA
- Configuração de firewall do Windows
- Comunicação com o Controller
- Sincronização de tempo com o Controller
- Status de registro VDA

Para o lançamento de sessões em VDAs, o Scout verifica:

- Disponibilidade da porta de comunicação de início de sessão
- Status dos serviços de início de sessão
- Iniciar sessão Configuração de firewall do Windows
- Licenças de acesso para cliente do VDA Remote Desktop Services
- Caminho de início do aplicativo VDA
- Configurações de registro de início de sessão

Para redirecionamento de fuso horário em VDAs, o Scout verifica:

- Instalação de hotfix do Windows
- Instalação de hotfix da Citrix
- Configurações da política de grupo da Microsoft
- Configurações da política de grupo Citrix

Para Profile Management em VDAs, o Scout verifica:

- Detecção do Hypervisor
- Detecção do Provisioning
- Citrix Virtual Apps and Desktops

- Configuração pessoal do vDisk
- Armazenamento do usuário
- Detecção de status do Profile Management Service
- Teste de hooking de Winlogon.exe

Para executar verificações no Profile Management, você deve instalar e ativar o Profile Management no VDA. Para obter mais informações sobre verificações de configuração do Profile Management, consulte o artigo do Knowledge Center CTX132805.

Verificações de integridade do StoreFront

As verificações do StoreFront verificam:

- 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
- O URL base tem um FQDN válido
- O endereço IP correto da URL base pode ser obtido
- O pool de aplicativos do IIS está usando .NET 4.0
- Se o certificado está vinculado à porta SSL para o 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

Verificações do Servidor de Licenças verificam:

- Conexão do Servidor de Licenças do Delivery Controller
- Status do acesso remoto do firewall do Servidor de Licenças
- Status do serviço Citrix Licensing
- Estado do período de carência do Servidor de Licenças
- Conexão de 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 Citrix Licensing está sendo executado na conta de serviço local
- Presença do arquivo `CITRIX.opt`
- Data de qualificação dos Customer Success Services
- 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 será descoberto.

Execute verificações de integridade

O procedimento de verificação de integridade inclui a seleção de máquinas, iniciar a verificação e, em seguida, revisar o relatório de resultados.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Health Check**.
2. Selecionar máquinas. Clique em **Find machine** para descobrir máquinas. A página **Select machines** lista todos os VDAs, controladores de entrega e servidores de licença descobertos 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 diagnósticos e clique em **Continue**.

   Para adicionar outros tipos de componentes (como servidores StoreFront e máquinas VDA), consulte Adicionar máquinas manualmente e Importar máquinas VDA. Você não pode adicionar manualmente Citrix Provisioning Servers ou servidores de licenças.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, certificando-se de que ele atende aos critérios listados nos testes de verificação. Se a verificação falhar, uma mensagem será publicada na coluna **Status** e a caixa de seleção dessa máquina será desmarcada. Você pode:

   - Resolver o problema e marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (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 **Continue**.
3. Execute as verificações de integridade nas máquinas selecionadas. O resumo lista as máquinas em que os testes são executados (as máquinas que você selecionou que passaram nos testes de verificação). Clique em **Start Checking**.

   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 **Stop Checking** no canto inferior direito da página. (Você não pode cancelar a verificação de integridade de uma

única máquina, apenas 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 **Stop Checking** no canto inferior direito muda para **Done**.
- Se uma verificação falhar, você poderá clicar em **Retry** na coluna **Action**.
- Se uma verificação for concluída sem problemas encontrados, a coluna **Action** estará vazia.
- Se uma verificação encontrar problemas, clique em **View Details** para mostrar os resultados.
- Depois que a verificação for concluída para todas as máquinas selecionadas, não clique em **Back**. (Se você fizer isso, os resultados da verificação serão perdidos.)

4. Quando as verificações forem concluídas, clique em **Done** para retornar à página de abertura do Scout.

Resultados da verificação de integridade

Para verificações Citrix geradoras de relatórios, os relatórios contêm:

- Hora e data em que o relatório de resultados foi gerado
- Máquinas que foram verificadas
- Condições que o cheque procurava 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 membro do grupo de usuários do domínio.
  - Você deve ser um administrador com direitos completos ou ter uma função personalizada com permissões somente leitura e **Run Environment Tests** para o site.
  - Defina a política de execução de script como pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** outros privilégios de execução de scripts também podem funcionar.

- Use **Executar como administrador** ao iniciar o Scout.

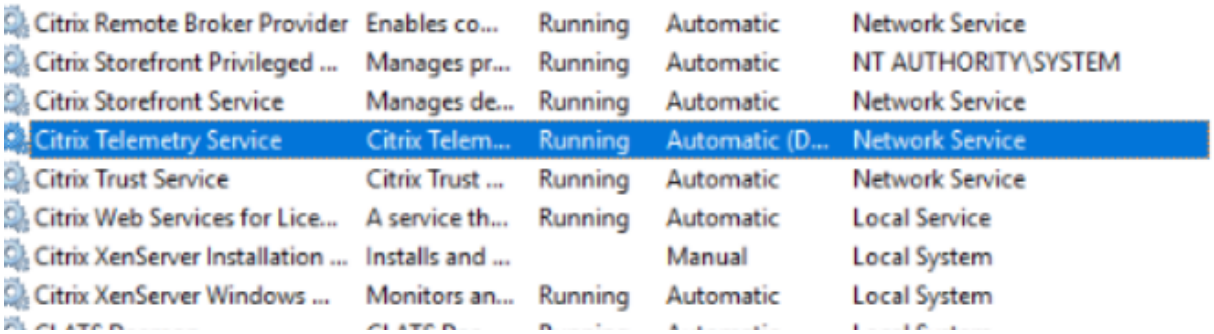
Para cada máquina da qual você coleta diagnósticos ou executa verificações de integridade:

- O Scout deve ter a capacidade 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 Infraestrutura de Gerenciamento do Windows (WMI) deve estar habilitado na máquina.
- Para definir um cronograma para coleta de diagnóstico, a máquina deve estar executando uma versão Scout compatível.

Não use o cifrão ($) em nomes de usuário especificados em nomes de caminho. Isso impede a coleta de informações diagnósticas.

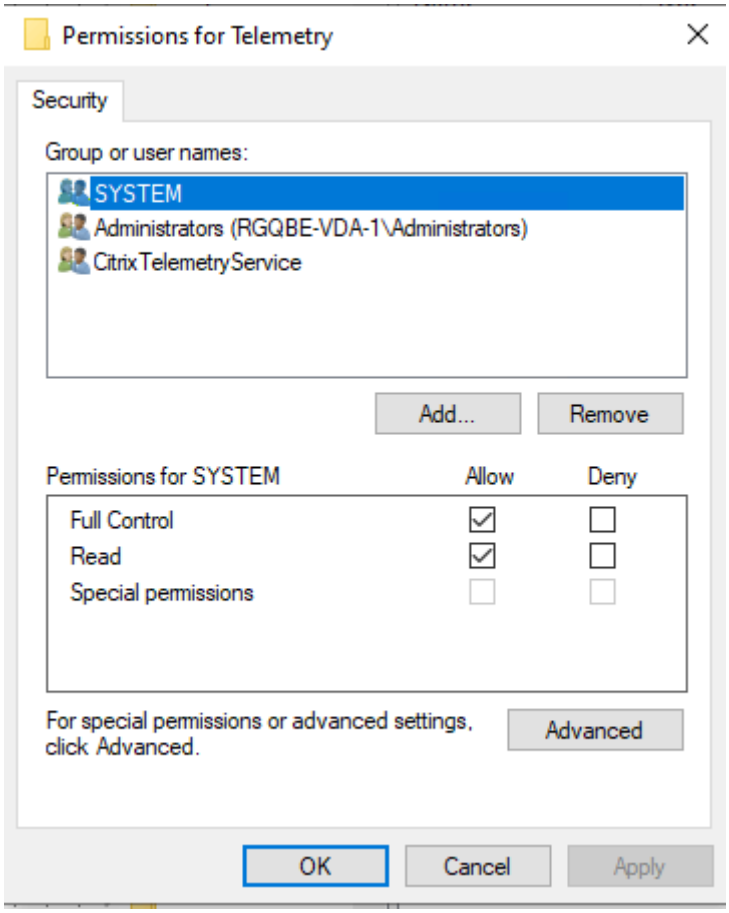
O Scout executa testes de verificação nas máquinas selecionadas para garantir que esses requisitos sejam atendidos.

O serviço de telemetria para Windows é executado no Serviço de Rede.

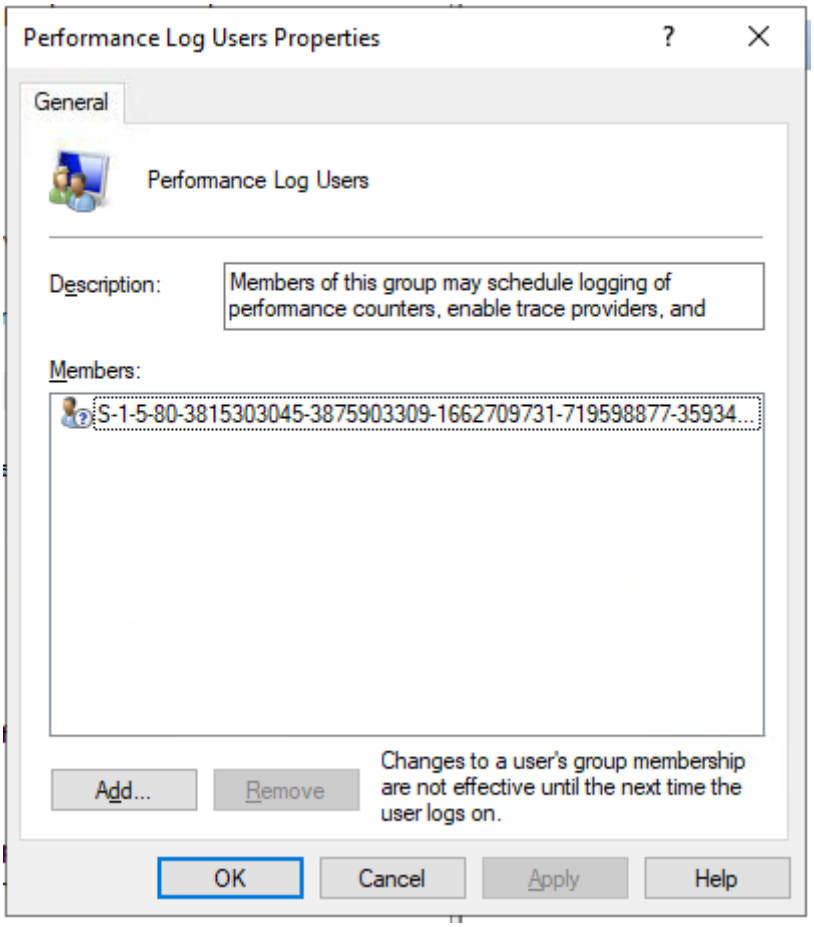


A pasta de rastreamento AOT é salva em `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Somente usuários no grupo Administrador, Sistema e Serviço de Telemetria SID têm permissão para acessar o registro `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.



O SID do Serviço de Telemetria permanece no grupo Usuários do Log de Desempenho após a desinstalação do Serviço de Telemetria, mas você pode removê-lo manualmente.



Testes de verificação

Antes de iniciar uma coleta de diagnóstico ou verificação de integridade, 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 cannot reach this machine** - Certifique-se de que:
  - A máquina está ligada.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir verificar se o firewall está configurado corretamente.)
  - O compartilhamento de arquivos e impressoras está ativado. Consulte a documentação da Microsoft para obter instruções.
- **Enable PSRemoting and WinRM** - Você pode ativar a comunicação remota do PowerShell 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 requires PowerShell 3.0 (minimum)** - Instale o PowerShell 3.0 (ou posterior) na máquina e, em seguida, ative a comunicação remota do PowerShell.
- **Unable to access LocalAppData directory on this machine** - Verifique se a conta tem permissão para gravar no diretório LocalAppData na máquina.
- **Cannot locate Citrix Telemetry Service** —Verifique se o Citrix Telemetry Service está instalado e foi iniciado na máquina.
- **Cannot get schedule** - Atualize a máquina para (mínimo) XenApp e XenDesktop 7.14.
- **WMI is not running on the machine** - Certifique-se de que o acesso ao Windows Management Instrumentation (WMI) está habilitado.
- **WMI connections blocked** - Ative o WMI no serviço Firewall do Windows.
- **Newer version of Citrix Telemetry Service required** - (A versão é verificada somente 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 estará incluída nas ações **Collect** ou **Trace & Reproduce** .
- **Scout cannot connect to the systemd socket on this machine** - Certifique-se de que:
  - A porta 7503 está aberta. Verifique se o systemd ctxtelemetry.socket está escutando na porta 7503 da máquina. A porta pode ser diferente se a porta ctxtelemetry.socket tiver sido alterada. Consulte Configuração do Scout para ajustar portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir verificar se o firewall está configurado corretamente.)
- **The Linux VDA Telemetry Service is not started on this machine** - Certifique-se de que:
  - A porta 7502 está aberta. Verifique se o Linux VDA Telemetry Service 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 portas.
  - A conexão de rede está funcionando corretamente. (Isso pode incluir verificar se o firewall está configurado corretamente.)

Compatibilidade de versão

Esta versão do Scout (3.x) destina-se a ser executada em Controllers e VDAs do Citrix Virtual Apps and Desktops (ou no mínimo XenApp e XenDesktop 7.14).

Uma versão anterior do Scout é fornecida com as versões XenApp e XenDesktop anteriores a 7.14. Para obter informações sobre essa versão anterior, consulte CTX130147.

Se você atualizar um Controlador ou VDA anterior a 7.14 para a versão 7.14 (ou uma versão com suporte posterior), a versão anterior do Scout será substituída pela versão atual.

Recurso	Scout 2.23	Scout 3.0
Suporte Citrix Virtual Apps and Desktops (além de XenApp e XenDesktop 7.14 a 7.18)	Sim	Sim
Suporte a XenDesktop 5.x, 7.1—7.13	Sim	Não
Suporte a XenApp 6.x, 7.5 a 7.13	Sim	Não
Entregue com produto	7.1–7.13	Começando com 7.14
Pode ser baixado do artigo CTX	Sim	Não
Capturar rastreamentos CDF	Sim	Sim
Capturar rastreamento constante (AOT)	Não	Sim
Permitir coleta de dados de diagnóstico	Até 10 máquinas ao mesmo tempo (por padrão)	Ilimitado (sujeito à disponibilidade de recursos)
Permitir que dados de diagnóstico sejam enviados para a Citrix	Sim	Sim
Permitir que dados de diagnóstico sejam salvos localmente	Sim	Sim
Suporte às credenciais do Citrix Cloud	Não	Sim
Suporte a credenciais Citrix	Sim	Sim
Suporte ao servidor proxy para uploads	Sim	Sim
Ajustar agendamentos	N/A	Sim
Suporte a scripts	Linha de comando (somente Controller local)	PowerShell usando cmdlets Call Home (qualquer máquina com o Serviço de Telemetria instalado)
Verificações de integridade	Não	Sim
Mascaramento de dados	Não	Começando com 3.17

Instalar e atualizar

Por padrão, o Scout é instalado ou atualizado automaticamente como parte do Citrix Telemetry Service quando você instala ou atualiza um VDA ou um controlador.

Se você omitir o Citrix Telemetry Service ao instalar um VDA ou remover o serviço posteriormente, execute `TelemetryServiceInstaller_xx.msi` a partir do `x64\Virtual Desktop Components` ou da pasta `x86\Virtual Desktop Components` ou na mídia de instalação do Citrix Virtual Apps and Desktops.

Quando você seleciona a ação **Collect** ou **Trace & Reproduce**, você será notificado se uma máquina estiver executando uma versão mais antiga do Citrix Telemetry Service. A Citrix recomenda usar a versão mais recente com suporte. Se você não atualizar o Serviço de Telemetria nessa máquina, ele não será incluído nas ações **Collect** ou **Trace & Reproduce** . Para atualizar o Serviço de Telemetria, use o mesmo procedimento que instalá-lo.

Autorização de upload

Se você planeja fazer upload de coleções de diagnóstico para a Citrix, você deve ter uma conta Citrix ou Citrix Cloud. (Essas são as credenciais que você usa para acessar downloads da Citrix ou acessar o Citrix Cloud Control Center.) Depois que as credenciais da conta forem validadas, um token é emitido.

Se você se autenticar com uma conta da Citrix ou uma conta do Citrix Cloud, clique em um link para acessar o Citrix Cloud usando HTTPS com seu navegador padrão. Depois de inserir suas credenciais do Citrix Cloud, o token é exibido. Copie o token e cole-o no Scout. Em seguida, você pode continuar no assistente Scout.

O token é armazenado localmente na máquina em que você está executando o Scout. Para habilitar o uso desse token na próxima vez que você executar **Collect** ou **Trace & Reproduce**, marque a caixa de seleção **Store token and skip this step in the future** .

Você deve reautorizar sempre que selecionar **Schedule** na página de abertura do Scout. Você não pode usar um token armazenado ao criar ou alterar um agendamento.

Usar um proxy para uploads

Se você quiser usar um servidor proxy para fazer upload de coleções para o Citrix, você pode instruir o Scout a usar as configurações de proxy definidas nas Propriedades da Internet do seu navegador. Como alternativa, você pode especificar o endereço IP e o número da porta do servidor proxy.

Encontrar máquina

No caso dos procedimentos **Collect**, **Trace & Reproduce** e **Schedule** o Scout lista os Controladores e VDAs que ele descobre automaticamente.

Quando você executa a Verificação de integridade do Scout a partir do Delivery Controller, clique em **Find machine** para descobrir máquinas, incluindo controladores de entrega, VDAs, servidores de licença e servidores StoreFront.

Quando você executa a verificação de integridade do Scout a partir de uma máquina associada ao domínio que não é 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 listar os Controllers e VDAs detectados, você pode adicionar manualmente outras máquinas na implantação, como servidores StoreFront, License Servers 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 Licenças manualmente.
- No momento, as verificações de integridade não oferecem suporte aos servidores Citrix Provisioning.

Em qualquer página do Scout que lista as máquinas descobertas, clique em **+ Adicionar máquina.**. Digite o FQDN da máquina que você deseja adicionar e clique em **Continue**. Repita para adicionar outras máquinas, conforme necessário. (Embora a inserção de um alias DNS em vez de um FQDN possa parecer válida, as verificações de integridade podem falhar.)

As máquinas adicionadas manualmente sempre aparecem na parte superior da lista de máquinas, acima das máquinas descobertas.

Uma maneira fácil de identificar uma máquina adicionada manualmente é o botão de exclusão vermelho na extremidade direita da linha. Somente máquinas adicionadas manualmente têm esse botão. Máquinas descobertas não o têm.

Para remover uma máquina adicionada manualmente, clique no botão vermelho na extremidade direita da linha. Confirme a exclusão. Repita para excluir outras máquinas adicionadas manualmente.

O Scout lembra as máquinas adicionadas manualmente até que você as remova. Quando você fecha e reabre o Scout, as máquinas adicionadas manualmente ainda estão listadas na parte superior da lista.

Rastreamentos CDF não são coletados ao usar **Trace & Reproduce** em servidores StoreFront. No entanto, todas as outras informações de rastreamento são coletadas.

Importar máquinas VDA

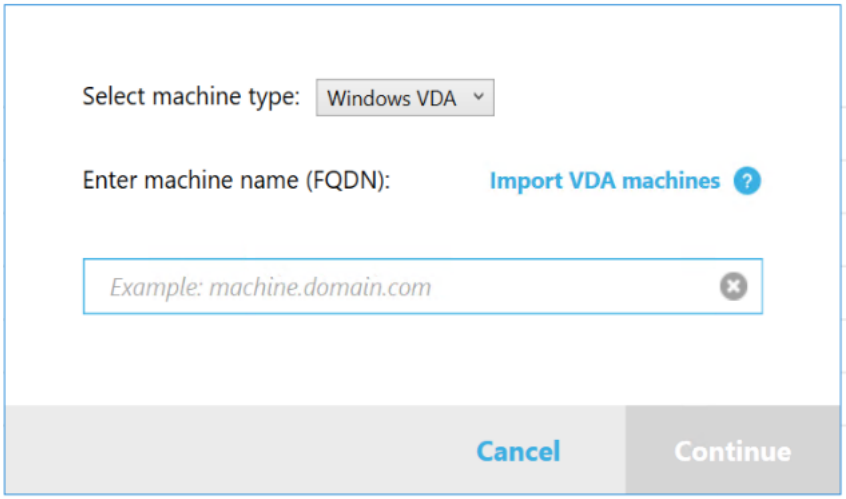
Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

1. Em Delivery Controller ou Connector, gere o arquivo de lista de máquinas com o comando PowerShell. No Connector, você deve inserir credenciais Citrix e selecionar o cliente na caixa de diálogo pop-up.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. Copie o arquivo machineList.txt para a máquina associada ao domínio que você deseja iniciar a verificação de integridade do Scout.
3. Na página Verificação de integridade do Scout, clique em **Add Machine**.
4. Selecione o tipo de máquina **Windows VDA**.
5. Clique em **Import VDA machines**.
6. Selecione o arquivo machineList.txt.
7. Clique em **Open**.

As máquinas VDA importadas estão listadas na página Scout Health Check.



Coletar diagnósticos

O procedimento **Collect** inclui a seleção de máquinas, iniciar a coleção de diagnósticos e, em seguida, carregar o arquivo que contém a coleção para a Citrix ou salvá-la localmente.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Collect**.
2. Selecionar máquinas.

   - Em um Controller, a página **Select machines** lista todos os VDAs e Controllers 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 **Select machines** lista somente a máquina local. Não há suporte para adicionar máquinas manualmente.

   Marque a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e clique em **Continue**.

   O Scout inicia automaticamente testes de verificação em cada máquina selecionada, verificando se ele atende aos critérios listados nos testes de verificação. Se a verificação for malsucedida, uma mensagem será publicada na coluna **Status** e a caixa de seleção dessa máquina não está marcada. Você pode:

   - Resolver o problema e marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignorar essa máquina (deixe a caixa de seleção desmarcada). Os diagnósticos não serão coletados dessa máquina.

   Quando os testes de verificação forem concluídos, clique em **Continue**.
3. Coletar diagnósticos. O resumo lista todas as máquinas das quais os diagnósticos são coletados (as máquinas que você selecionou que passaram nos testes de verificação). Clique em **Start Collecting**.

   Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta de uma máquina.
   - Para interromper uma coleção em andamento em uma única máquina, clique em **Cancel** na coluna **Action** dessa máquina.
   - Para interromper todas as coleções em andamento, clique em **Stop Collection** no canto inferior direito da página. Os diagnósticos de máquinas que concluíram a coleta são mantidos. Para retomar a coleção, clique em **Retry** na coluna **Action** de cada máquina.
   - Quando a coleção for concluída para todas as máquinas selecionadas, o botão **Stop Collection** no canto inferior direito muda para **Continue**.
   - Para coletar diagnósticos novamente, clique em **Collect Again** na coluna **Action** dessa máquina. A coleta mais recente substitui a anterior.
   - Se uma coleção falhar, você poderá clicar em **Retry** na coluna **Action** . Somente coleções bem-sucedidas são carregadas ou salvas.

- Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Back**. (Se você clicar nesse botão, a coleta será perdida.)

Quando a coleção for concluída, clique em **Continue**.

4. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para o Citrix ou salve-o na máquina local.

   Se você optar por carregar o arquivo agora, vá para a Etapa 5.

   Se você optar por salvar o arquivo localmente:

   - É exibida uma caixa de diálogo **Salvar** do Windows. Navegue até o local desejado.
   - Quando o salvamento local for concluído, o nome do caminho do arquivo é exibido e vinculado. Você pode visualizar o arquivo. Você pode fazer upload do arquivo mais tarde para a Citrix. Consulte CTX136396.

   Clique em **Done** para retornar à página de abertura do Scout. Você não precisa concluir nenhuma outra etapa neste procedimento.

5. Autentique para uploads e, opcionalmente, especifique um proxy. Para obter detalhes, consulte Autorização de upload.

   - Se você não tiver autenticado por meio do Scout, continue com esta etapa.
   - Se você tiver autenticado por meio do Scout, o token de autorização armazenado será usado por padrão. Se for isso que você deseja fazer, selecione essa opção e clique em **Continue**. Você não é solicitado a fornecer credenciais para essa coleção. Vá para a Etapa 6.
   - Se você tiver autenticado anteriormente, mas quiser reautorizar e obter um novo token, clique em **Change/Reauthorize** e continue com esta etapa.

   Escolha se você deseja usar credenciais Citrix ou credenciais do Citrix Cloud para autenticar o upload. Clique em **Continue**. A página de credenciais será exibida somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configure proxy**. Você pode instruir o Scout a usar as configurações de proxy definidas nas 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 de proxy.
   - Para uma conta do Citrix Cloud, clique em **Generate token**. Seu navegador padrão é iniciado em uma página do Citrix Cloud na qual um token é exibido. Copie o token e cole-o na página Scout.
   - Para uma conta Citrix, insira suas credenciais.

Quando terminar, clique em **Continue**.

6. Insira informações sobre o upload.

   - O campo 'name'contém o nome padrão do arquivo para o diagnóstico coletado. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo nome vazio, o nome padrão será usado.)
   - Opcionalmente, especifique um número de caso do Citrix Support de 8 dígitos.
   - No campo opcional **Description**, descreva o problema e indique quando o problema ocorreu, se aplicável.

   Quando terminar, clique em **Start Upload**.

   Durante o upload, a parte inferior esquerda da página fornece um valor aproximado da porcentagem do upload que foi concluída. Para cancelar um upload em andamento, clique em **Stop Upload**.

   Quando o upload for concluído, a URL de sua localização é exibida e vinculada. Você pode seguir o link para o local Citrix para visualizar a análise do upload ou copiar o link.

   Clique em **Done** para retornar à página de abertura do Scout.

Rastrear e reproduzir

O procedimento **Trace and Reproduce** inclui a seleção de máquinas, iniciar um rastreamento, reproduzir problemas, concluir a coleção de diagnósticos e, em seguida, carregar o arquivo para o Citrix ou salvá-lo localmente.

Este procedimento é semelhante ao procedimento **Collect** padrão. No entanto, ele permite que você inicie um rastreamento em máquinas e recrie problemas nessas máquinas. Todas as coleções de diagnósticos incluem informações de rastreamento AOT. Este procedimento adiciona rastreamentos de CDF para ajudar na solução de problemas.

1. Inicie o Scout. No menu **Iniciar** da máquina, selecione **Citrix > Citrix Scout**. Na página de abertura, clique em **Trace & Reproduce**.
2. Selecionar máquinas. A página **Select machines** 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 rastros e diagnósticos. Depois 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, certificando-se de que ele atende aos critérios listados nos testes de verificação. Se a

verificação falhar para uma máquina, uma mensagem será publicada na coluna **Status** e a caixa de seleção dessa máquina não estará marcada. Você pode:

- Resolver o problema e marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
- Ignorar essa máquina (deixe a caixa de seleção desmarcada). Diagnósticos e traços não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continue**.

3. Inicie o traço. O resumo lista todas as máquinas das quais os traços são coletados. Clique em **Iniciar rastreamento**.

   Em uma ou mais das máquinas selecionadas, reproduza os problemas que você enfrentou. A coleção de rastreamento continua enquanto você está fazendo isso. Quando terminar de reproduzir o problema, clique em **Continue** no Scout. Isso interrompe o rastreamento.

   Depois de interromper o rastreamento, indique se você reproduziu o problema durante o rastreamento.

4. Colete diagnósticos de máquinas. Clique em **Start Collecting**. Durante a coleta:

   - A coluna **Status** indica o estado atual da coleta de uma máquina.
   - Para interromper uma coleção em andamento em uma única máquina, clique em **Cancel** na coluna **Action** dessa máquina.
   - Para interromper todas as coleções em andamento, clique em **Stop Collection** no canto inferior direito da página. Os diagnósticos de máquinas que concluíram a coleta são mantidos. Para retomar a coleção, clique em **Retry** na coluna **Action** de cada máquina.
   - Quando a coleção for concluída para todas as máquinas selecionadas, o botão **Stop Collection** no canto inferior direito muda para **Continue**.
   - Para coletar diagnósticos novamente de uma máquina, clique em **Collect Again** na coluna **Action** dessa máquina. A coleta mais recente substitui a anterior.
   - Se uma coleção falhar, você poderá clicar em **Retry** na coluna **Action** . Somente coleções bem-sucedidas são carregadas ou salvas.
   - Depois que a coleta for concluída para todas as máquinas selecionadas, não clique em **Back**. (Se você fizer isso, a coleção será perdida.)

   Quando a coleção for concluída, clique em **Continue**.

5. Salve ou carregue a coleta. Escolha se deseja carregar o arquivo para o 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:

   - É exibida uma caixa de diálogo Salvar do Windows. Selecione o local desejado.

- Quando o salvamento local for concluído, o nome do caminho do arquivo é exibido e vinculado. Você pode visualizar o arquivo. Lembre-se: Você pode fazer upload do arquivo mais tarde da Citrix; consulte CTX136396 com relação a Citrix Insight Services.

Clique em **Done** para retornar à página de abertura do Scout. Você não precisa concluir nenhuma outra etapa neste procedimento.

6. Autenticar para uploads e, opcionalmente, especificar proxy. Veja a autorização de Upload para obter detalhes desse processo.

   - Se você não tiver autenticado por meio do Scout, continue com esta etapa.
   - Se você for autenticado por meio do Scout, o token de autorização armazenado será usado por padrão. Se isso for o que você deseja fazer, escolha essa opção e clique em **Continue**. Você não é solicitado a fornecer credenciais para essa coleção. Vá para a Etapa 7.
   - Se você tiver sido autenticado anteriormente, mas quiser reautorizar e obter um novo token, clique em **Change/Reauthorize** e continue com esta etapa.

   Escolha se você deseja usar credenciais Citrix ou credenciais do Citrix Cloud para autenticar o upload. Clique em **Continue**. A página de credenciais será exibida somente se você não estiver usando um token armazenado.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configure proxy**. Você pode instruir o Scout a usar as configurações de proxy definidas nas 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 de proxy.
   - Para uma conta do Citrix Cloud, clique em **Generate token**. Seu navegador padrão é iniciado para uma página do Citrix Cloud na qual um token é exibido. Copie o token e cole-o na página Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continue**.

7. Forneça informações sobre o upload.

   Insira os detalhes do upload:

   - O campo ‘name’contém o nome padrão do arquivo para o diagnóstico coletado. Isso é suficiente para a maioria das coletas, embora você possa alterar o nome. (Se você excluir o nome padrão e deixar o campo nome vazio, o nome padrão será usado.)
   - Opcionalmente, especifique um número de caso do Citrix Support de 8 dígitos.
   - No campo opcional Description, descreva o problema e indique quando o problema ocorreu, se aplicável.

Quando terminar, clique em **Start Upload**.

Durante o upload, a parte inferior esquerda da página fornece um valor aproximado da porcentagem do upload que foi concluída. Para cancelar um upload em andamento, clique em **Stop Upload**.

Quando o upload for concluído, a URL de sua localização é exibida e vinculada. Você pode seguir o link para o local Citrix para visualizar a análise do upload ou copiar o link.

Clique em **Done** para retornar à página de abertura do Scout.

Habilitar coleta de logs adicionais

A função **Enable additional log collection** permite que você use a função trace e reproduza a função com mais ferramentas, como perfmon, Netsh, DebugView e Wireshark.

> **Nota:**
>
> Isso só se aplica a máquinas locais.

Para configurar a coleta de logs adicionais:

1. Inicie o Citrix Scout.
2. Clique na engrenagem de **Settings**.
3. Clique em **Enable additional log collection with more tools**.
4. Clique em **Salvar**.

Para coletar logs adicionais:

1. Na página inicial do Scout, clique em **Trace & Reproduce**.
2. Na página **Select machines**, clique na engrenagem no lado direito da máquina local.
3. Na página **Select the tools require for logging:**, clique em **Download Tools**.
4. Na página **Download Tools**, selecione as ferramentas que deseja usar e clique em **Download**. As ferramentas são baixadas, exceto o Wireshark. O Wireshark só pode ser baixado e instalado manualmente.
   Nota: se optar por baixar outras ferramentas manualmente, você deve 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, descompacte o conteúdo do arquivo em `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`.
5. Na página **Select the tools require for logging:**, clique em **Refresh Status**. Todas as ferramentas selecionadas aparecem como **Present** na coluna Status.
6. Selecione as ferramentas para registro e clique em **Next**.
7. Siga as instruções em 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 o rastreamento, os logs de Process Monitor poderão crescer rapidamente. Certifique-se de selecionar apenas as ferramentas que são necessárias. Você também pode monitorar o tamanho dos logs em *%temp%\Scout-CDC-Log*.

Agendar coletas

> **Nota:**
>
> No momento, você pode agendar coletas, mas não verificações de integridade.

O procedimento Schedule compreende a seleção de máquinas e, em seguida, definir ou cancelar a programação. As coletas agendadas são carregadas automaticamente para o Citrix. (Você pode salvar coleções 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 **Schedule**.
2. Selecionar máquinas. Todos os VDAs e Controllers no site estão listados. Você pode filtrar a exibição por nome da máquina.

   Quando você instalou VDAs e Controllers usando a interface gráfica, se você definir um agendamento do Call Home (consulte Citrix Call Home), o Scout exibirá essas configurações, por padrão. Você pode usar esta versão do Scout para iniciar coleções agendadas pela primeira vez ou alterar uma programação configurada anteriormente.

   Embora você tenha habilitado/desativado o Call Home para cada máquina separadamente durante a instalação do componente, um agendamento configurado no Scout afeta todas as máquinas selecionadas.

   Marque a caixa de seleção ao lado de cada máquina da qual você deseja coletar diagnósticos e clique em **Continue**.

   Para adicionar outras máquinas manualmente (como servidores StoreFront ou Citrix Provisioning), consulte Adicionar máquinas manualmente.

   O Scout inicia automaticamente testes de verificação nas máquinas selecionadas, verificando se ele atende aos critérios nos testes de verificação. Se a verificação falhar para uma máquina, uma mensagem será publicada na coluna **Status** e a caixa de seleção dessa máquina não estará marcada. Você pode:

   - Resolver o problema e marcar a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.

- Ignorar essa máquina (deixe a caixa de seleção desmarcada). Diagnósticos (ou rastreamentos) não são coletados dessa máquina.

Quando os testes de verificação forem concluídos, clique em **Continue**.

A página de resumo lista as máquinas às quais os agendamentos são aplicados. Clique em **Continue**.

3. Defina o agendamento. Indique quando você deseja que o diagnóstico seja coletado. Lembre-se: A programação afeta todas as máquinas selecionadas.

   - Para configurar uma programação semanal para as máquinas selecionadas, clique em **Weekly**. Escolha o dia da semana. Insira a hora do dia (relógio de 24 horas) para que a coleta comece.
   - Para configurar uma programação diária para as máquinas selecionadas, clique em **Daily**. Insira a hora do dia (relógio de 24 horas) para que a coleta comece.
   - Para cancelar uma programação existente para as máquinas selecionadas (e não substituí-la por outra), clique em **Off**. Isso cancela qualquer agendamento configurado anteriormente para essas máquinas.

   Clique em **Continue**.

4. Autentique para uploads e, opcionalmente, especifique um proxy. Veja a autorização de Upload para obter detalhes desse processo. Lembre-se: Você não pode usar um token armazenado para autenticar ao trabalhar com um agendamento do Scout.

   Escolha se você deseja usar credenciais Citrix ou credenciais do Citrix Cloud para autenticar o upload. Clique em **Continue**.

   Na página de credenciais:

   - Se você quiser usar um servidor proxy para o upload do arquivo, clique em **Configure proxy**. Você pode instruir o Scout a usar as configurações de proxy definidas nas 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 de proxy.
   - Para uma conta do Citrix Cloud, clique em **Generate token**. Seu navegador padrão é iniciado em uma página do Citrix Cloud na qual um token é exibido. Copie o token e cole-o na página Scout.
   - Para uma conta Citrix, insira suas credenciais.

   Quando terminar, clique em **Continue**.

   Revise o cronograma configurado. Clique em **Done** para retornar à página de abertura 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 sigilosas quanto à segurança. O recurso de mascaramento de dados Citrix Scout permite mascarar dados confidenciais 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 máquina, nomes de domínio, nomes de usuário, nomes de hipervisor, nomes de grupo de entrega, nomes de catálogo, nomes de aplicativos e SIDs.

> **Nota:**
>
> Os rastreamentos CDF são criptografados e não podem ser mascarados.
>
> Os logs Linux VDA são compactados para o formato `.tar.gz2` e não podem ser mascarados.

Colete novos diagnósticos e execute o 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 em que o Scout está instalado: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Lançamento Scout: `ScoutUI.exe datamasking`.
4. Clique em **Collect** ou **Trace & Reproduce** para coletar diagnósticos.
5. Após a conclusão da coleta, selecione **Enable data masking**. Essa opção está ativada por padrão.
6. Configure a máscara de dados. Você pode usar as regras padrão ou personalizar as regras.
7. Selecione se deseja carregar ou salvar a coleta de diagnósticos.
    - Se você selecionar **Upload the diagnostics collection to Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Save the diagnostics collection on your local machine**, tanto o diagnóstico original quanto o mascarado serão salvos no local especificado.

Execute o mascaramento de dados em diagnósticos existentes

1. No Windows, abra o prompt de comando como administrador.
2. Vá para o diretório em que 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 "Enable data masking"para continuar. Essa opção está ativada 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 coleta de diagnósticos.

    - Se você selecionar **Upload the diagnostics collection to Citrix**, os arquivos de diagnóstico mascarados serão carregados para a Citrix.
    - Se você selecionar **Save the diagnostics collection on your local machine**, tanto o diagnóstico original quanto o mascarado serão salvos no local especificado.

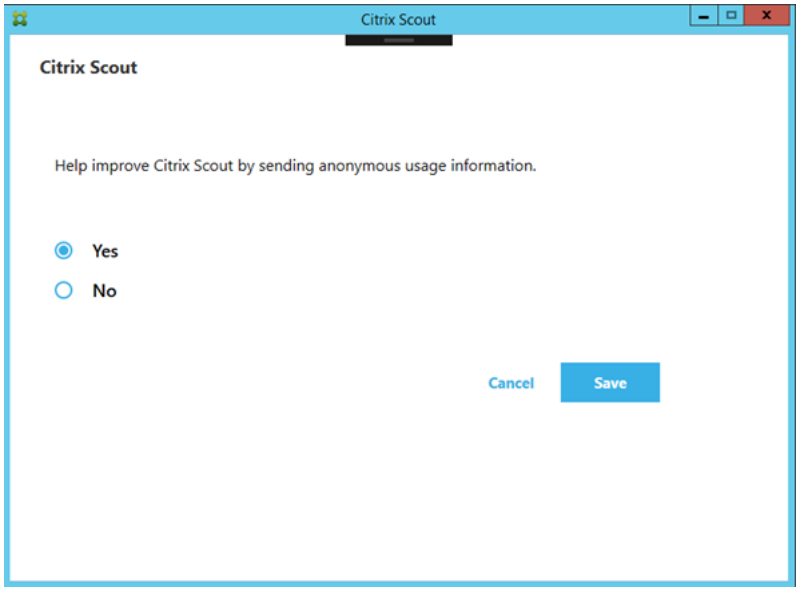
Masked data file and mapping file locations

Depois de carregar ou salvar a coleção de diagnósticos, clique no link para abrir os diagnósticos original e mascarado e abra o arquivo de informações de mapeamento.

Coleta de dados de uso

Quando você usa o Scout, a Citrix usa o Google Analytics para coletar dados de uso anônimos que serão usados para futuros recursos e melhorias do produto. A coleta de dados está ativada por padrão.

Para alterar a coleta e o upload de dados de uso, clique na engrenagem **Settings** na interface do usuário do Scout. Você pode escolher se deseja enviar as informações selecionando **Yes** ou **No** e, em seguida, clicando em **Save**.



Coletar rastreamento Citrix Diagnostic Facility (CDF) na inicialização do sistema

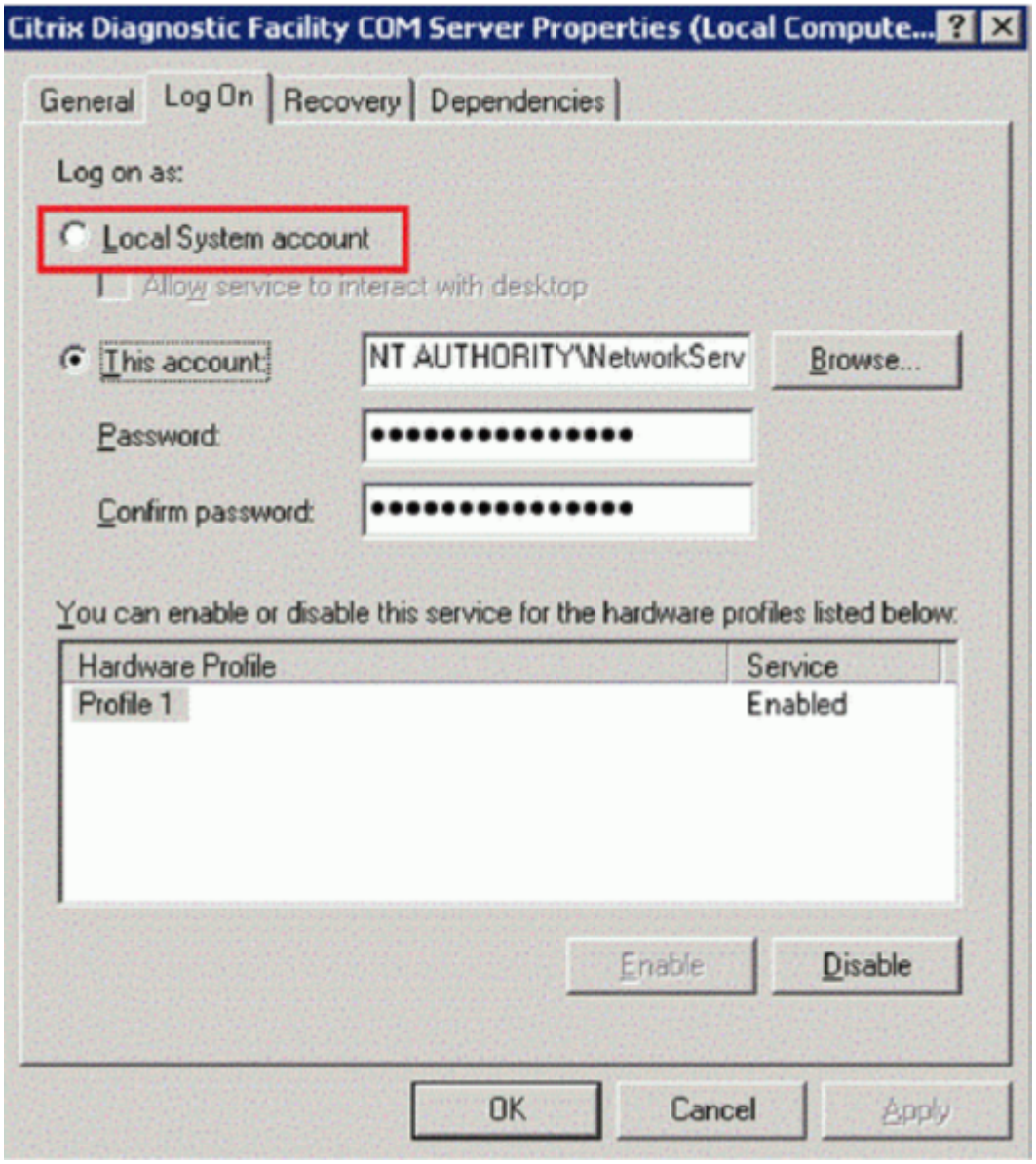
June 28, 2023

O utilitário CDFControl é um controlador de rastreamento de eventos ou consumidores que captura mensagens de rastreamento Citrix Diagnostic Facility (CDF) exibidas de vários provedores de rastreamento da Citrix. Sua utilidade é solucionar problemas complexos relacionados à Citrix, analisar o suporte a filtros e coletar dados de desempenho. Para baixar o utilitário CDFControl, consulte CTX111961.

Usar a conta Sistema Local

Para usar a conta Sistema Local para o serviço de servidor CDF COM, execute as seguintes etapas:

1. Clique em **Executar** no menu **Iniciar**.
2. Digite `services.msc` na caixa de diálogo e clique em **OK**.
3. Selecione o serviço **Citrix Diagnostics Facility COM Server** e escolha **Propriedades**.
4. Clique na guia **Logon** e ative a conta **Sistema local**. Em seguida, clique em **OK**.

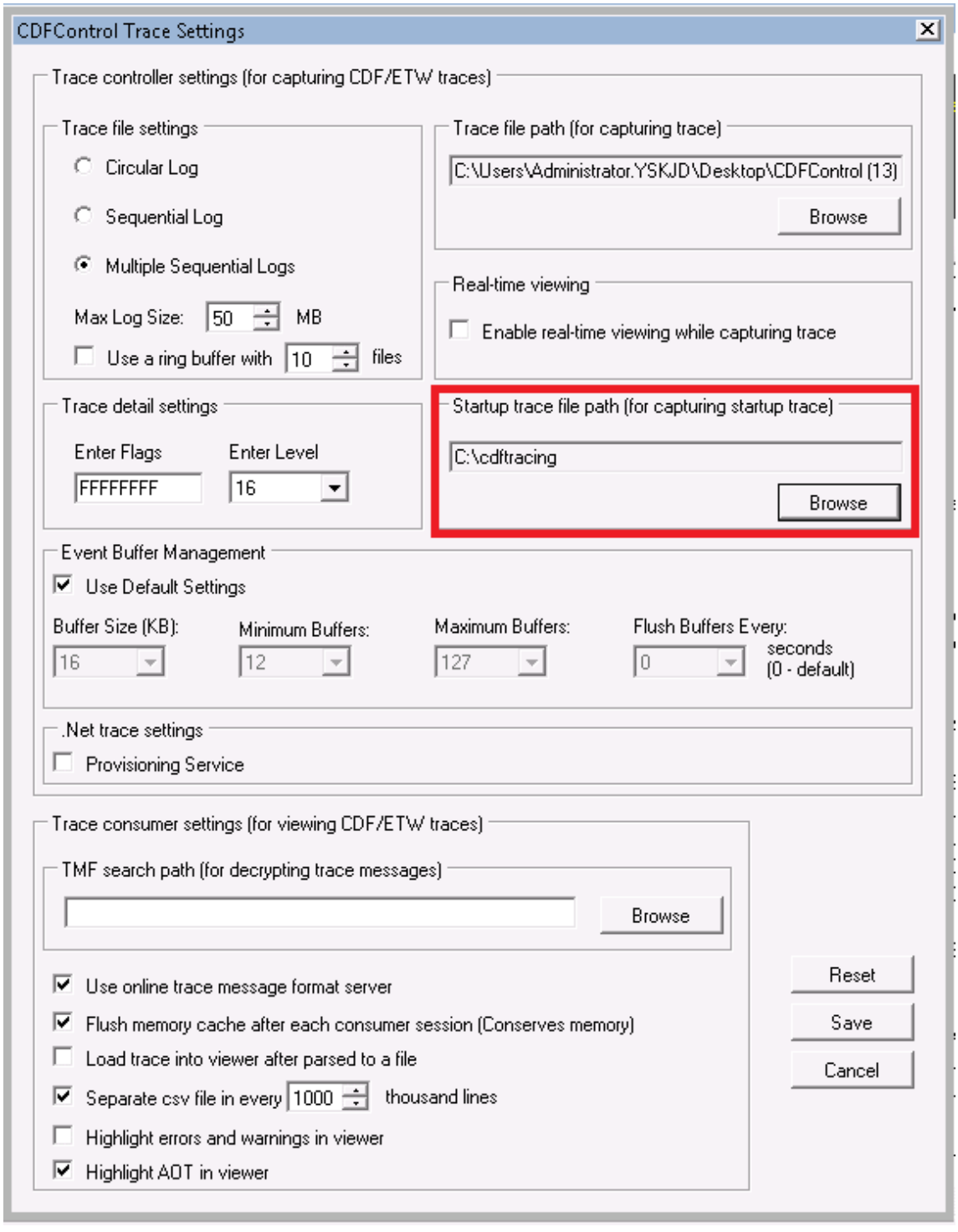


5. Reinicie o serviço.

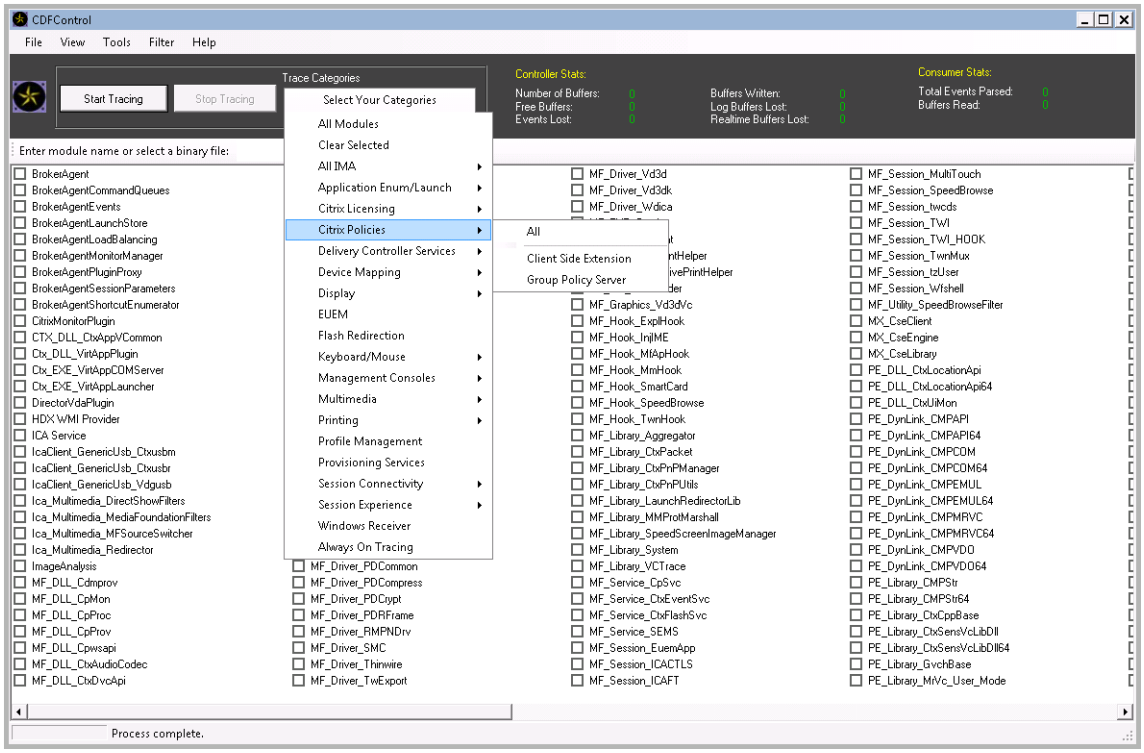
Coletar um rastreamento na inicialização do sistema

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 **Options** no menu **Tools**.
2. Especifique o caminho do arquivo de rastreamento na seção **Startup trace file path for capturing startup trace**. Em seguida, clique em **Save**.



3. Selecione as **categorias de rastreamento** recomendadas pelo suporte Citrix. (No exemplo a seguir, foi selecionado **Citrix Policies**. Essa seleção é apenas um exemplo. Recomendamos que você habilite os provedores para o problema específico que está solucionando.)



4. Selecione **Startup Tracing** e selecione **Enable** no menu **Tools**.

   Depois de selecionar **Enable**, a barra animada inicia a rolagem. Essa atividade não afeta o procedimento. Continue para o próximo passo.

5. Depois que **Startup Tracing** for ativado, feche **CDFControl utility** e reinicialize o sistema.
6. Inicie o utilitário **CDFControl**. Depois que o sistema for reinicializado e o erro aparecer, desative o rastreamento de inicialização selecionando **Startup Tracing** no menu **Tools** e clicando em **Disable**.
7. Pare o serviço de servidor **Citrix Diagnostics Facility COM**.
8. Vá para o caminho do arquivo de rastreamento especificado na etapa 2 e colete o arquivo de log de rastreamento (.etl) para análise.
9. Inicie o serviço de servidor **Citrix Diagnostics Facility COM**.

Administração delegada

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O modelo de administração delegada oferece a flexibilidade de corresponder à forma como a sua organização deseja delegar atividades administrativas, usando controle baseado em objeto e função. A administração delegada acomoda implantações de todos os tamanhos e permite configurar mais granularidade de permissão 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 suas contas do Active Directory. Cada administrador está associado a um ou mais pares de função e escopo.
- **Funções:** uma função representa um cargo de trabalho e tem permissões definidas associadas a ela. Por exemplo, a função Administrador do Grupo de Entrega tem permissões como "Criar grupo de entrega"e "Remover área de trabalho do grupo de entrega". Um administrador pode ter várias funções para um site, ou seja, uma pessoa possa ser Administrador de Grupo de Entrega e Administrador de Catálogo de Máquinas. As funções podem ser incorporadas ou personalizadas.

  As funções internas são:

Função	Permissions
Full Administrator	Pode executar todas as tarefas e operações. Um administrador completo é sempre combinado com o escopo Todos.
Read Only Administrator	Pode ver todos os objetos nos 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 Log de Configuração) e quaisquer objetos com escopo Londres (por exemplo, Grupos de Entrega de Londres). No entanto, esse administrador não pode ver objetos no escopo de Nova York (supondo que os escopos Londres e Nova York não se sobrepõem).

Função	Permissions
Help Desk Administrator	Pode exibir grupos de entrega e gerenciar sessões, máquinas e computadores associados a esses grupos. Pode ver informações do catálogo de máquinas e do host para os grupos de entrega que estão sendo monitorados. Também pode executar operações de gerenciamento de sessão e gerenciamento de energia da máquina para as máquinas nesses grupos de entrega.
Machine Catalog Administrator	Pode criar e gerenciar catálogos de máquina e provisionar as máquinas neles. Pode criar catálogos de máquinas a partir da infraestrutura de virtualização, Provisioning Services e máquinas físicas. Esta função pode gerenciar imagens básicas e instalar softwares, mas não pode atribuir aplicativos ou áreas de trabalho aos usuários.
Delivery Group Administrator	Pode entregar aplicativos, áreas de trabalho, máquinas e computadores; também pode gerenciar as sessões associadas. Também pode gerenciar configurações de aplicativos e áreas de trabalho, como configurações de gerenciamento de energia e políticas.
Host Administrator	Pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, computadores, aplicativos ou áreas de trabalho aos usuários.

Em determinadas edições do produto, você pode criar funções personalizadas para atender aos requisitos da sua organização e delegar permissões com mais detalhes. Você pode usar funções personalizadas para alocar permissões na granularidade de uma ação ou tarefa em um console.

- **Escopos:** um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma que seja relevante para a sua organização (por exemplo, o conjunto de Grupos de Entrega usado pela equipe de vendas). Os objetos podem estar em mais de um escopo; você pode pensar em objetos rotulados com um ou mais escopos. Há um escopo interno: "All", que contém Todos os objetos. A função de administrador completo é sempre casada com o escopo Todos.

Exemplo

A empresa XYZ decidiu gerenciar aplicativos e áreas de trabalho com base no departamento (Contas, Vendas e Armazém) e sistema operacional do computador (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 usam.

Os seguintes administradores foram criados:

Administrador	Funções	Escopos
domínio/fred	Full Administrator	Todos (a função de administrador completo sempre tem o escopo All)
domínio/rob	Read Only Administrator	Todos
domínio/heidi	Administrador somente leitura, administrador de assistência técnica	Todos de Vendas
domínio/warehouseadmin	Help Desk Administrator	Armazém
domínio/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 executar tarefas de assistência técnica em grupos de entrega no escopo 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 warehouseadmin do Active Directory pode exibir e executar tarefas de assistência técnica em máquinas no escopo Armazém.
- Peter é especialista em Windows 7 e pode gerenciar todos os catálogos de máquinas do Windows 7 e pode entregar aplicativos, áreas de trabalho, computadores e máquinas com Windows 7, independentemente do escopo do departamento em que estão. O administrador considerou tornar Peter um administrador completo para o escopo Win7. No entanto, ela decidiu contra isso, porque um administrador completo também tem direitos completos sobre todos os objetos que não têm 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 alguns administradores fazem tudo. Não há delegação. Nesse caso, crie cada administrador com a função de administrador completo interna, que tem o escopo Todos.
- Em implantações maiores com mais máquinas, computadores, aplicativos e áreas de trabalho, é necessária mais delegação. Vários administradores podem ter responsabilidades funcionais (funções) mais específicas. Por exemplo, dois são administradores completos e os outros são administradores de assistência técnica. Além disso, um administrador pode gerenciar apenas determinados grupos de objetos (escopos), como catálogos de máquinas. Nesse caso, crie novos escopos, além de administradores com uma das funções internas e os escopos apropriados.
- Implantações ainda maiores podem exigir mais escopos ou escopos mais específicos, além de administradores diferentes com funções não convencionais. Nesse caso, edite ou crie mais escopos, crie funções personalizadas e crie cada administrador com uma função interna ou personalizada, além de escopos novos e existentes.

Para flexibilidade e facilidade de configuração, você pode criar escopos quando criar um administrador. Você também pode especificar escopos ao criar ou editar Catálogos de Máquinas ou conexões.

Criar e gerenciar administradores

Quando você cria um site como administrador local, sua conta de usuário se torna automaticamente um administrador completo com permissões completas sobre todos os objetos. Depois que um site é criado, os administradores locais não têm privilégios especiais.

A função de administrador completo sempre tem o escopo All; você não pode alterar isso.

Por padrão, um administrador está ativo. Desativar um administrador pode ser necessário se você estiver criando o administrador agora, mas a pessoa só for iniciar as tarefas administrativas mais tarde. Para administradores ativos existentes, você pode desativar vários deles enquanto estiver reorganizando seu objeto/escopos e, em seguida, reativá-los quando estiver pronto para usar a configuração atualizada. Você não pode desativar um administrador completo se isso resultar em nenhum administrador completo ativo. A caixa de seleção ativar/desativar está disponível quando você cria, copia ou edita um administrador.

Quando você exclui um par de função/escopo durante a cópia, edição ou exclusão de um administrador, isso exclui apenas a relação entre a função e o escopo do administrador. Isso não exclui

nem a função nem o escopo. Também não afeta nenhum outro administrador que esteja configurado com esse par de função/escopo.

Para criar e gerenciar administradores, siga estas etapas:

1. Entre no Web Studio, clique em **Administrators** no painel esquerdo e clique na guia **Administrators**.
2. Siga as instruções para a tarefa que você deseja concluir:
    - **Criar um administrador:** clique em **Create Administrator** na barra de ações. Digite ou navegue até o nome da conta de usuário, selecione ou crie um escopo e, depois, selecione uma função. O novo administrador está ativado por padrão; você pode alterar isso.
    - **Copiar um administrador:** selecione o administrador e clique em **Copy Administrator** na barra de ações. Digite ou navegue até o nome da conta de usuário. Você pode selecionar e editar ou excluir qualquer um dos pares de função/escopo e adicionar novos pares. O novo administrador está ativado por padrão; você pode alterar isso.
    - **Editar um administrador:** selecione o administrador e clique em **Edit Administrator** na barra de ações. Você pode editar ou excluir qualquer um dos pares de função/escopo e adicionar novos pares.
    - **Excluir um administrador:** selecione o administrador e clique em **Delete Administrator** na barra de ações. Você não pode excluir um administrador completo se isso resultar em nenhum administrador completo ativo.

O painel superior exibe os administradores que você criou. Selecione um administrador para exibir seus detalhes no painel inferior. A coluna **Warnings** indica se os pares de função e escopo associados ao administrador contêm funções ou escopos inutilizáveis. A seguinte mensagem de aviso será exibida se um par de função e escopo associados contiver funções ou escopos inutilizáveis:

- Função ou escopo associado não utilizável

> **Importante:**
>
> Uma mensagem de aviso só aparece quando um par de função e escopo associados contém funções ou escopos inutilizáveis ou ambos.

Para remover o par de função e escopo do administrador, execute uma das seguintes etapas:

- Exclua o par de função e escopo.
    1. Na barra de ações, clique em **Edit Administrator**.
    2. Na janela **Administrator Name and Details**, selecione o par de função e escopo e clique em **Delete**.
    3. Clique em **Save** para sair.
- Exclua o administrador.

1. Na barra de ações, clique em **Delete Administrator**.
2. Na janela de confirmação, clique em **Delete**.

Criar e gerenciar funções

Quando os administradores criam ou editam uma função, eles podem ativar apenas as permissões que eles próprios têm. Isso impede que os administradores criem uma função com mais permissões do que as que têm no momento e a atribuam a si mesmos (ou editem uma função à qual já estão atribuídos).

Os nomes de funções 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, barra vertical, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo. As descrições podem conter até 256 caracteres Unicode.

Não é possível editar ou excluir uma função interna. Não é possível excluir uma função personalizada se algum administrador a estiver usando.

> **Nota:**
>
> Apenas algumas edições do produto suportam funções personalizadas. Somente as edições que suportam funções personalizadas têm entradas relacionadas na barra de ações.

Para criar e gerenciar funções, siga estas etapas:

1. Entre no Web Studio, clique em **Administrators** no painel esquerdo e clique na guia **Roles**.
2. Siga as instruções para a tarefa que você deseja concluir:
   - **Exibir detalhes da função:** selecione a função. O painel inferior lista os tipos de objetos e as permissões associadas para a função. Clique na guia **Administrators** no painel inferior para exibir uma lista de administradores que atualmente têm a função.
   - **Criar uma função personalizada:** clique em **Create Role** no painel de ações. Insira um nome e uma descrição. Selecione os tipos de objetos e as permissões.
   - **Copiar uma função:** selecione a função e clique em **Copy Role** na barra de ações. Altere o nome, a descrição, os tipos de objetos e as permissões, conforme necessário.
   - **Editar uma função personalizada:** selecione a função e clique em **Edit Role** na barra de ações. Altere o nome, a descrição, os tipos de objetos e as permissões, conforme necessário.
   - **Excluir uma função personalizada:** selecione a função e clique em **Delete Role** na barra de ações. Quando solicitado, confirme a exclusão.

Criar e gerenciar escopos

Quando você cria um site, o único escopo disponível é o escopo "All", que não pode ser excluído.

Você pode criar escopos usando o procedimento a seguir. Você também pode criar escopos quando criar um administrador; cada administrador deve estar associado a pelo menos um par de função e escopo. Ao criar ou editar áreas de trabalho, catálogos de máquinas, aplicativos ou hosts, você pode adicioná-los a um escopo existente. Se você não adicioná-los a um escopo, eles permanecem parte do escopo "All".

Na criação do site não se pode aplicar um escopo nem em objetos de administração delegada (escopos e funções). No entanto, os objetos aos quais você não pode aplicar escopo são incluídos no escopo "All". (Administradores completos sempre têm o escopo Todos.) Máquinas, ações de energia, áreas de trabalho e sessões não têm escopo diretamente aplicado. Os administradores podem ter permissões alocadas a esses objetos por meio de catálogos de máquinas ou grupos de entrega associados.

Regras para criar e gerenciar escopos:

- Os nomes de escopo podem conter até 64 caracteres Unicode. Os nomes de escopo não podem incluir: barra invertida, barra, ponto e vírgula, dois pontos, cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda, seta para a direita, barra vertical, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas ou apóstrofo.
- A descrição dos escopos pode conter até 256 caracteres Unicode.
- Quando você copia ou edita um escopo, lembre-se de que a remoção de objetos do escopo pode tornar esses objetos inacessíveis ao administrador. Se o escopo editado estiver casado com uma ou mais funções, certifique-se de que as atualizações do escopo não tornem nenhum par de função/escopo inutilizável.

Para criar e gerenciar escopos, siga estas etapas:

1. Entre no Web Studio, clique em **Administrators** no painel esquerdo e clique na guia **Scopes**.
2. Siga as instruções para a tarefa que você deseja concluir:
    - **Criar um escopo:** clique em **Create Scope** na barra de ações. Insira um nome e uma descrição. Para incluir todos os objetos de um tipo específico (por exemplo, Grupos de Entrega), selecione o tipo de objeto. Para incluir objetos específicos, expanda o tipo e selecione objetos individuais (por exemplo, Grupos de Entrega usados pela equipe de vendas).
    - **Copiar um escopo:** selecione o escopo e clique em **Copy Scope** na barra de ações. Insira um nome e uma descrição. Altere os tipos de objetos e objetos, conforme necessário.
    - **Editar um escopo:** selecione o escopo e clique em **Edit Scope** na barra de ações. Altere o nome, a descrição, os tipos de objetos e os objetos, conforme necessário.

- **Excluir um escopo:** selecione o escopo e clique em **Delete Scope** na barra de ações. Quando solicitado, confirme a exclusão.

Criar relatórios

Você pode criar dois tipos de relatórios de administração delegados:

- 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, grupos de entrega e catálogos de máquinas). Você gera esse relatório a partir do Web Studio.

  Para criar esse relatório, siga estas etapas:

  1. Entre no Web Studio, clique em **Administrators** no painel esquerdo
  2. Selecione um administrador e clique em **Create Report** na barra de ações.

  Você também pode solicitar esse 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 esse relatório executando um script do PowerShell chamado OutputPermissionMapping.ps1.

  Para executar esse 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

Parâmetro	Descrição
-Show	(Válido somente quando o parâmetro -Path também é especificado.) Quando você grava a saída em um arquivo, -Show faz com que a saída seja aberta em um programa apropriado, como um navegador da Web.
CommonParameters	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
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Em um prompt de comando do Windows, o comando do exemplo anterior é:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
<!--NeedCopy-->
```

Delivery Controllers

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles

> de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

O Delivery Controller é o componente do lado do servidor que é responsável por gerenciar o acesso do usuário, além de intermediar e otimizar conexões. Os Controllers também fornecem Machine Creation Services que criam imagens de área de trabalho 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 mais tarde. Há dois benefícios principais de ter mais de um Controller em um site.

- **Redundância:** como prática recomendada, em um site de produção, sempre tenha pelo menos dois Controllers em diferentes servidores físicos. Se um Controller falhar, os outros podem gerenciar conexões e administrar o site.
- **Escalabilidade:** à medida que a atividade do site cresce, o mesmo acontece com a utilização da CPU na atividade do Controller e do banco de dados. Controllers adicionais permitem que você lide com mais usuários e mais aplicativos e com solicitações da área de trabalho, além de 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 comunicam-se com o banco de dados do site na zona primária.

> **Importante:**
>
> Não altere o nome do computador ou a associação de domínio de um Controller após a configuração do site.

Como os VDAs se registram nos Controllers

Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) em um Delivery Controller no site. Para obter informações sobre o registro VDA, consulte Registro de VDA com controladores.

Adicionar, remover ou mover Controllers

Para adicionar, remover ou mover um Controller, você deve ter permissões à função de servidor e à função de banco de dados listadas no artigo Bancos de dados.

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

Ao adicionar um Delivery Controller a um site, certifique-se de adicionar credenciais de logon da máquina aos SQL Servers de réplica que você usa para alta disponibilidade.

Se a sua implantação usa espelhamento de banco de dados:

- Antes de adicionar, remover ou mover um Controller, certifique-se de que os bancos de dados principal e espelhado estejam em execução. Além disso, se você estiver usando scripts com o SQL Server Management Studio, ative o modo SQLCMD antes de executar os scripts.
- Para verificar o espelhamento após adicionar, remover ou mover um Controller, execute o cmdlet `Get-configdbconnection` do PowerShell. Esse cmdlet garante que o parceiro de failover tenha sido definido na cadeia de conexão para o espelho.

Depois de adicionar, remover ou mover um Controller:

- Se a atualização automática estiver ativada, os VDAs receberão uma lista atualizada de Controllers dentro de 90 minutos.
- Se a atualização automática não estiver ativada, assegure-se de que a configuração da política do Controller ou a chave do registro ListOfDDCs estejam atualizadas para todos os VDAs. Depois de mover um Controller para outro site, atualize a configuração de política ou a chave do registro nos dois sites.

Adicionar um Controller

Você pode adicionar Controllers ao criar um site e posteriormente. Você não pode adicionar Controllers instalados com uma versão anterior do software a um site que foi criado com essa versão.

1. Execute o instalador em um servidor que tem um sistema operacional suportado. Instale o componente Delivery Controller e outros componentes principais desejados. Conclua o assistente de instalação.
2. Se você ainda não criou um site, execute o Citrix Site Manager neste Controller para criar um site. O endereço IP desse controlador é adicionado automaticamente ao novo site.

   Se você planeja gerar scripts que inicializam os bancos de dados, adicione os Controllers antes de gerar os scripts.
3. Se você já criou um site, siga estas etapas:

   a) Execute o Citrix Site Manager neste Controller, clique em **Join an existing site** e digite o endereço de um Controller no site ao qual você deseja ingressar.
   b) Execute a ferramenta de configuração do Studio para adicionar o Controller ao Web Studio.

Remover um Controller

A remoção de um Controller de um site não desinstala o software Citrix ou outros componentes. 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 de volta ao mesmo site ou a outro site posteriormente. Um site requer pelo menos um Controller, portanto, você não pode remover o último listado no Web Studio.

Quando você remove um Controller de um site, o logon do Controller no servidor de banco de dados não é removido. Isso evita a possibilidade de remover um logon usado pelos serviços de outros produtos na mesma máquina. O login deve ser removido manualmente se não for mais necessário. A permissão da função de servidor `securityadmin` é necessária para remover o logon.

Depois de remover um Controller:

- Os VDAs voltam a se registrar usando o registro de atualização automática com os outros Controllers disponíveis. Esse novo registro ocorre somente se o mecanismo de atualização automática estiver habilitado e os VDAs puderem alcançar outros controladores (na mesma zona secundária do Controller removido, ou na zona primária para implantações locais).
- Atualize as informações do Controller no Citrix StoreFront. Para obter mais informações, consulte Gerenciar Controllers.
- No Citrix StoreFront, atualize as URLs STA (Secure Ticket Authority) para o acesso remoto por meio do Citrix Gateway. Para obter mais informações, consulte Gerenciar Secure Ticket Authority.
- No Citrix Gateway, atualize todas as URLs STA do servidor virtual. Para obter mais informações, consulte Citrix Gateway.

> **Importante:**
>
> Não remova o Controller do Active Directory antes de removê-lo do site.

1. Certifique-se de que o Controller esteja ligado, para que o Web Studio carregue em menos de uma hora. Depois que o Web Studio carregar o Controller que você deseja remover, verifique se todos os serviços no Controller estão em execução e se o Controller está desligado.
2. Entre no Web Studio, selecione **Settings** no painel esquerdo.
3. Localize o bloco **Delivery Controller** e clique em **Edit**.
4. Na página **Manage Delivery Controller**, selecione o Controller que você deseja remover.
5. Selecione **Remove Controller**. Se você não tiver as permissões e funções corretas de banco de dados, será oferecida a opção de gerar um script que permita que o administrador do seu banco de dados remova o Controller para você.

   O Web Studio realiza uma pré-verificação antes de remover um Controller. É seguro remover um controlador se ele estiver desligado e não estiver nos seguintes status de serviço:

   - Unknown
   - Pending failure
   - Older version

- Newer version
- Version change in progress
- Missing mandatory features

Se o Controller não estiver desligado e apresentar um dos status de serviço mencionados, o Web Studio solicitará que você desligue o Controller.

6. Você deve remover a conta de máquina do Controller do servidor do banco de dados. Antes de removê-la, verifique se outro serviço não está usando a conta.

Depois de usar o Web Studio para remover um Controller, o tráfego para o Controller pode prolongar-se por um curto período de tempo para garantir a conclusão adequada das tarefas em andamento. Se você quiser forçar a remoção de um Controller em menos 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 nenhuma 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 Zonas para obter informações sobre como essa mudança pode afetar o registro de VDA e outras operações.

1. Selecione **Zone** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione um Controller.
3. Selecione **Move items** na barra de ações.
4. Na página **Move items** que aparece, selecione a zona para onde você deseja mover o Controller.
5. Clique em **Salvar**.

Mover um VDA para outro site

Se um VDA foi provisionado usando o Citrix Provisioning ou for 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 criada em um site de teste para um site de produção. Os VDAs provisionados usando o Machine Creation Services (MCS) não podem ser movidos de um site para outro. O MCS não aceita mudança da ListOfDDCs que um VDA consulta para se registrar em um Controller. Os VDAs provisionados usando MCS sempre verificam a ListOfDDCs associada ao site em que foram criados.

Há duas maneiras de mover um VDA para outro site: usando o instalador ou as políticas 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 pelo nível de grupo de entrega para iniciar uma migração de VDA em fases entre os sites.

    - Controllers: contendo FQDNs (entradas DNS) de um ou mais Controllers no site 2.
    - Enable auto update of Controllers: deixe a configuração desativada.

2. Cada VDA no grupo de entrega é alertado dentro de 90 minutos sobre a nova política. O VDA ignora a lista de Controllers que recebe (porque a atualização automática está desativada); selecione um dos Controllers especificados na política, que lista os Controllers no site 2.
3. Quando o VDA se registra com sucesso em um Controller no site 2, ele recebe a ListOfDDCs do site 2 e informações da política, que tem a atualização automática ativada por padrão. O Controller no qual o VDA foi registrado no site 1 não está na lista enviada pelo Controller no site 2. Assim, o VDA se registra novamente, escolhendo entre os Controllers na lista do site 2. A partir daí, o VDA é atualizado automaticamente com informações do site 2.

Para obter informações sobre como usar o Editor de Política de Grupo, consulte a documentação de políticas da Citrix.

Suporte a IPv4/IPv6

June 28, 2023

Esta versão oferece suporte a implantações de IPv4 puro, IPv6 puro e pilha dupla 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 da política **Only use IPv6 Controller registration**

As comunicações de IPv6 são controladas com duas configurações de política da Citrix relacionadas à conexão VDA.

- **Configuração principal que força o uso de IPv6:** Only use IPv6 Controller registration.

  Essa configuração de política controla qual a forma de endereço que o VDA usa para se registrar no Delivery Controller.

  Quando permitido, o VDA se registra e se comunica com o Controller usando um único endereço IPv6 escolhido na seguinte precedência: endereço IP global, ULA (Unique Local Address), endereço local de link (somente se nenhum outro endereço IPv6 estiver disponível).

  Quando desativado, o VDA registra e se comunica com o Controlador usando o endereço IPv4 da máquina. Este é o valor padrão.

  Se uma equipe usa frequentemente uma rede IPv6, publique as áreas de trabalho e aplicativos para esses usuários com base em uma imagem ou Unidade Organizacional (UO) que tenha a configuração de política **Only use IPv6 Controller registration** ativada.

  Se uma equipe usa frequentemente uma rede IPv4, publique as áreas de trabalho e aplicativos para esses usuários com base em uma imagem ou Unidade Organizacional (UO) 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 houver um registrado. Essa configuração especifica a rede em que o VDA se registra. O VDA se registra somente no primeiro endereço que corresponde com a máscara de rede especificada.

  Esse parâmetro é válido somente quando a política **Only use IPv6 Controller registration** está ativada. Padrão = cadeia de caracteres vazia

Considerações sobre implantação

Se o 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 os usuários.

A reconexão de sessão falha se a conexão for iniciada em uma rede IPv6 e você tentar se conectar novamente de um cliente que tenha somente acesso IPv4.

Licenciamento do Citrix Virtual Apps and Desktops usando o Web Studio

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

No Web Studio, você pode gerenciar e rastrear o licenciamento, se o servidor de licenças estiver no mesmo domínio do Web Studio ou em um domínio confiável. Para obter informações sobre tarefas de licenciamento, consulte a documentação de licenciamento e Licenciamento multitipo.

A tabela a seguir lista as edições e os modelos de licença com suporte:

Produtos	Edições	Modelos de licença
Citrix Virtual Apps	Premium, Advanced, Standard	Simultâneo
Citrix Virtual Desktops	Premium, Advanced, Standard	Usuário/dispositivo e simultâneo

Para obter mais informações, consulte Licença simultânea e licença de Licença de usuário/dispositivo.

Versão atual suportada (CRs) e versão Long Term Service Release (LTSRs)

A tabela a seguir lista a **versão mínima compatível de LS** para o Citrix Virtual Apps and Desktops, XenApp e XenDesktop. Para obter mais informações sobre as datas do ciclo de vida dos produtos Citrix, consulte a Product Matrix.

> **Importante:**
>
> As informações na tabela a seguir são fornecidas apenas para compatibilidade do produto. A Citrix recomenda que você sempre use a versão mais recente disponível do Citrix License Server para se beneficiar das melhorias funcionais ou de segurança que possa conter.
>
> **Nota:**
>
> O License Server VPX foi preterido e não receberá mais nenhuma manutenção ou correções de segurança. Os clientes que usam a 11.16.6 ou versões anteriores do License Server VPX são aconsel-

> hados a migrar para a versão mais recente do License Server para Windows assim que possível.

Versão atual	Versão LS mínima compatível
2212	11.17.2.0 compilação 35000
2209	11.17.2.0 compilação 35000
2206	11.17.2.0 compilação 35000
2203	11.17.2.0 compilação 35000
2112	11.17.2.0 compilação 35000
2109	11.17.2.0 compilação 35000
2106	11.17.2.0 compilação 35000
2103	11.16.3.0 compilação 28000

Long Term Service Release	Versão LS mínima compatível
2203 LTSR	11.17.2.0 compilação 35000
1912 LTSR	11.16.3.0 compilação 28000
7.15 LTSR	11.15.0.0 compilação 24100
7.6 LTSR	11.14.0.1 compilação 21103

Para obter informações sobre produtos legados e versões de produtos, consulte a Legacy Product Matrix.

Você deve ser um administrador de licença completo para concluir as tarefas a seguir. Para exibir as informações de licença no Web Studio, um administrador deve ter pelo menos a permissão de administração delegada Read Licensing. As funções internas Full Administrator e Read-Only Administrator têm essa permissão.

Baixar e instalar uma licença da Citrix usando o Web Studio

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione **Allocate Licenses** na barra de ações.
3. Insira o código de acesso à licença que você recebeu em um e-mail da Citrix depois que as licenças são compradas ou renovadas.

4. Selecione um produto e escolha **Allocate Licenses**. As licenças disponíveis para esse produto são alocadas e baixadas. Depois de alocar e baixar todas as licenças para um código de acesso à licença específico, você não poderá reutilizar esse código de acesso à licença. Para realizar outras transações com o mesmo código, faça logon em My Account.

Adicione licenças armazenadas em seu computador local ou na rede

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione **Add Licenses** na barra de ações.
3. Procure um arquivo de licença e adicione-o ao servidor de licenças.

Alterar o servidor de licenças

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione **Change License Server** na barra de ações.
3. Digite o endereço do servidor de licenças no formato *nome:porta*, onde o nome é um DNS, NetBIOS ou endereço IP. Se você não especificar um número de porta, a porta padrão (27000) será usada.

Selecione o tipo de licença que deve ser usada

- Ao configurar o Site, depois de especificar o servidor de licenças, você será solicitado a selecionar o tipo de licença que deve ser usada. Se não houver licenças no servidor, a opção de usar o produto por um período de teste de 30 dias sem licença será selecionada automaticamente.
- Se houver licenças no servidor, seus detalhes serão exibidos e você poderá selecionar uma delas. Ou, você pode adicionar um arquivo de licença ao servidor e, em seguida, selecioná-lo.

Alterar a edição do produto e o modelo de licenciamento

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione **Edit Product Edition** na barra de ações.
3. Atualize as opções apropriadas.

Para acessar o console de administração de licenças, selecione **License Administration Console** na barra de ações. O console aparece imediatamente ou, se o painel estiver configurado como protegido por senha, você será solicitado a fornecer credenciais do License Administration Console. Para obter detalhes sobre como usar o console, consulte a documentação de licenciamento.

> **Nota:**
>
> Quando você alterna as licenças no Web Studio, a alteração leva até 5 minutos para aparecer no Citrix Director. Por exemplo, se você alternar entre Advanced e Premium ou vice-versa.

Adicionar um administrador de licenciamento

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione a guia **Licensing Administrators**.
3. Selecione **Add licensing administrator** na barra de ações.
4. Navegue até o usuário que você deseja adicionar como administrador e escolha as permissões.

Altere as permissões de um administrador de licenciamento ou exclua um administrador de licenciamento

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione a guia **Licensing Administrators** e, em seguida, selecione o administrador.
3. Selecione **Edit licensing administrator** ou **Delete licensing administrator** na barra de ações.

Adicionar um grupo de administradores de licenciamento

1. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione a guia **Licensing Administrators**.
3. Selecione **Add licensing administrator group** na barra de ações.
4. Navegue até o grupo que você deseja atuar como administradores de licenciamento e escolha permissões. Adicionar um grupo do Active Directory dá 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. Entre no Web Studio e selecione **Licensing** no painel esquerdo.
2. Selecione a guia **Licensing Administrators** e, em seguida, selecione o grupo de administradores.
3. Selecione **Edit licensing administrator group** ou **Delete licensing administrator group** na barra de ações.

Exibir informações da licença

Entre no Web Studio e selecione **Licensing** no painel esquerdo. É exibido um resumo do uso da licença e das configurações do site com uma lista de todas as licenças atualmente instaladas no servidor de licenças especificado.

Verifique se as configurações de licenciamento do site, que incluem o tipo de produto, a edição da licença e o modelo de licenciamento, correspondem às licenças que o Servidor de Licenças configurado usa. Caso contrário, talvez seja necessário baixar ou alocar suas licenças de saída para corresponder às configurações de licença do site.

Exibir alertas de expiração de licença

O Web Studio consulta datas de expiração do arquivo de licença a partir do Citrix License Server. O Web Studio alerta os administradores na guia Overview se os arquivos de licença estiverem prestes a expirar ou já expiraram.

Links relacionados

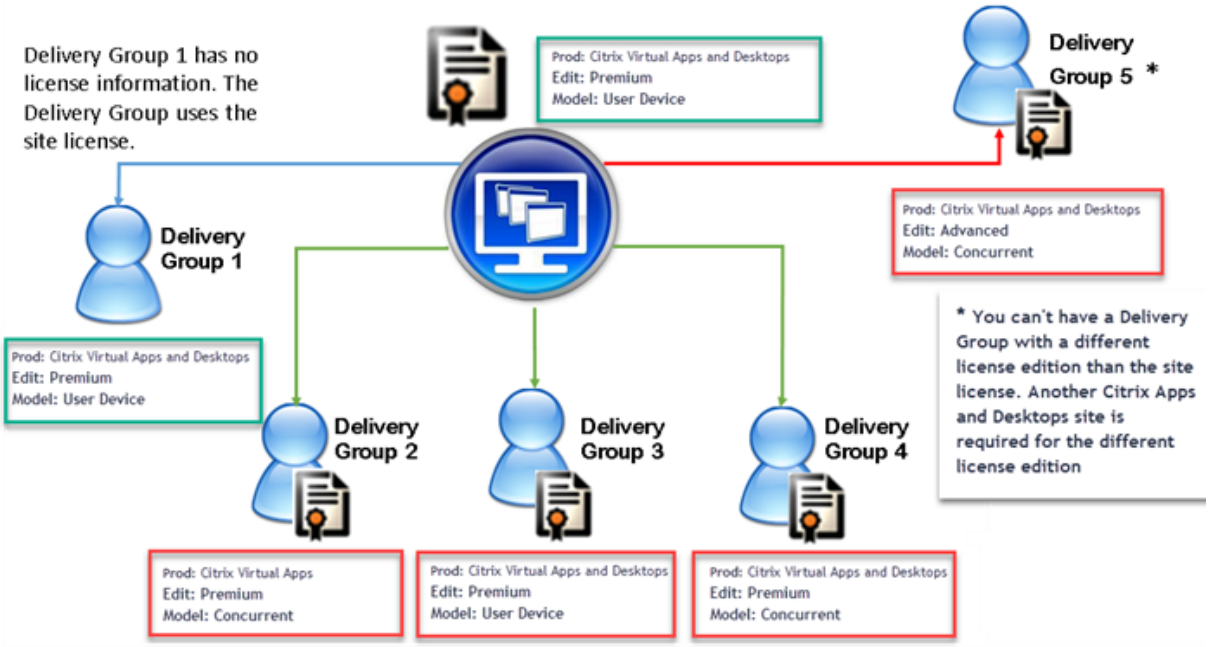
- Consulte Assinatura local da Citrix para licenças de varejo anuais e temporárias.
- Consulte Transition and Trade-Up (TTU) com Hybrid Rights.

Licenciamento multitipos

June 28, 2023

O licenciamento multitipo dá suporte ao consumo de diferentes tipos de licença para grupos de entrega em um único site de Citrix Virtual Apps and Desktops. **Tipo** é uma combinação única de ID do produto (XDT ou MPS) e Modelo (UserDevice ou Concurrent). Os grupos de entrega devem usar a mesma Product Edition (PLT/Premium ou ENT/Advanced) conforme configurado no nível do site. Esteja ciente das considerações especiais do final deste artigo ao procurar configurar o licenciamento de vários tipos para suas implantações do Citrix Virtual Apps and Desktops.

Se o licenciamento de vários tipos não estiver configurado, tipos de licença diferentes só poderão ser usados quando configurados para sites separados. Os grupos de entrega usam a licença do site. Para limitações importantes de notificação quando o licenciamento de vários tipos estiver configurado, consulte Considerações especiais.



Para determinar os grupos de entrega que consomem os diferentes tipos de licenças, use estes cmdlets do Broker PowerShell:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Para instalar licenças, use:

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

As datas dos Customer Success Services são específicas para cada arquivo de licença e para cada produto e modelo. Grupos de entrega definidos de forma diferente podem ter datas de Customer Success Services diferentes entre si.

Considerações especiais

O licenciamento multitipo tem funcionalidades diferentes 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 diferente da configuração do site:

- Nenhuma informação ao se aproximar dos limites de licença ou do gatilho ou expiração do período de carência suplementar.

- Nenhuma notificação quando um grupo específico tiver um problema.

Os grupos de entrega configurados para licenças de vários tipos consomem SOMENTE esse tipo de licença e não voltam para a 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 multitipo 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 dos recursos associados. As quatro colunas de compatibilidade especificam quais combinações de modelo de produto e licença são compatíveis para licenciamento de vários tipos. CCU e CCS representam licenças simultâneas e UD são licenças de usuário/dispositivo.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_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

Broker PowerShell SDK

O objeto **DesktopGroup** tem essas duas propriedades que você pode manipular usando os cmdlets New-BrokerDesktopGroup e Set-BrokerDesktopGroup associados.

Nome	Valor	Restrição
LicenseModel	Um parâmetro (Concurrent ou UserDevice) que especifica o modelo de licenciamento para o grupo. Se nenhum for especificado, o modelo de licença de todo o site será usado.	Se a alternância de recurso estiver desativada, a tentativa de definir uma propriedade falhará.
ProductCode	Uma string de texto de XDT (para Citrix Virtual Desktops) ou MPS (para Citrix Virtual Apps) que especifica o ID do produto de licenciamento para o grupo. Se nenhum for especificado, o código do produto em todo o site será usado.	Se a alternância de recurso estiver desativada, a tentativa de definir uma propriedade falhará.

Para obter mais informações sobre o LicenseModel e ProductCode, consulte about_Broker_Licensing.

New-BrokerDesktopGroup

Cria um grupo de área de trabalho para gerenciar a intermediação de grupos de desktops. Para obter mais informações sobre esse cmdlet, consulte https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

Set-BrokerDesktopGroup

Desativa ou ativa um grupo de desktop corretor existente ou altera suas configurações. Para obter mais informações sobre esse cmdlet, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

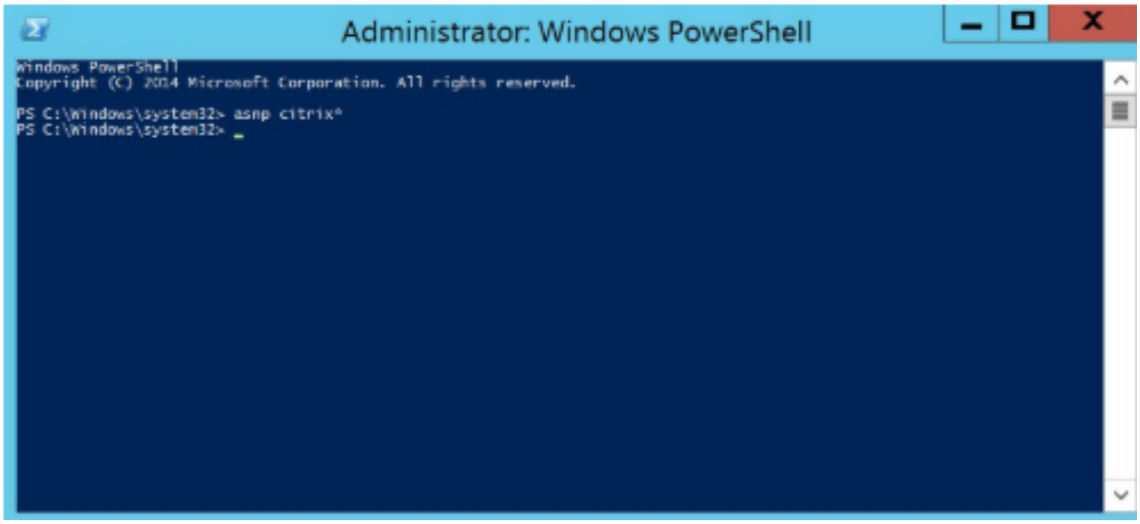
Get-BrokerDesktopGroup

Recupera grupos de desktop 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 por meio de New-BrokerDesktopGroup ou Set-BrokerDesktopGroup, serão fornecidos valores nulos. Se nulo, serão usados o modelo de licença

em todo o site e o código do produto. Para obter mais informações sobre esse cmdlet, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

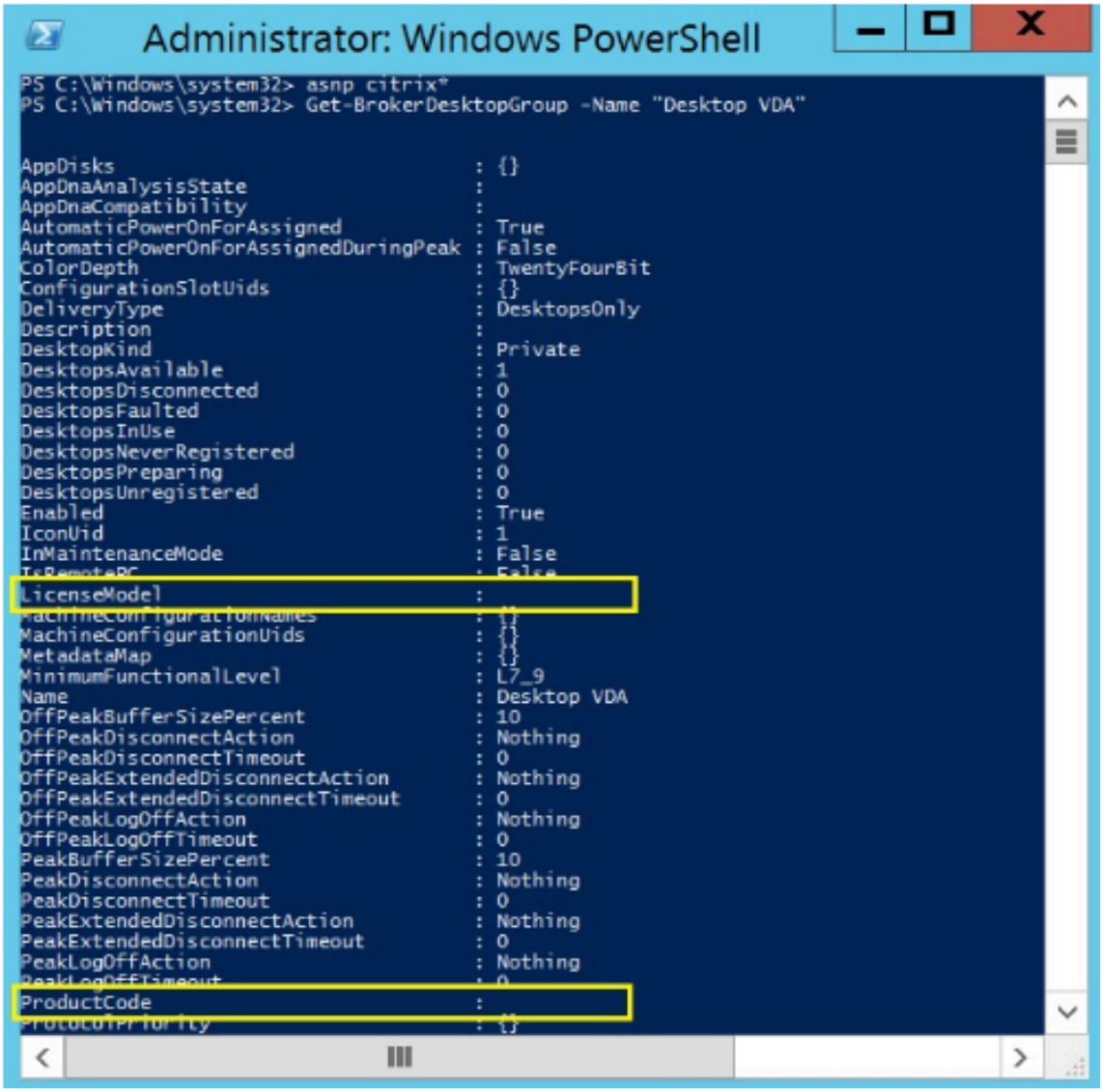
Configurar diferentes produtos e modelos de licença por grupo de entrega

1. Abra o PowerShell com direitos administrativos e adicione o snap-in da Citrix.

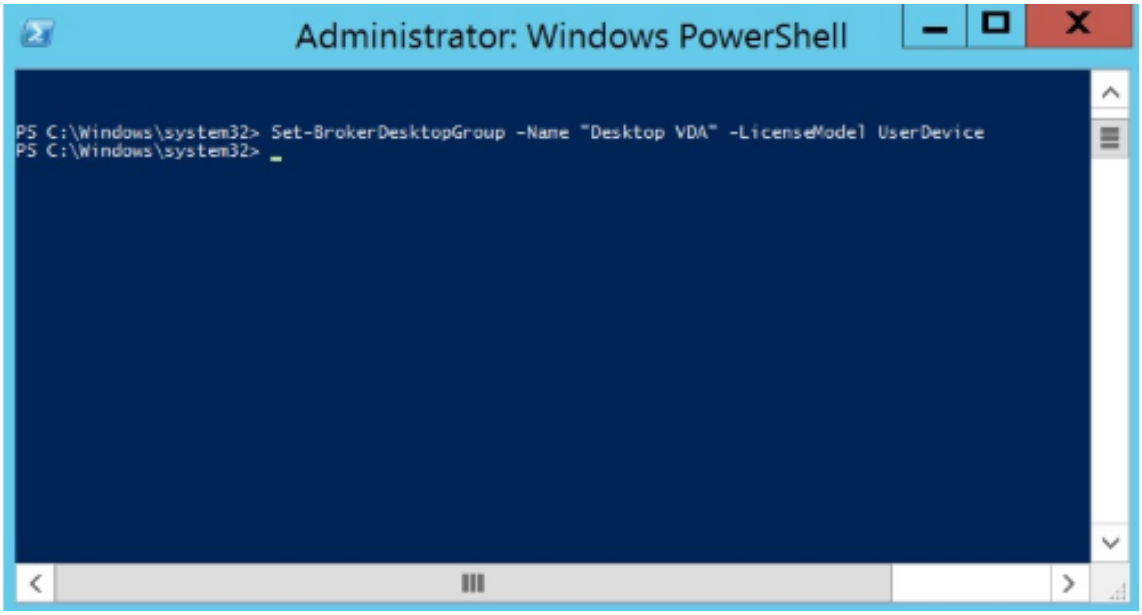


2. Execute o comando **Get-BrokerDesktopGroup** —**Name "DeliveryGroupName"** para exibir a configuração de licença atual. Encontre os parâmetros **LicenseModel** e **ProductCode**. Se você não configurou esses parâmetros antes, eles podem estar em branco.

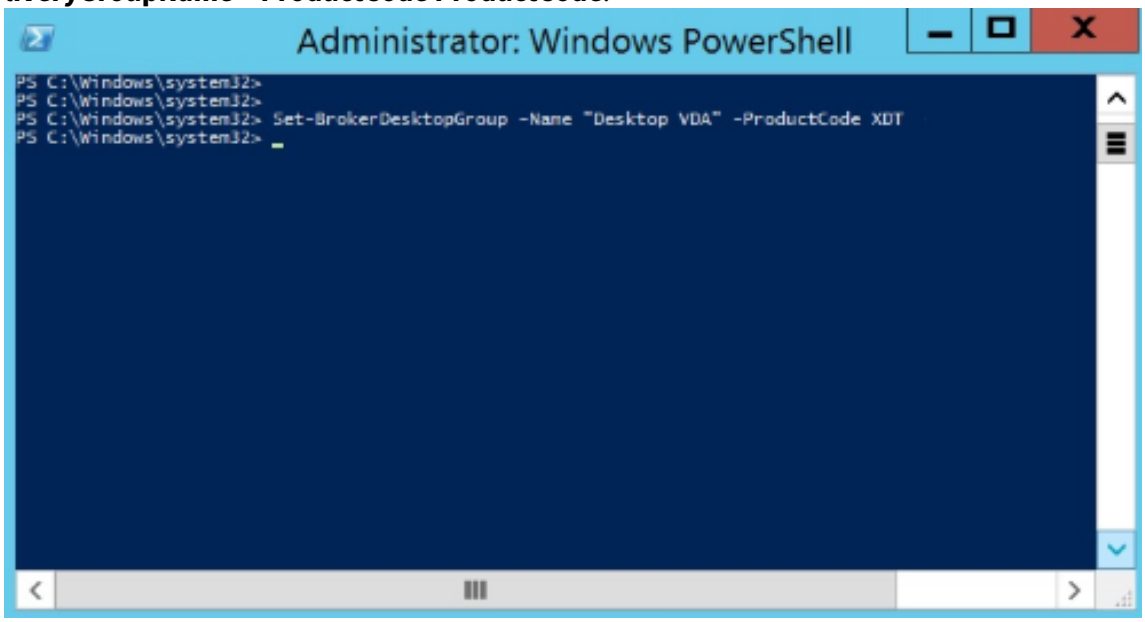
> **Nota:**
>
> Se um grupo de entrega não tiver informações de licença definidas, ele assumirá como padrão **Licença de site no nível do site**.



3. Altere o modelo de licença executando o comando: **Set-BrokerDesktopGroup —Name "DeliveryGroupName"—LicenseModel LicenseModel**.

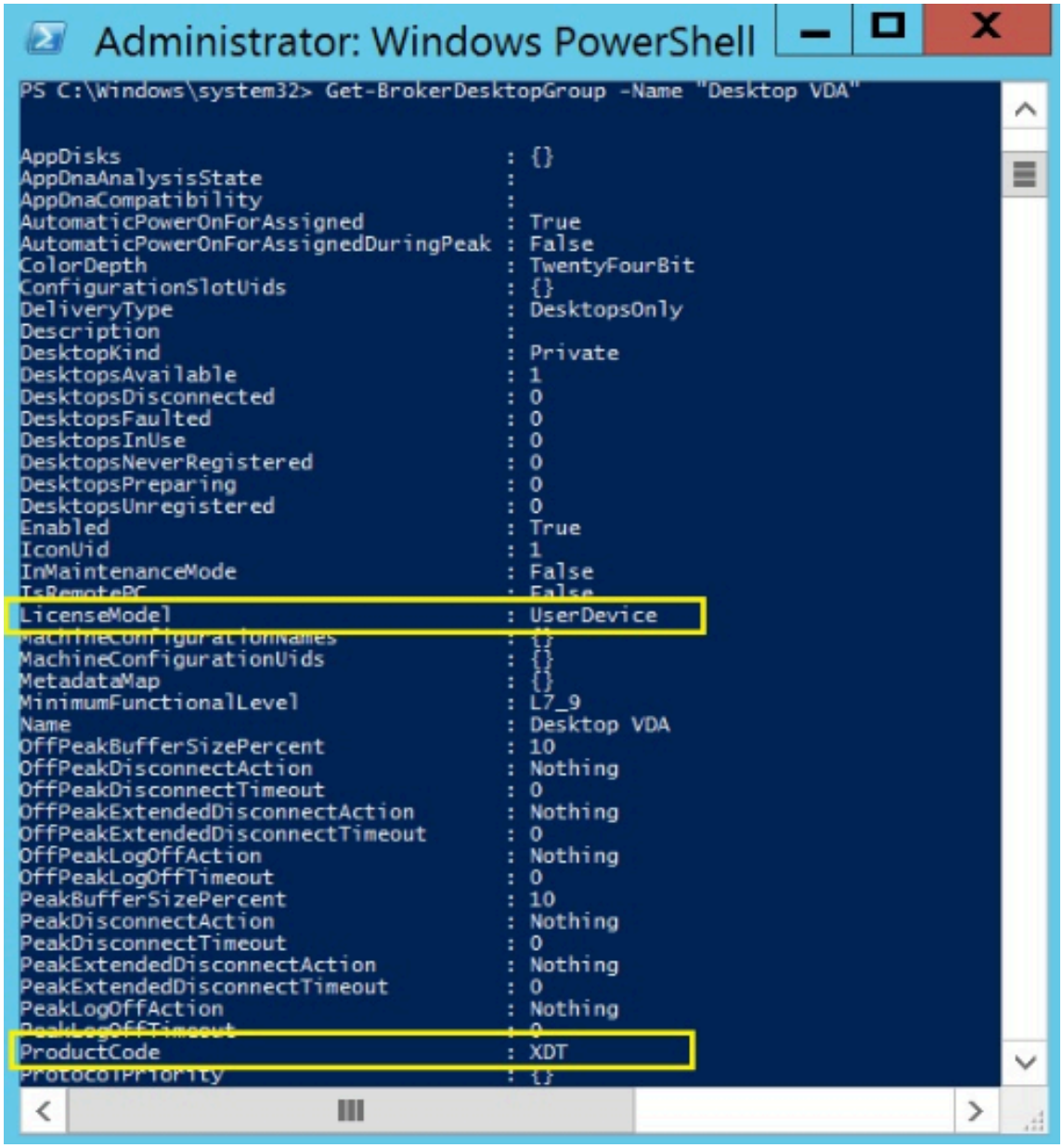


4. Altere o produto de licença executando o comando: **Set-BrokerDesktopGroup –Name “DeliveryGroupName”–ProductCode ProductCode**.



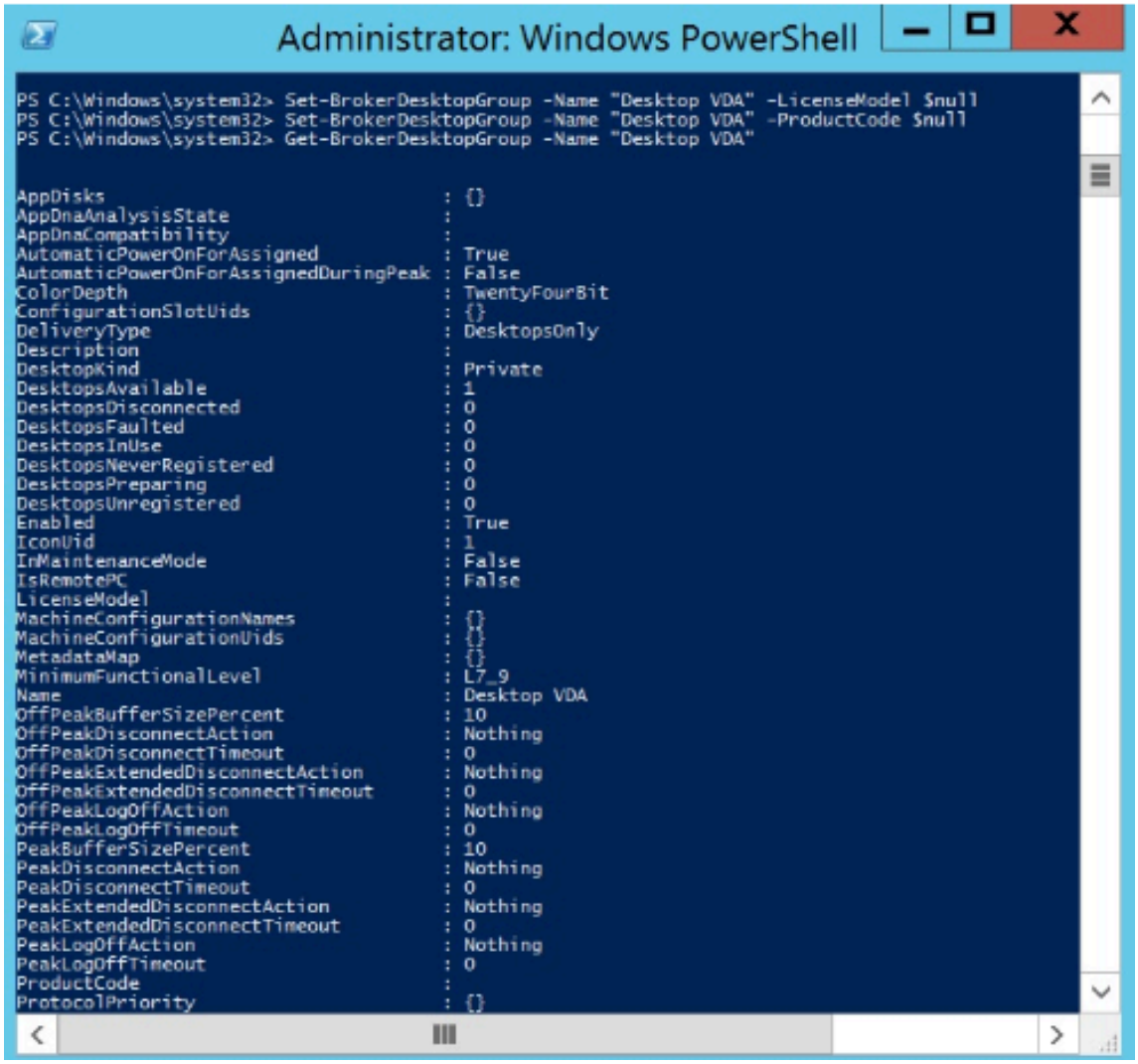
5. Digite o comando **Get-BrokerDesktopGroup —Name “DeliveryGroupName”** para validar as alterações.

> **Nota:**
>
> Você não pode misturar e combinar edições no mesmo site. Por exemplo, licenças Premium e Advanced. Vários sites são necessários se você tiver licenças de edições diferentes.



6. Remova a configuração da licença executando os mesmos comandos **Set-BrokerDesktopGroup** conforme descrito nas etapas anteriores, e defina o valor como **$null**.

> **Nota:**
>
> O Studio não exibe a configuração de licença para cada grupo de entrega. Use o PowerShell para visualizar a configuração atual.



Exemplo

Este exemplo de cmdlet do PowerShell ilustra a configuração do licenciamento de vários tipos para dois grupos de entrega existentes e cria e define 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 do PowerShell **Get-BrokerDesktopGroup**.

1. Definimos o primeiro grupo de entrega para XenApp e Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Apps Premium Concurrent”-ProductCode MPS -LicenseModel Concurrent

2. Definimos o segundo grupo de entrega para XenDesktop e Concurrent.

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”-ProductCode XDT -LicenseModel Concurrent

3. Criamos e definimos o terceiro grupo de entrega para XenDesktop e UserDevice.

   New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Perguntas frequentes sobre licenciamento

June 28, 2023

> **Nota:**
>
> - Para recursos de continuidade de negócios relacionados à pandemia do COVID-19, consulte CTX27055.
> - Para obter 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 à licença em um e-mail. Existem três maneiras de gerar arquivos de licença usando o código de acesso à licença:

- **Manage Licenses** na página MyAccount em `citrix.com`. Para obter mais informações, consulte Gerenciar licenças no citrix.com.
- Web Studio para alocar sua compra e o arquivo de licença é instalado automaticamente em seu Citrix License Server.
- Citrix Licensing Manager dentro do Citrix License Server para alocar sua compra e instalar o arquivo de licença. Para obter mais informações, consulte Instalar licenças.

Como alocar licença em myaccount?

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 Web Service for Licensing é 8083

O que é o Citrix License Server?

O Citrix License Server é um sistema que permite que as licenças sejam compartilhadas em toda a rede. Para obter mais informações, consulte Visão geral das operações de licenciamento.

Posso virtualizar ou agrupar o Citrix License Server?

Sim. Você pode virtualizar ou agrupar em cluster o Citrix License Server. Para obter mais informações, consulte Servidores de licenças em cluster.

Quais benefícios estão disponíveis para mim se eu virtualizar o Citrix License Server?

A virtualização do Citrix License Server fornece uma solução redundante. Essa solução permite a mobilidade entre vários servidores físicos sem a necessidade de tempo de inatividade.

Há alguma limitação a considerar se eu virtualizar o Citrix License Server?

Não.

O Citrix License Server gerencia todas as licenças para minha implantação do Citrix Virtual Apps and Desktops?

O Citrix License Server gerencia todas as licenças que você recebe para o Citrix Virtual Apps and Desktops, exceto licenças na Premium Edition usadas com o Citrix Gateway. Os servidores de licença se incorporam aos dispositivos de rede conforme necessário para esses dispositivos de rede orientados à segurança gerenciem essas licenças.

O que é o Citrix Licensing Manager?

O Citrix Licensing Manager permite o download e a alocação de arquivos de licença do Servidor de licenças no qual você instalou o Citrix Licensing Manager. O Citrix Licensing Manager é o método de gerenciamento recomendado do License Server, que permite o seguinte:

- Registro de código curto do Servidor de Licenças para o Citrix Cloud e fácil remoção do registro.
- Configure contas de usuário e grupo.
- Use o painel para exibir licenças instaladas, em uso, expiradas e disponíveis e datas dos Customer Success Services.
- Exportar dados de uso da licença para uso em relatórios.
- Configure o período de retenção de dados de uso histórico. O período padrão de retenção de dados é de 180 dias.
- Instalação simplificada de arquivos de licença no Servidor de Licenças usando um código de acesso à licença ou arquivo baixado.
- Ative e desative o período de carência suplementar.
- Configurar o programa de melhoria da experiência do cliente (CEIP) e o Call Home.
- Verifica automaticamente ou manualmente se há licenças de renovação do Customer Success Services e notifica você ou instala as licenças, se encontradas.
- Notifica você sobre o estado do Servidor de Licenças - Licença de inicialização ausente, problemas de tempo, falhas do carregador.
- Modificar estas portas:
  - Servidor de licenças (padrão 27000)
  - Daemon do fornecedor (padrão 7279)
  - Serviços da Web para licenciamento (padrão 8083)

Para obter mais informações, consulte Citrix Licensing Manager.

Onde está o Citrix License Administration Console?

O License Administration Console não tem mais suporte e foi removido do Servidor de Licenças 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 Servidor de Licenças 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 da licença?

O período de atribuição de licença é o termo em que uma licença do Citrix Virtual Apps and Desktops é atribuída a um usuário ou dispositivo. O período de atribuição de licença padrão é de 90 dias.

Como posso saber quantas licenças minha organização comprou?

Todas as licenças compradas estão disponíveis para revisão e acesso a qualquer momento (24x7) na sua caixa de ferramentas **Manage Licenses** segura na página **My Account** em https://www.citrix.c

om.

Como posso saber quantas licenças estão em uso em um determinado momento?

O Citrix Licensing Manager e o Studio fornecem detalhes sobre o uso de licenças em tempo real.

Recuperação e manutenção de desastres do servidor

Para obter informações sobre recuperação de desastres e manutenção do seu License Server, consulte Recuperação de desastres e manutenção na documentação do Citrix Licensing.

Licenciamento do Citrix Virtual Apps and Desktops

Como o Citrix Virtual Apps and Desktops é licenciado?

O licenciamento Citrix Virtual Apps and Desktops oferece modelos de licença de usuário/dispositivo e simultâneos.

Usuário/dispositivo:

O modelo flexível de usuário/dispositivo se alinha com:

- Uso de desktop em toda a empresa.
- Licenciamento de virtualização de desktop da Microsoft subjacente.
- Licenciamento simultâneo para clientes com usuários que precisam apenas de acesso ocasional a seus desktops e aplicativos virtuais.

O licenciamento de usuário/dispositivo dá aos usuários acesso a suas áreas de trabalho e aplicativos virtuais a partir de um número ilimitado de dispositivos. As licenças de dispositivo oferecem um número ilimitado de acessos do usuário às áreas de trabalho e aplicativos virtuais a partir de um único dispositivo. Essa abordagem oferece flexibilidade máxima e melhora o alinhamento com o licenciamento de virtualização de área de trabalho da Microsoft.

> **Importante:**
>
> Você não pode alocar licenças manualmente para um usuário ou dispositivo. O Servidor de Licenças ou o serviço em nuvem atribui licenças. Com o licenciamento de usuário/dispositivo, uma vez que uma licença é atribuída, ela não poderá ser atribuída a outro usuário antes de decorridos 90 dias de inatividade.

Simultâneas:

As licenças simultâneas permitem uma conexão com um número ilimitado de aplicativos e desktops virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida somente durante uma sessão ativa. Se a sessão se desconectar ou for encerrada, a licença será reinserida no pool.

Para obter mais informações sobre licenciamento de usuário/dispositivo, consulte Licença de usuário/dispositivo e licenças simultâneas, consulte Licença simultânea.

É possível experimentar o Citrix Virtual Apps and Desktops antes de comprar licenças?

Sim. Você pode baixar o software Citrix Virtual Apps and Desktops e executá-lo no modo de avaliação. O modo de avaliação permite que você use o Citrix Virtual Apps and Desktops no local por 30 dias, para 10 conexões, sem licença. Para obter mais informações, consulte Licenças de avaliação.

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) para Citrix Cloud está disponível para serviço de avaliação com base na aprovação. Verifique com seu representante Citrix para obter mais detalhes.

Como a Citrix define a simultaneidade para Citrix Virtual Apps and Desktops?

O modelo simultâneo Citrix Virtual Apps and Desktops permite uma conexão com um número ilimitado de aplicativos e áreas de trabalho virtuais para qualquer usuário e qualquer dispositivo. Uma licença é consumida somente durante uma sessão ativa. Se a sessão se desconectar ou for encerrada, a licença será reinserida no pool para reemissão. Para obter mais informações, consulte Licença simultânea.

Posso implantar várias edições das licenças Citrix Virtual Apps and Desktops em um Servidor de Licenças comum?

Sim. O Servidor de Licenças gerencia licenças para Citrix Virtual Apps and Desktops simultaneamente. Recomendamos que você instale a versão mais recente do Servidor de Licenças. Se você não tiver certeza se a versão do Servidor de Licenças está atual, verifique-a comparando sua versão com o número no site de downloads da Citrix.

Um único site pode usar as licenças Citrix Virtual Apps e Citrix Virtual Apps and Desktops?

Dependendo da versão, um único site Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode oferecer suporte a ambos os modelos de licenciamento - usuário/dispositivo ou simultâneo. Um único site Citrix Virtual Apps ou Citrix Virtual Apps and Desktops pode dar suporte a apenas uma edição. Para obter mais informações, consulte Licenciamento multitipos.

As versões mínimas que suportam o licenciamento de vários tipos são XenApp e XenDesktop 7.15 Long Term Service Release (LTSR) e Citrix Virtual Apps and Desktops 7 1808.

Posso selecionar Citrix Virtual Apps simultâneo como modelo de produto se eu tiver licenças simultâneas do Citrix Virtual Apps and Desktops ou do Citrix Virtual Apps and Desktops instaladas no Servidor de licenças?

Se você usar o Citrix Virtual Apps como um recurso do Citrix Virtual Apps and Desktops Advanced ou Premium Edition, seu modelo de licença do Citrix Virtual Apps será o mesmo que a Advanced ou Premium Edition do Citrix Virtual Apps and Desktops. Se você comprou o Citrix Virtual Apps and Desktops, configure seu licenciamento como Citrix Virtual Apps and Desktops, mesmo que você planeje usar somente a funcionalidade Citrix Virtual Apps. Selecione Citrix Virtual Apps como modelo de produto somente se você tiver licenças autônomas simultâneas do Citrix Virtual Apps instaladas no Servidor de licenças.

Quais componentes do produto estão incluídos em cada edição Citrix Virtual Apps e Citrix Virtual Apps and Desktops?

Para obter uma matriz de recursos completa por edição, consulte Recursos do Citrix Virtual Apps and Desktops.

Como licencio ambientes Citrix Virtual Desktops em conformidade com a EULA do Citrix Virtual Apps and Desktops?

Para implantar o Citrix Virtual Apps and Desktops sob o usuário/dispositivo ou o modelo de licença simultâneo em conformidade com a EULA do Citrix Virtual Apps and Desktops, aplique os arquivos de licença ao seu Servidor de licenças. O servidor de licenças então controla e monitora a conformidade com as licenças. Recomendamos que você configure seu produto com base no que você comprou. Por exemplo, se você comprar 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 Product License Compliance Center.

Como licencio os ambientes Citrix Virtual Apps em conformidade com a EULA do Citrix Virtual Apps?

Para implantar o Citrix Virtual Apps sob o modelo de licença simultâneo em conformidade com a EULA do Citrix Virtual Apps, aplique os arquivos de licença ao seu Servidor de licenças. O servidor de licenças então controla e monitora a conformidade com as licenças.

Existe um requisito de licenciamento para as opções de serviço do Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) or 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 da LTSR. Para obter mais informações, consulte Citrix Virtual Apps and Desktops e opções de serviço do Citrix Hypervisor

Como funcionam as horas em pool do Serviço Remote Browser Isolation (RBI)?

Quando você compra um mínimo de 25 usuários do serviço, você recebe 5000 horas de direitos para usar o serviço, agrupados para todos os usuários. As compras subsequentes de direitos de usuário não aumentam o direito de horas agrupadas. Para aumentar o direito das horas de serviço, compre pacotes complementares.

Posso usar o Remote PC Access com licenças CCU?

Sim.

Para obter informações sobre o acesso remoto ao PC, consulte Acesso remoto ao PC.

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 um único usuário conexões ilimitadas de dispositivos ilimitados. Se um usuário se conectar a uma área de trabalho ou dispositivo, o usuário precisará de uma licença atribuída a esse usuário para acessar uma área de trabalho ou aplicativo virtual. O servidor de licenças ou o serviço em nuvem atribui a licença. Você não pode atribuir essas licenças manualmente. A licença é atribuída ao usuário, não ao dispositivo compartilhado. Depois que uma licença é atribuída, ela não poderá ser atribuída a outro usuário até após 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. Sob o 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 oferecer suporte a vários usuários que compartilham o dispositivo. Por exemplo, um dispositivo compartilhado pode ser uma estação de trabalho em sala de aula ou uma estação de trabalho clínica em um hospital.

Posso converter minhas licenças simultâneas 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 Citrix Virtual Desktops Standard Edition e quiser o modelo de licença de usuário/dispositivo, atualize para Citrix Virtual Apps and Desktops Advanced ou Premium Edition.

De	Para padrão simultâneo	Para usuário/dispositivo padrão	Para usuário/dispositivo avançado	Para usuário/dispositivo premium
Licenças simultâneas do Citrix Virtual Desktops Standard Edition	N/A	Conversão simultânea para usuário/dispositivo NÃO permitida	Você não pode converter modelos de licença, mas pode atualizar para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.	Você não pode converter modelos de licença, mas pode atualizar para o Citrix Virtual Apps and Desktops Advanced ou Premium Edition.
Licenças de usuário/dispositivo Citrix Virtual Desktops Standard Edition	Conversão de usuário/dispositivo para simultâneo NÃO é permitida	N/A	N/A	N/A

Em que o licenciamento simultâneo funciona de forma diferente do licenciamento de usuário/dispositivo?

Baseamos o licenciamento simultâneo em conexões de dispositivos simultâneos. Uma licença simultânea está em uso somente quando um dispositivo tiver estabelecido uma conexão ativa. Quando

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 a locação expire.

Sob o 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 Servidor de Licenças atribui licenças otimamente a usuários ou dispositivos com base no uso. Você não pode atribuir essas licenças manualmente.

Como eu 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 ilimitados e aplicativos virtuais a partir de um número ilimitado de dispositivos. O licenciamento simultâneo permite acesso ilimitado a desktops virtuais ilimitados e aplicativos virtuais 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.
<!--NeedCopy-->
```

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 off-line.

No modelo de usuário/dispositivo, qual é o número máximo de usuários que podem acessar um dispositivo licenciado?

Cada dispositivo licenciado pode atender a um número ilimitado de usuários dentro de uma organização.

Sob o modelo de usuário/dispositivo, qual é o número máximo de áreas de trabalho virtuais ou aplicativos web do RBI que um usuário licenciado pode consumir em um determinado momento?

Cada usuário licenciado pode se conectar a um número ilimitado de desktops virtuais ou aplicativos da Web.

Posso comprar licenças Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados no meu ambiente Citrix Virtual Apps and Desktops atual?

Sim. Você pode comprar licenças Citrix Virtual Apps and Desktops para aumentar o número de usuários/dispositivos licenciados em seu ambiente Citrix Virtual Apps and Desktops existente.

Como libero uma licença autorizada de usuário/dispositivo?

Para liberar a atribuição de um usuário/dispositivo autorizado, use o utilitário `udadmin` de acordo com os termos da EULA. Em seguida, o servidor de licenças 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 comprada?

As licenças de usuário/dispositivo incluem um crédito a descoberto de 10%, que é incluído quando as licenças são geradas. O crédito a descoberto também está incluído na contagem de licenças instalada. Se o pico de uso exceder a contagem instalada, incluindo o crédito a descoberto, o acesso para mais usuários será negado. Compre e implante uma nova licença para permitir o acesso para mais usuários.

Se todas as licenças estiverem em uso, incluindo a licença a descoberto, o período de carência suplementar permitirá conexões ilimitadas com um produto. O período de carência suplementar lhe dá tempo para determinar por que você excedeu a contagem máxima de licenças e comprar mais licenças sem causar transtornos aos seus usuários. Esse período dura até 15 dias decorrentes ou você instala mais licenças de varejo, o que ocorrer primeiro. Para obter mais informações, consulte Período de carência adicional.

O Director exibe os estados do período de carência. Para obter mais informações, consulte Panels on the 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 deixa sua organização, você pode liberar a licença desse usuário sem notificar a Citrix. Use o utilitário `udadmin` para liberar a licença. Se você não liberar a licença, o servidor de licenças liberará automaticamente qualquer licença após 90 dias de inatividade. Essas informações estão sujeitas 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 poderá liberar a licença sem notificar a Citrix, para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

O que acontece se substituirmos um dispositivo licenciado na minha organização?

Se você substituir um dispositivo licenciado existente, poderá liberar a licença sem notificar a Citrix para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar a licença.

O que acontece se um dispositivo licenciado estiver fora de serviço por um período prolongado?

Quando um dispositivo licenciado existente está fora de serviço por um período prolongado, você poderá liberar a licença sem notificar a Citrix para que ela fique disponível para reatribuição. Use o utilitário `udadmin` para liberar as licenças. Se você não liberar a licença, o servidor de licenças liberará automaticamente qualquer licença após 90 dias de inatividade. Essas informações estão sujeitas aos termos especificados no EULA.

Posso alternar licenças de usuário para licenças de dispositivo depois de atribuir as licenças a um dispositivo ou usuário?

Sim. Essa alteração acontece automaticamente. O Servidor de Licenças atribui licenças a usuários ou dispositivos com base em padrões de uso. Se os padrões de uso mudarem, o Servidor de Licenças poderá alternar a atribuição com base no novo uso. O Servidor de Licenças sempre atribui licenças

da maneira mais econômica para o cliente. Além disso, o Servidor de Licenças monitora 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

Sob o 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 muitos usuários e permite conexões ilimitadas.

Posso implantar licenças simultâneas de uma versão anterior do Citrix Virtual Apps and Desktops e novas licenças de usuário/dispositivo ou simultâneas em um único Servidor de Licenças?

Sim. Você pode continuar usando o mesmo Servidor de Licenças para oferecer suporte a implantações licenciadas de 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 usando o mesmo Servidor de Licenças para oferecer suporte a implantações licenciadas simultâneas e usuário/dispositivo ou simultâneas.

As edições Citrix Virtual Apps and Desktops Advanced e Premium incluem licenças simultâneas Citrix Virtual Apps?

As licenças de usuário/dispositivo Citrix Virtual Apps and Desktops Advanced e Premium incluem licenças simultâneas Citrix Virtual Apps apenas para compatibilidade. Essas licenças simultâneas são para uso somente com versões anteriores de produtos incompatíveis com licenças de usuário/dispositivo. O uso das licenças de compatibilidade simultâneas incluídas com licenças de usuário/dispositivo só é permitido com essas versões - versões do XenApp anteriores a 6.5 e versões do XenDesktop anteriores à 5.0 Service Pack 1.

O que acontece se eu exceder minha contagem de licenças simultâneas compradas?

Se todas as licenças estiverem em uso, o período de carência suplementar permite conexões ilimitadas com um produto. O período de carência suplementar lhe dá tempo para determinar por que

você excedeu a contagem máxima de licenças e comprar mais licenças sem causar transtornos aos seus usuários. Esse período dura até 15 dias decorrentes ou você instala mais licenças de varejo, o que ocorrer primeiro. Para obter mais informações, consulte Período de carência adicional.

O Director exibe os estados do período de carência. Para obter mais informações, consulte Panels on the Director Dashboard.

Licenças a descoberto

Como obtenho licenças a descoberto?

Os produtos (excluindo o Citrix Cloud) que dão suporte a modelos de licença de usuário/dispositivo, usuário ou dispositivo incluem um recurso de licença a descoberto que permite usar um número limitado de licenças extras para impedir a negação de acesso. Oferecemos qualquer recurso de crédito a descoberto como conveniência, não como direito à licença. As licenças simultâneas e de servidor não contêm crédito a descoberto. Todas as licenças a descoberto usadas devem ser compradas dentro de 30 dias após o primeiro uso, mas o uso não está limitado a 30 dias. A Citrix se reserva o direito de remover qualquer recurso de crédito a descoberto em lançamentos de novos produtos. Para obter mais informações, consulte Licença a descoberto.

Como posso identificar um crédito a descoberto de licenças?

Você pode visualizar informações de uso, incluindo o número de licenças no crédito a descoberto no Citrix Licensing Manager. O Studio também contém informações de uso de crédito a descoberto.

O que acontece quando uma licença de crédito a descoberto é consumida?

Uma licença é atribuída a partir de suas licenças instaladas para permitir o acesso ao ambiente Citrix Virtual Apps and Desktops. Essa licença de crédito a descoberto fornece tanto acesso e funcionalidade quanto suas outras licenças.

Posso receber um alerta quando minhas licenças de crédito a descoberto forem consumidas?

Atualmente, não há alertas específicos fornecidos quando as licenças de crédito a descoberto são consumidas.

Por quanto tempo uma licença de crédito a descoberto pode ser consumida?

Compre todas as licenças de crédito a descoberto usadas dentro de 30 dias após o primeiro uso.

Outras informações de licenciamento específicas do produto

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- Citrix Hypervisor
- Citrix Licensing

Cache do host local

June 28, 2023

Para garantir que o banco de dados do site do Citrix Virtual Apps and Desktops esteja sempre disponível, a Citrix recomenda começar com uma implantação do SQL Server tolerante a falhas, seguindo as práticas recomendadas de alta disponibilidade da Microsoft. (Para recursos de alta disponibilidade do SQL Server compatíveis, consulte Bancos de dados.) No entanto, problemas de rede e interrupções podem resultar em usuários que não conseguem se conectar a seus aplicativos ou áreas de trabalho.

O recurso de Cache de host local permite que as operações de troca de conexão em um site continuem quando ocorre uma interrupção. Uma interrupção ocorre quando a conexão entre um Delivery Controller e o banco de dados do site falha em um ambiente Citrix local. O Cache de host local é ativado quando o banco de dados do site fica inacessível por 90 segundos.

A partir do XenApp e XenDesktop 7.16, o recurso de concessão de conexão (um recurso de alta disponibilidade predecessor em versões anteriores) foi removido do produto e não está mais disponível.

Conteúdo de dados

O Cache de host local inclui as seguintes informações, que são um subconjunto das informações no banco de dados principal:

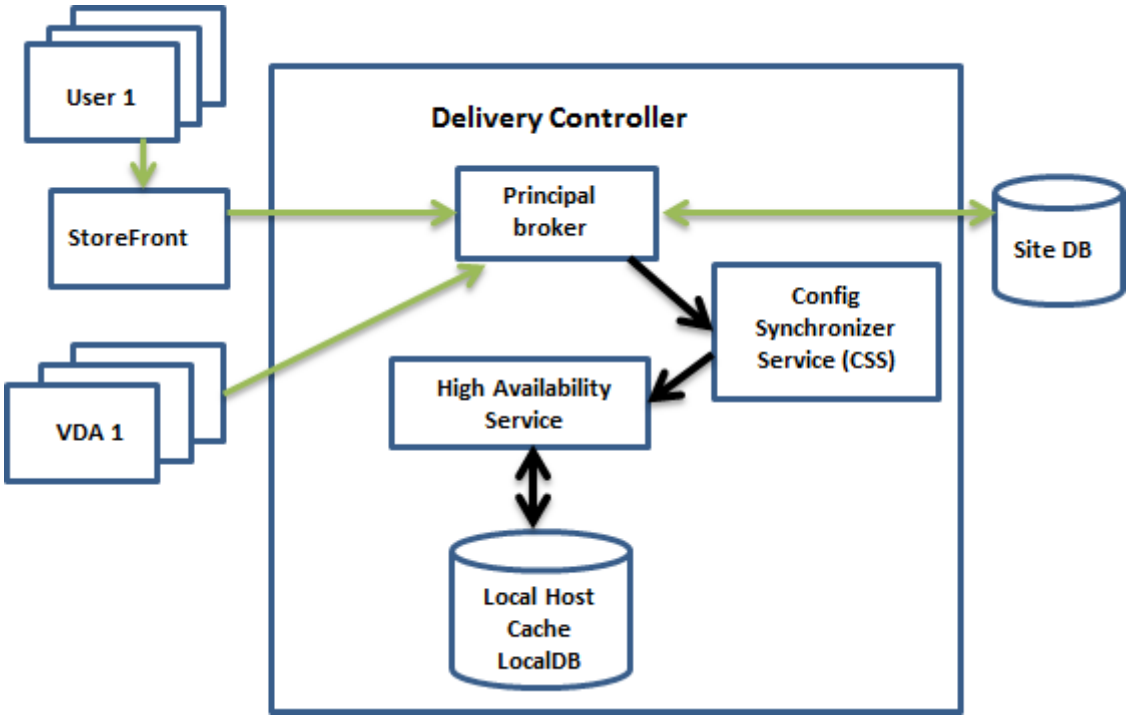
- Identidades de usuários e grupos que têm direitos aos recursos publicados no site.
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados no site.
- Identidades de máquinas VDA (incluindo máquinas Remote PC Access) configuradas no site.
- Identidades (nomes e endereços IP) de máquinas cliente Citrix Receiver que estão sendo usadas ativamente para a conexão a recursos publicados.

Ele também contém informações para conexões atualmente ativas que foram estabelecidas enquanto o banco de dados principal estava indisponível:

- Resultados análises de ponto de extremidade de máquina cliente realizadas pelo Citrix Receiver.
- Identidades de máquinas de infraestrutura (como servidores NetScaler Gateway e StoreFront) envolvidas em operações do site.
- Data, hora e tipo das atividades recentes dos usuários.

Como funciona

O gráfico a seguir ilustra os componentes do Cache de host local e os caminhos de comunicação durante as operações normais.



Durante as operações normais

- O *agente principal* (Citrix Broker Service) em um Controller aceita solicitações de conexão do StoreFront. O agente se comunica com o banco de dados do site para conectar usuários com VDAs que estão registrados no Controller.
- O Citrix Config Synchronizer Service (CSS) consulta o agente a cada minuto, aproximadamente, para ver se foi feita alguma alteração. As alterações podem ser iniciadas pelo administrador (como alterar uma propriedade de grupo de entrega) ou podem ser ações do sistema (como atribuições de máquina).

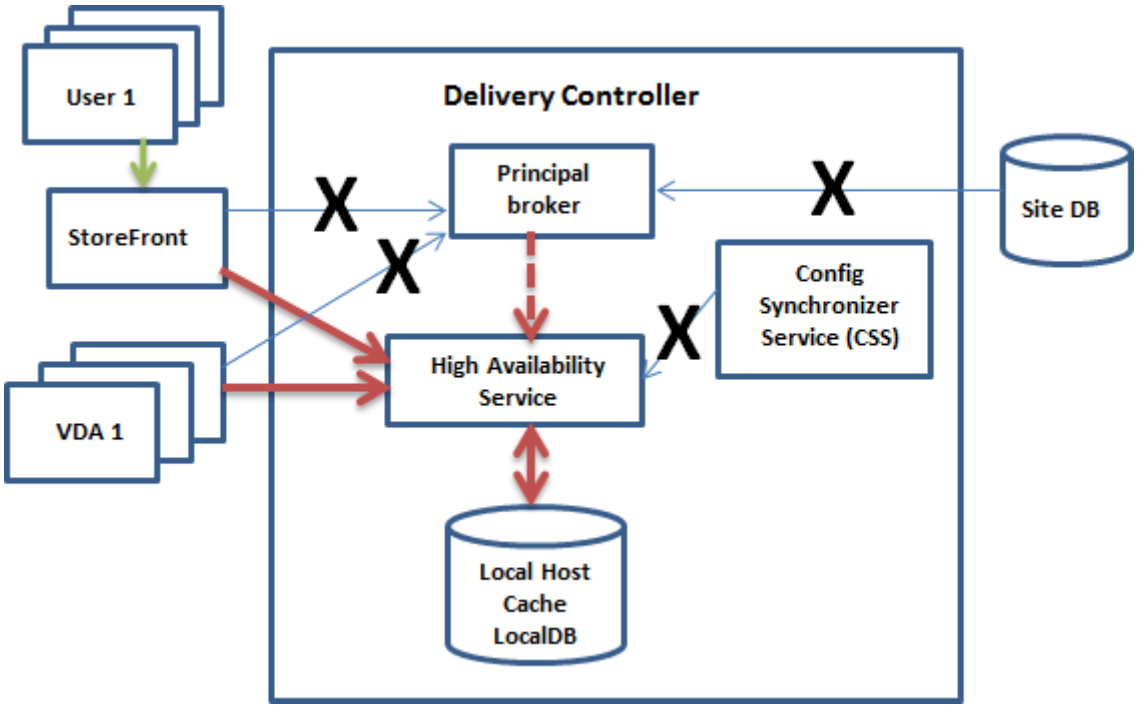
- Se uma alteração de configuração tiver ocorrido desde a verificação anterior, o CSS sincroniza (copia) as informações com um agente secundário no Controller. (O agente secundário também é conhecido como serviço de alta disponibilidade.)

  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 do Microsoft SQL Server Express LocalDB no Controller. Esse banco de dados é referido como o banco de dados do cache de host local. O CSS garante que as informações no banco de dados do cache de host local correspondam às informações no banco de dados do site. O banco de dados do cache de host local é recriado toda vez que a sincronização ocorre.

  O Microsoft SQL Server Express LocalDB (usado pelo banco de dados do cache de host local) é instalado automaticamente quando você instala um Controller. (Você pode proibir essa instalação ao instalar um Controller usando a linha de comando.) O banco de dados do cache de host local não pode ser compartilhado entre os Controllers. Você não precisa fazer backup do banco de dados do cache de host local. Ele é recriado toda vez que uma alteração de configuração é detectada.

- Se nenhuma alteração tiver ocorrido desde a última verificação, nenhum dado será copiado.

O gráfico a seguir ilustra as alterações nos caminhos de comunicação se o agente principal perder o contato com o banco de dados do site (quando uma interrupção começa).



Durante uma interrupção

Quando uma interrupção começa:

- O agente secundário começa a escutar e processar as solicitações de conexão.
- Quando a interrupção começa, o agente secundário não tem dados de registro do VDA atuais, mas quando o VDA se comunica com ele, um processo de registro é disparado. Durante esse processo, o agente secundário também obtém as informações de sessão atuais sobre o VDA.
- Enquanto o agente secundário está lidando com as conexões, o Brokering Principal continua a monitorar a conexão. Quando a conexão é restaurada, o Brokering Principal instrui o agente secundário a parar de escutar informações de conexão, e o Brokering Principal retoma as operações de intermediação. A próxima vez que um VDA se comunicar com o Brokering Principal, um processo de registro é disparado. O agente secundário remove quaisquer registros de VDA restantes da interrupção anterior. O CSS retoma a sincronização de informações quando detecta que ocorreram alterações de configuração 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. Isso afeta apenas a inicialização de novas sessões.

Você também pode disparar uma interrupção intencionalmente. Consulte Forçar uma interrupção para obter detalhes sobre por que e como fazer isso.

Sites com vários Controllers

Entre suas outras tarefas, o CSS rotineiramente fornece ao agente secundário informações sobre todos os Controllers na zona. (Se a sua implantação não contiver várias zonas, essa ação afetará todos os Controllers no site.) Tendo essa informação, cada agente secundário sabe sobre todos os agentes secundários de pares em execução em outros Controllers na zona.

Os agentes secundários comunicam-se uns com os outros em um canal separado. Esses agentes usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual agente secundário intermediará as operações na zona se ocorrer uma interrupção. Durante a interrupção, todos os VDAs se registram no agente secundário eleito. Os agentes secundários não eleitos na zona rejeitam ativamente as solicitações de entrada de conexão e registro de VDA.

Se um agente secundário eleito falhar durante uma interrupção, outro agente secundário é eleito para assumir o controle, e os VDAs se registram no agente secundário recém-eleito.

Durante uma interrupção, se um Controller for reiniciado:

- Se esse Controller não for o agente eleito, a reinicialização não terá impacto.
- Se esse Controller for o agente eleito, um Controller diferente será eleito, fazendo com que os VDAs se registrem. Depois que o Controller reiniciado liga, ele assume automaticamente a intermediação, o que faz com que os VDAs se registrem novamente. Nesse cenário, o desempenho pode ser afetado durante os registros.

Se você desligar um Controller durante as operações normais e ligá-lo durante uma interrupção, o Cache de host local não pode ser usado nesse Controller se for eleito como o agente.

Os logs de eventos fornecem informações sobre as escolhas.

O que não está disponível durante uma interrupção e outras diferenças

Não há limite de tempo imposto para operar no modo de interrupção. No entanto, a Citrix recomenda restaurar a conectividade o mais rápido possível.

Durante uma interrupção:

- Você não pode usar o Studio.
- Você tem acesso limitado ao SDK do PowerShell.
  - Você deve primeiro:
    * 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*`.
    * Os cmdlets de gerenciamento de energia `New-BrokerHostingPowerAction`, `Set-BrokerHostingPowerAction` e `Remove-BrokerHostingPowerAction`.
- As credenciais do Hypervisor não podem ser obtidas do Host Service. Todas as máquinas estão em um estado de energia desconhecido e nenhuma operação de energia pode ser emitida. No entanto, as VMs no host que estão ligadas podem ser usadas para solicitações de conexão.
- Uma máquina atribuída só pode ser usada se a atribuição ocorreu durante as operações normais. Novas atribuições não podem ser feitas durante uma interrupção.

- O registro e a configuração automática de máquinas Remote PC Access não são possíveis. No entanto, as máquinas que foram registradas e configuradas durante a operação normal são utilizáveis.
- Aplicativos hospedados no servidor e usuários de área de trabalho podem usar mais sessões do que seus limites de sessão configurados, se os recursos estiverem em zonas diferentes.
- Os usuários podem iniciar aplicativos e áreas de trabalho somente a partir de VDAs registrados na zona que contém o agente secundário eleito/ativo atualmente. As inicializações entre zonas (de um agente secundário em uma zona para um VDA em uma zona diferente) não são suportadas durante uma interrupção.
- Se uma interrupção do banco de dados do site ocorrer antes de uma reinicialização programada começar para os VDAs em um grupo de entrega, as reinicializações começam quando a interrupção termina. Isso pode ter resultados inesperados. Para obter mais informações, consulte Reinicializações agendadas atrasadas devido à interrupção do banco de dados.
- A preferência de zona não pode ser configurada. Se configuradas, as preferências não serão consideradas na inicialização da sessão.
- A opção de restrições de tag está ativada, as sessões podem falhar de forma intermitente na inicialização.

Suporte a aplicativos e áreas de trabalho

O cache de host local oferece suporte a aplicativos e áreas de trabalho hospedados em servidor e a áreas de trabalho estáticas (atribuídas).

O cache de host local oferece suporte a VDAs de área de trabalho em grupos de entrega em pool, como se segue:

- Por padrão, os VDAs de áreas de trabalho com gerenciamento de energia em grupos de entrega em pool (criados pelo MCS ou Citrix Provisioning) que têm a propriedade `ShutdownDesktopsAfterUse` ativada são colocados no modo de manutenção quando ocorre uma interrupção. Você pode alterar esse padrão, para permitir que essas áreas de trabalho sejam usadas durante uma interrupção.

  No entanto, você não pode contar com o gerenciamento de energia durante a interrupção. (O gerenciamento de energia é retomado depois das operações normais serem retomadas.) Além disso, essas áreas de trabalho podem conter dados do usuário anterior, porque não foram reiniciadas.
- Para substituir o comportamento padrão, ele deve ser ativado em todo o site e em cada grupo de entrega afetado. Execute os seguintes cmdlets do PowerShell.

  Em todo o site:


```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

Para cada grupo de entrega afetado, execute o seguinte comando do PowerShell:

```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
 $true
```

Ativar esse recurso no site e nos grupos de entrega não afeta como a propriedade configurada `ShutdownDesktopsAfterUse` funciona durante as operações normais.

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 agente secundário pode usar até 1 GB de RAM se uma interrupção durar por um intervalo prolongado com muitos logons ocorrendo (por exemplo, 12 horas com 10.000 usuários). Esses requisitos de memória são além dos requisitos normais de RAM para o Controller, portanto, portanto, pode ser necessário aumentar a quantidade total da capacidade de RAM.

Se você usar uma instalação do SQL Server Express para o banco de dados do site, o servidor terá dois processos sqlserver.exe.

Considerações de configuração do núcleo e do soquete da CPU

A configuração da CPU de um Controller, particularmente o número de núcleos disponíveis para o SQL Server Express LocalDB, afeta diretamente o desempenho do cache de host local, mais ainda do que a alocação de memória. Essa sobrecarga de CPU é observada somente durante o período de interrupção quando o banco de dados fica inacessível e o agente secundário está ativo.

Embora o LocalDB possa usar vários núcleos (até 4), ele é limitado a apenas um único soquete. Adicionar mais soquetes não melhora o desempenho (por exemplo, ter 4 soquetes com 1 núcleo cada). Em vez disso, a Citrix recomenda o uso de vários soquetes com vários núcleos. Nos testes da Citrix, uma configuração 2x3 (2 soquetes, 3 núcleos) proporcionou melhor desempenho do que as configurações 4x1 e 6x1.

Considerações sobre armazenamento

À medida que os usuários acessam recursos durante uma interrupção, o LocalDB cresce. Por exemplo, durante um teste de logon/logoff em execução a 10 logons por segundo, o banco de dados aumentou 1 MB a cada 2 a 3 minutos. Quando a operação normal é retomada, o banco de dados local é recriado e o espaço é retornado. No entanto, deve haver espaço suficiente disponível na unidade onde o LocalDB está instalado para permitir o aumento 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 agente secundário lida com todas as conexões, portanto, em sites (ou zonas) que fazem o balanceamento de carga entre vários Controllers durante operações normais, o agente secundário eleito precisa lidar com muito mais solicitações do que o normal durante uma interrupção. Portanto, as demandas de CPU serão maiores. Cada agente secundário no site (zona) deve ser capaz de lidar com a carga adicional imposta pelo banco de dados do cache de host local e todos os VDAs afetados, porque o agente secundário eleito durante uma interrupção pode mudar.

Limites de VDI:

- Em uma implantação de VDI de zona única, até 10.000 VDAs podem ser manipulados de forma eficaz durante uma interrupção.
- Em uma implantação de VDI de várias zonas, até 10.000 VDAs em cada zona podem ser manipulados de forma eficaz durante uma interrupção, até um máximo de 40.000 VDAs no site. Por exemplo, cada um dos seguintes sites pode ser manipulado 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 no site pode ser afetado. Os avaliadores de carga (especialmente, regras de contagem de sessões) podem ser excedidos.

Durante o tempo que demora até que todos os VDAs se registrem em um agente secundário, o serviço pode ficar sem informações completas sobre as sessões atuais. Assim, a solicitação de conexão de um usuário durante esse intervalo pode resultar no início de uma nova sessão, mesmo que a reconexão com uma sessão existente tenha sido possível. Esse intervalo (quando o "novo"agente secundário adquire informações de sessão de todos os VDAs durante o novo registro) é inevitável. As sessões que são conectadas quando uma interrupção começa não são afetadas durante o intervalo de transição, mas as novas sessões e as reconexões de sessão podem ser afetadas.

Esse intervalo ocorre sempre que os VDAs devem se registrar:

- Uma interrupção começa: ao migrar de um agente principal para um agente secundário.
- Falha do agente secundário durante uma interrupção: ao migrar de um agente secundário que falhou para um agente secundário recém-eleito.
- Recuperação de uma interrupção: quando as operações normais são retomadas e o agente principal retoma o controle.

Você pode diminuir o intervalo diminuindo o valor do registro `HeartbeatPeriodMs` do Citrix Broker Protocol (padrão = 600000 ms, que é 10 minutos). Esse valor de pulsação é o dobro do intervalo que o VDA usa para pings, assim, o valor padrão resulta em um ping a cada 5 minutos.

Por exemplo, o comando a seguir altera a pulsação 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
```

Atenção ao alterar o valor da pulsação. Aumentar a frequência resulta em maior carga nos Controllers durante os modos normal e de interrupção.

O intervalo não pode ser eliminado inteiramente, não importando a rapidez com que os VDAs se registram.

O tempo necessário para sincronizar entre agentes secundários aumenta com o número de objetos (como VDAs, aplicativos, grupos). Por exemplo, sincronizar 5000 VDAs pode levar 10 minutos ou mais para concluir.

Diferenças das versões do XenApp 6.x

Embora essa implementação do cache de host local compartilhe o nome do recurso Cache de Host Local no XenApp 6.x e versões anteriores do XenApp, há melhorias significativas. Essa implementação é mais robusta e imune à corrupção. Os requisitos de manutenção são minimizados, como a eliminação da necessidade de comandos `dsmaint` periódicos. Esse cache de host local é uma implementação totalmente diferente, tecnicamente.

Gerenciar cache de host local

Para que o cache de host local funcione corretamente, a política de execução do PowerShell de 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. Somente o agente secundário se comunica com esse banco de dados. Você não pode usar cmdlets do PowerShell para alterar nada sobre esse banco de dados. O LocalDB não pode ser compartilhado entre Controllers.

O software do banco de dados do 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, tenha em mente que o recurso Cache de Host Local não funciona sem o banco de dados, e você não pode usar um banco de dados diferente com o agente secundário.

A instalação desse banco de dados LocalDB não tem efeito sobre se você instala ou não 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 o SQL Server Express LocalDB.

Configurações padrão após a instalação e atualização do produto

Durante uma nova instalação do Citrix Virtual Apps and Desktops (versão mínima 7.16), o Cache de Host Local é ativado.

Após uma atualização (para a versão 7.16 ou posterior), o Cache de Host Local é ativado se houver menos de 10.000 VDAs em toda a implantação.

Ativar e desativar cache de host local

- Para ativar o cache de host local, insira:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Para determinar se o cache de host local está ativado, insira `Get-BrokerSite`. Verifique se a propriedade `LocalHostCacheEnabled` é `True`.

- Para desativar o cache de host local, insira:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Lembre-se: a partir do XenApp e XenDesktop 7.16, a concessão de conexão (o recurso que precedeu o Cache de Host Local começando com a versão 7.6) foi removida do produto e não está mais disponível.

Verificar se o Cache de Host Local está funcionando

Para verificar se o Cache de Host Local 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 do SQL Server Express LocalDB foi criado em cada Delivery Controller. Isso confirma que o agente secundário pode assumir, se necessário.

  - No servidor do Delivery Controller, vá para `C:\Windows\ServiceProfiles\NetworkService`.
  - Confirme que `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.

- Force uma interrupção nos controladores de entrega. Depois de verificar se o Cache de Host Local 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 do evento, o modo da interrupção é referido como *HA mode*.*

Config Synchronizer Service:

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados do Cache de Host Local usando o agente de cache de host local.

- 503: o Citrix Config Sync Service recebeu uma configuração atualizada. Esse evento indica o início do processo de sincronização.
- 504: o Citrix Config Sync Service importou uma configuração atualizada. A importação da configuração foi concluída com sucesso.
- 505: o Citrix Config Sync Service falhou na importação. A importação da configuração não foi concluída com sucesso. Se uma configuração anteriormente bem-sucedida estiver disponível, ela será usada se ocorrer uma interrupção. No entanto, ela não estará atualizada com a configuração atual. Se não houver nenhuma configuração anterior disponível, o serviço não poderá participar da intermediação de sessão durante uma interrupção. Nesse caso, consulte a seção de Resolução de problemas e entre em contato com o Suporte Citrix.
- 507: o Citrix Config Sync Service abandonou uma importação porque o sistema está no modo de interrupção e o agente de cache de host local está sendo usado para a intermediação. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque ocorreu uma interrupção. Esse é o comportamento esperado.
- 510: não há dados de configuração do Configuration Service recebidos do Configuration Service principal.
- 517: houve um problema de comunicação com o agente primário.
- 518: script Config Sync anulado porque o agente secundário (High Availability Service) não está em execução.

High Availability Service:

Este serviço também é conhecido como agente de cache de host local.

- 3502: ocorreu uma interrupção e o agente de cache de host local está executando operações de intermediação.
- 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, deliberadamente, forçar uma interrupção.

- Se a operação da sua rede é interrompida repetidamente. Forçar uma interrupção até que os problemas de rede sejam resolvidos evita a transição contínua entre os modos normal e de interrupção (e as tempestades de registros de VDA frequentes resultantes).
- Para testar um plano de recuperação de desastres.
- Para ajudar a garantir que o Cache de Host Local está funcionando corretamente.
- Durante a substituição ou 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 agente de Cache de Host Local a entrar no modo de interrupção, independentemente do estado do banco de dados. Definir o valor para `0` retira o agente de Cache de Host Local do modo de interrupção.

Para verificar eventos, monitore o arquivo de log `Current_HighAvailabilityService` em `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`.

Solução de problemas

Várias ferramentas de solução de problemas estão disponíveis quando uma importação de sincronização para o banco de dados do Cache de Host Local falha e um evento 505 é publicado.

CDF tracing: contém opções para os módulos `ConfigSyncServer` e `BrokerLHC`. Essas opções, juntamente com outros módulos de agentes, provavelmente identificarão o problema.

Report: se uma importação de sincronização falhar, você pode gerar um relatório. Esse relatório para no objeto que está causando o erro. Esse recurso de relatório afeta a velocidade de sincronização, portanto, a Citrix recomenda desativá-lo quando não estiver em uso.

Para ativar e produzir um relatório de rastreamento CSS, insira o seguinte comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```


O relatório HTML é publicado em `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`.

Depois que o relatório for gerado, insira o seguinte comando para desativar o recurso de relatório:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

Export the broker configuration: fornece a configuração exata para fins de depuração.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Por exemplo, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Gerenciar chaves de segurança

June 28, 2023

> **Importante:**
>
> - Você deve usar este recurso em combinação com o StoreFront 1912 LTSR CU2 ou posterior.
> - O recurso Secure XML só é suportado no Citrix ADC e no Citrix Gateway versão 12.1 ou superior.
>
> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Este recurso permite que você autorize apenas máquinas StoreFront e Citrix Gateway aprovadas para se comunicarem com Delivery Controllers. Depois que você habilitar esse recurso, todas as solicitações que não contenham a chave serão bloqueadas. Use esse recurso para adicionar uma camada extra de segurança para se proteger contra ataques originados na rede interna.

Eis aqui um fluxo de trabalho geral para usar esse recurso:

1. Ative o Web Studio para mostrar as configurações do recurso.
2. Defina as configurações do seu site.
3. Defina as configurações do StoreFront.
4. Defina as configurações do Citrix ADC.

Ativar o Web Studio para mostrar as configurações do recurso

Por padrão, as configurações das chaves de segurança estão ocultas do Web Studio. Para permitir que o Web Studio os exiba, use o SDK do PowerShell da seguinte forma:

1. Execute o SDK do PowerShell do Citrix Virtual Apps and Desktops.
2. Em uma janela de comando, execute os seguintes comandos:

    - `Add-PSSnapIn Citrix*`. Esse comando adiciona os snap-ins da Citrix.
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

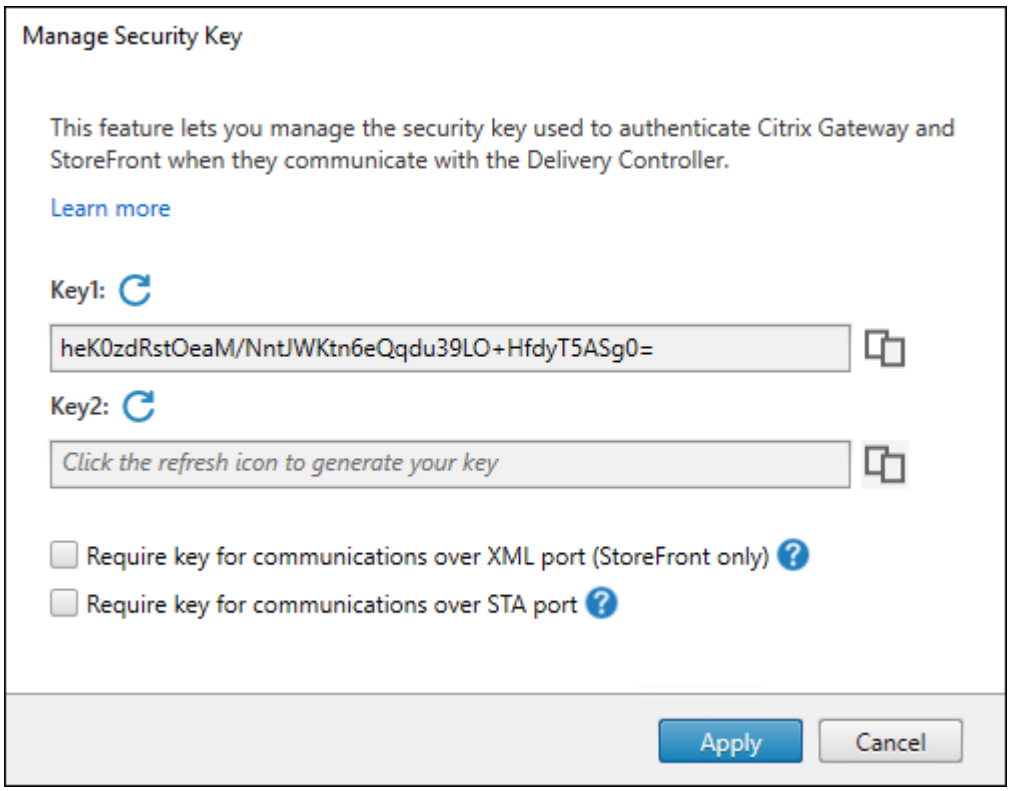
Para obter mais informações sobre o PowerShell SDK, consulte SDKs e APIs.

Definir configurações para o site

Você pode usar o Web Studio ou o PowerShell para definir as configurações da chave de segurança do seu site.

Usar o Web Studio

1. Entre no Web Studio, selecione **Settings** no painel esquerdo.
2. Localize o bloco **Manage security key** e clique em **Edit**. A página **Manage Security Key** é exibida.



3. Clique no ícone de atualização para gerar as chaves.

> **Importante:**
>
> - Existem duas chaves disponíveis para uso. Você pode usar a mesma chave ou chaves diferentes para comunicações pelas portas XML e STA. Recomendamos que você use apenas uma chave de cada vez. A chave não utilizada é usada apenas para a rotação de chaves.
> - Não clique no ícone de atualização para atualizar a chave já em uso. Se você fizer isso, ocorrerá a interrupção do serviço.

4. Selecione onde uma chave é necessária para a comunicação:

   - **Require key for communications over XML port (StoreFront only)**. Se selecionada, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por essa porta. Para obter informações sobre como alterar a porta XML, consulte o artigo do Knowledge Center CTX127945.
   - **Require key for communications over STA port**. Se selecionada, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por essa porta. Para obter informações sobre como alterar a porta STA, consulte o artigo do Knowledge Center CTX101988.

5. Clique em **Save** para aplicar as alterações e fechar a janela.

Usar o PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações do Web Studio.

1. Execute o SDK do PowerShell remoto do Citrix Virtual Apps and Desktops
2. Em uma janela de comando, execute o seguinte comando:
   - `Add-PSSnapIn Citrix*`
3. Execute os seguintes comandos para gerar uma chave e configurar Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Execute os seguintes comandos para gerar uma chave e configurar Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Execute um ou ambos os comandos a seguir para habilitar o uso de uma chave na autenticação de comunicações:
   - Para autenticar comunicações pela porta XML:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Para autenticar comunicações pela porta STA:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte a ajuda do comando do PowerShell para obter orientação e sintaxe.

Definir as configurações do StoreFront

Depois de concluir a configuração do seu site, você precisa definir as configurações relevantes do StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos do PowerShell:

- Para configurar a chave para comunicações pela porta XML, use os comandos `Get-STFStoreServie` e `Set-STFStoreService`. Por exemplo:

  ```
  PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80
   -TransportType HTTP -Servers <domain name1, domain name2> -
  XMLValidationEnabled $true -XMLValidationSecret <the key you
  generated in Web Studio>
  ```

- Para configurar a chave para comunicações pela porta STA, use o comando `New-STFSecureTicketAuth`. Por exemplo:

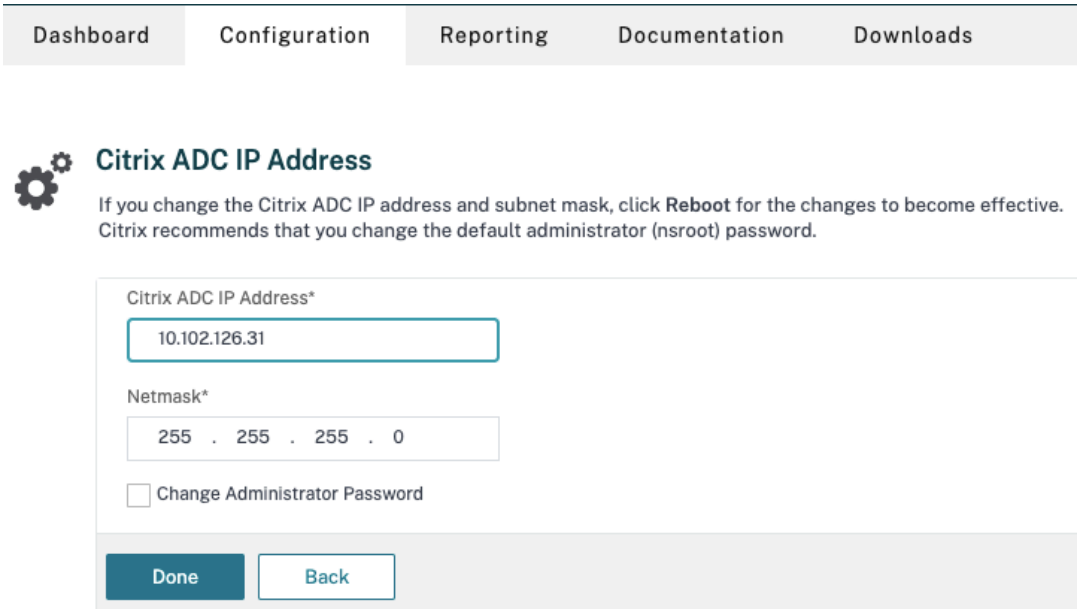

```
- PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL
  > -StaValidationEnabled $true -StavalidationSecret <the key
  you generated in Web Studio>
```

Consulte a ajuda do comando do PowerShell para obter orientação e sintaxe.

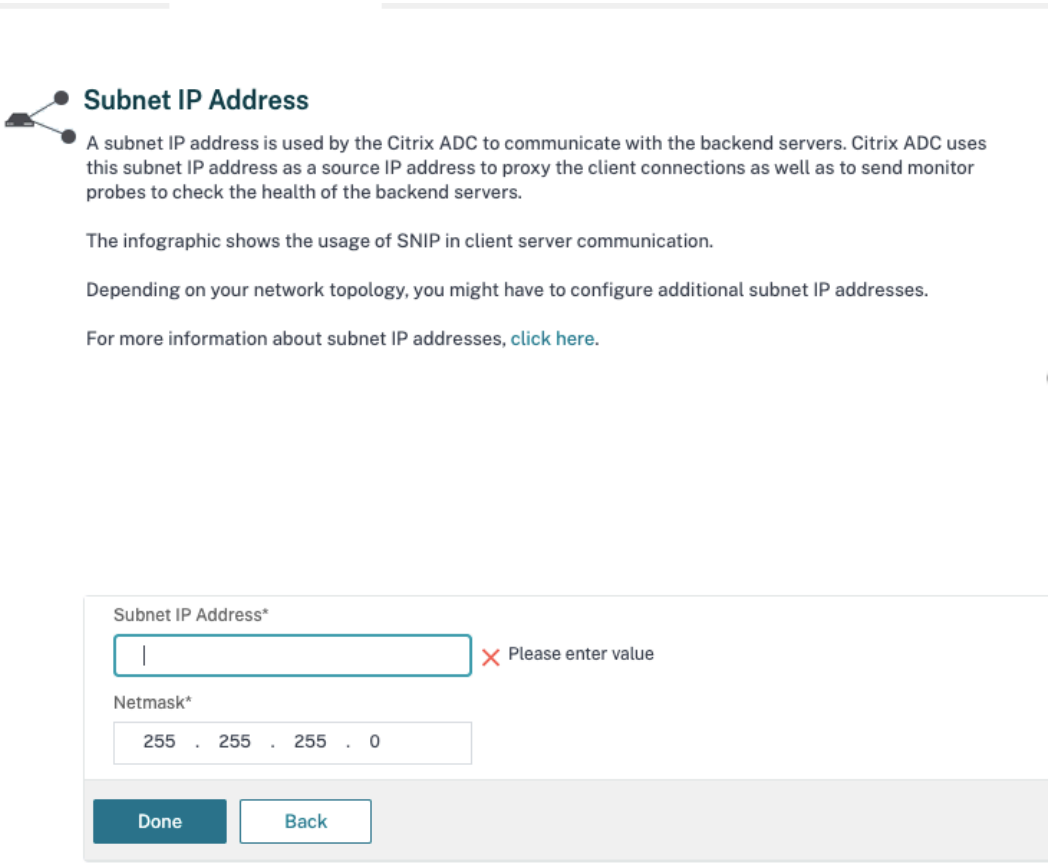
Definir configurações do Citrix ADC

> **Nota:**
>
> A configuração desse recurso do Citrix ADC não é necessária, a menos que você use o Citrix ADC como gateway. Se você usa o Citrix ADC, siga estas etapas:

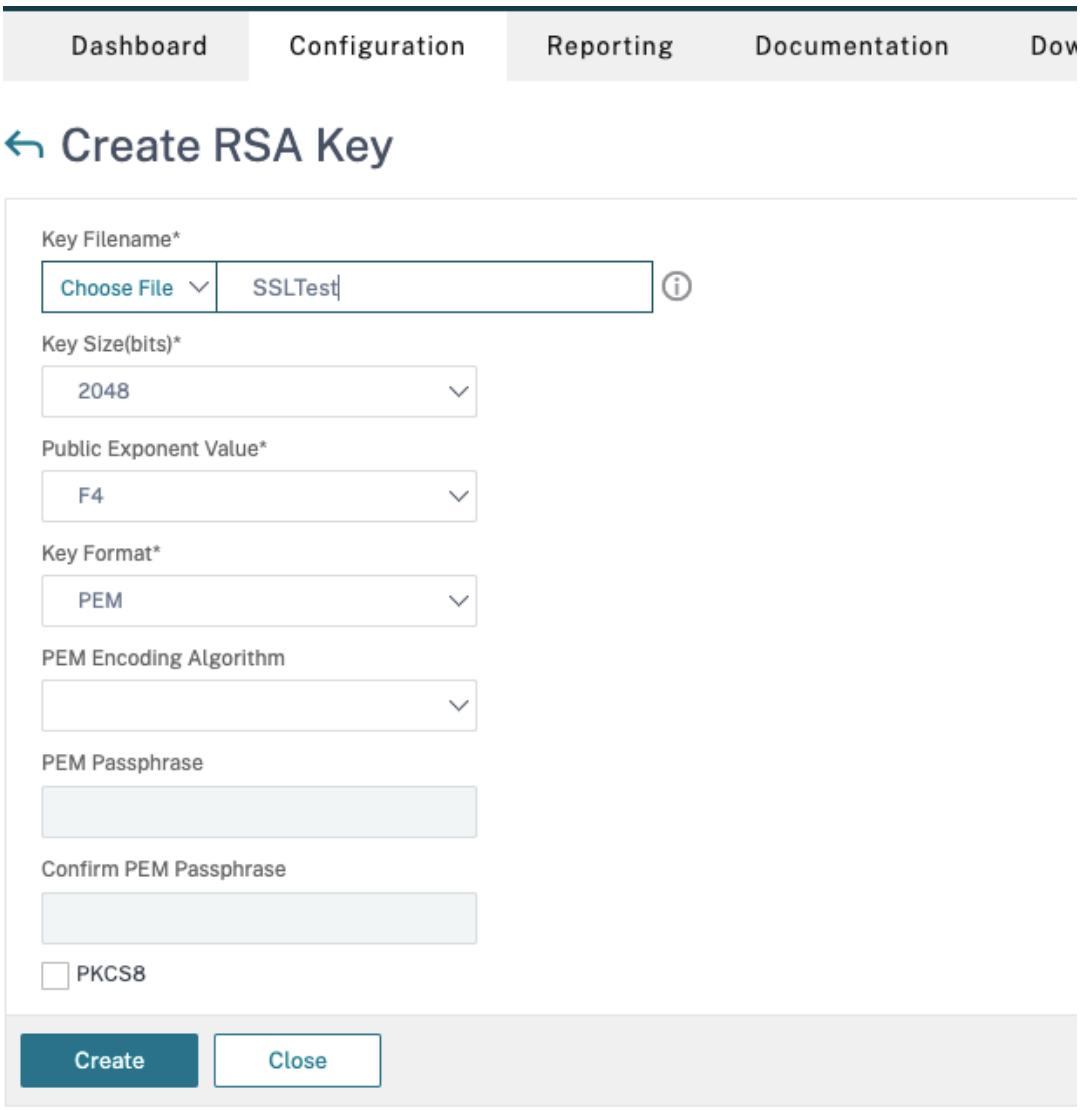
1. Verifique se a seguinte configuração de pré-requisito já está em vigor:
   - Os seguintes endereços IP relacionados ao Citrix ADC são configurados.
     - Endereço IP de gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



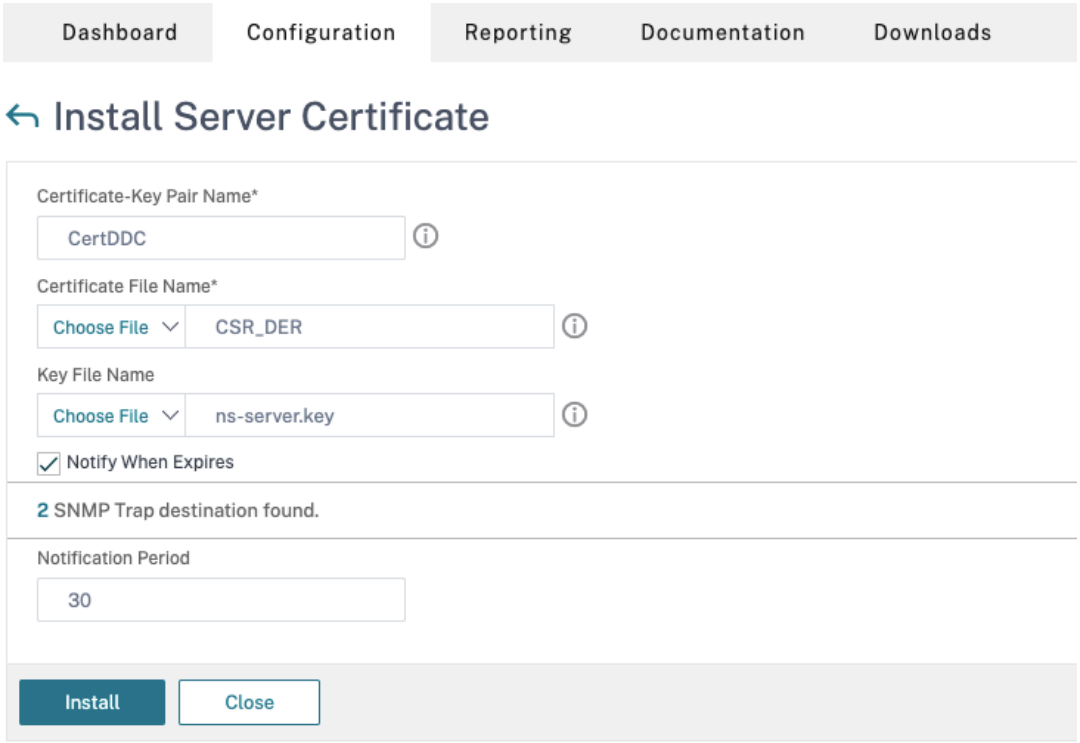
     - Endereço IP de sub-rede (SNIP) para permitir a comunicação entre o appliance Citrix ADC e os servidores back-end. Para obter detalhes, consulte Configuração de endereços IP de sub-rede.
     - Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no appliance ADC para iniciar a sessão. Para obter detalhes, consulte Criar um servidor virtual.

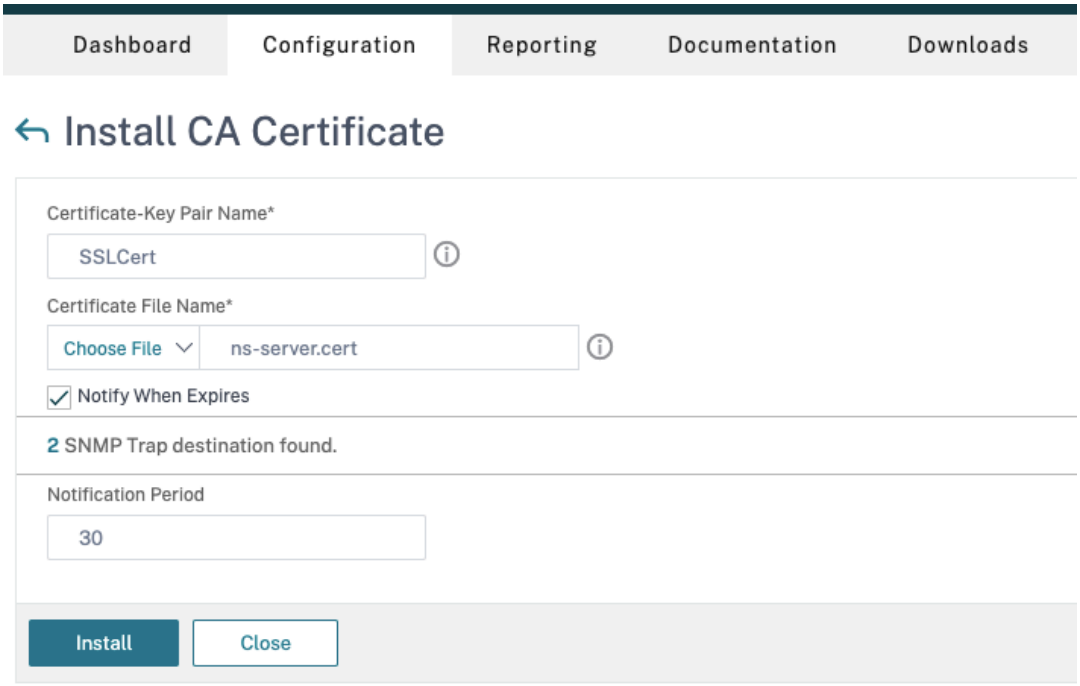


- Os modos e recursos necessários no dispositivo Citrix ADC estão ativados.
  - Para ativar os modos, na GUI do Citrix ADC, navegue até **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, navegue até **System > Settings > Configure Basic Features**.
- As configurações relacionadas aos certificados estão completas.
  - A solicitação de assinatura de certificado (CSR) é criada. Para obter detalhes, consulte Criar um certificado.

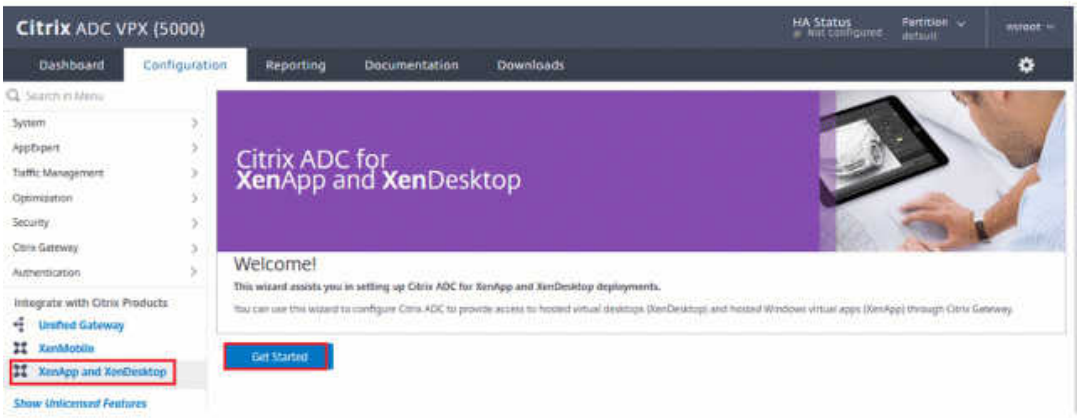


- O servidor e os certificados CA e os certificados raiz estão instalados. Para obter detalhes, consulte Instalação, link e atualizações.



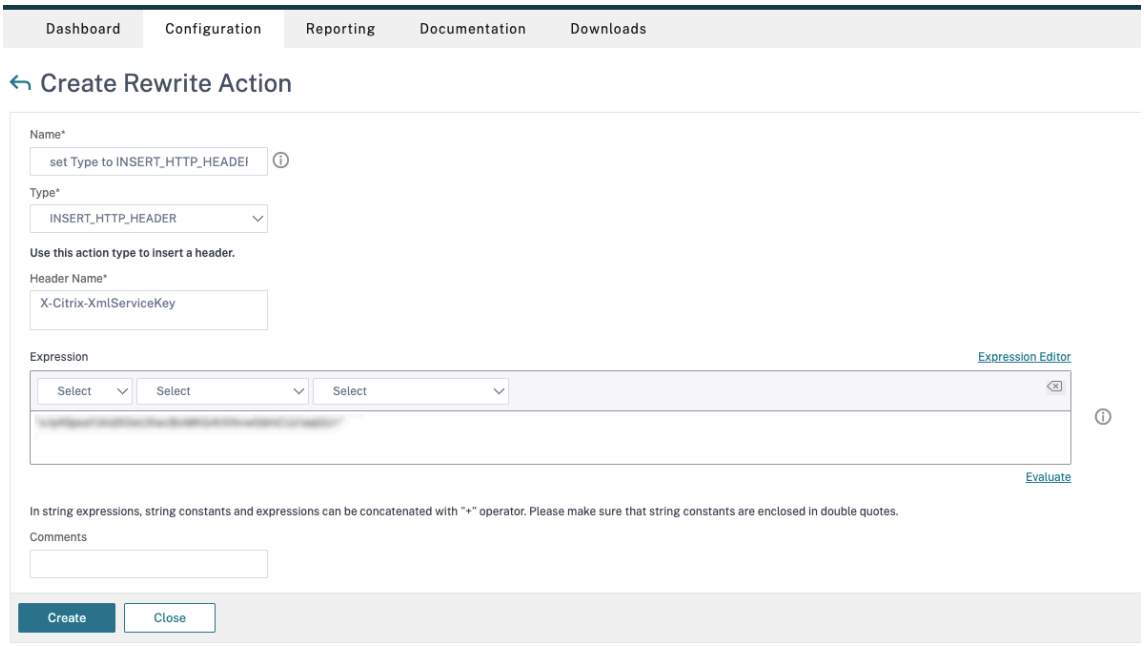


- Um Citrix Gateway foi criado para o Citrix Virtual Desktops. Teste a conectividade clicando no botão **Test STA Connectivity** para confirmar se os servidores virtuais estão online. Para obter detalhes, consulte Configuração do Citrix ADC para Citrix Virtual Apps and Desktops.

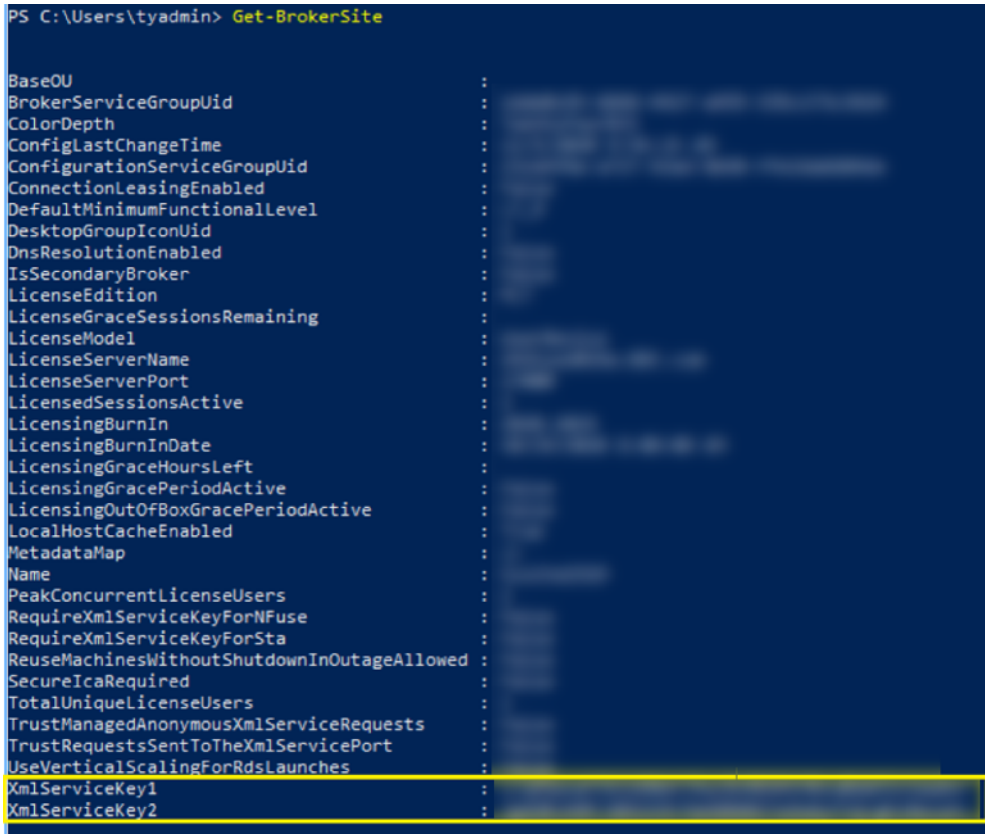


2. Adicione uma ação de regravação Para obter detalhes, consulte Configurando uma ação de regravação.

   a) Navegue até **AppExpert > Rewrite > Actions**.
   b) Clique em **Add** para adicionar uma nova ação de regravação. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".



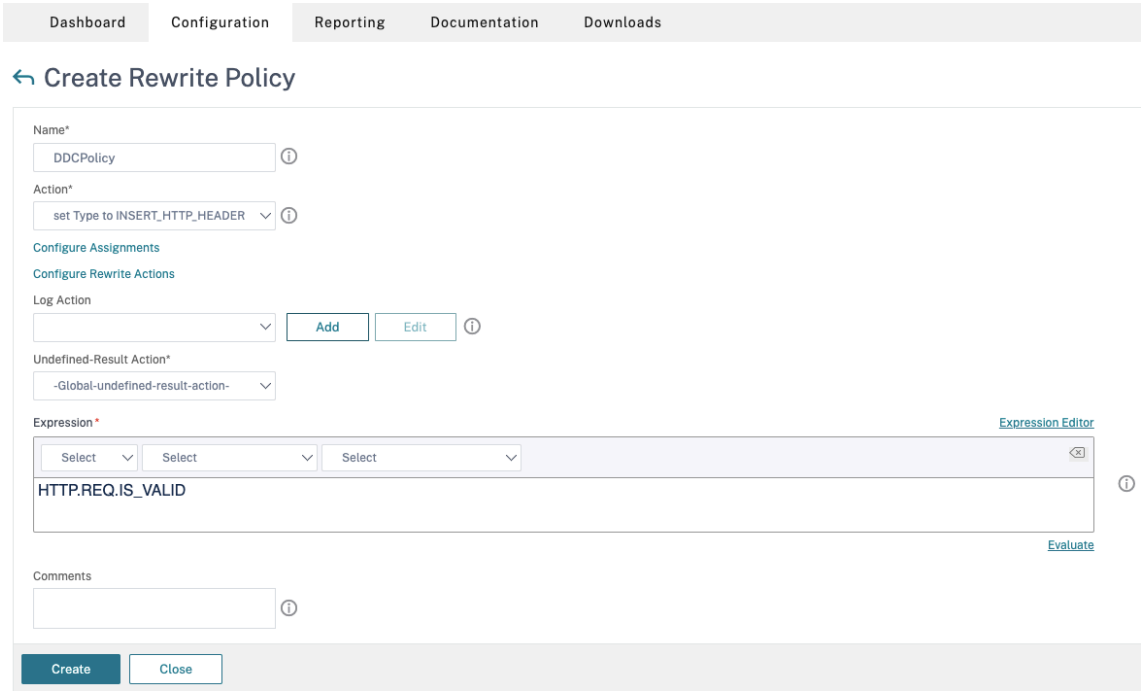
   a) Em **Type**, selecione **INSERT_HTTP_HEADER**.
   b) Em **Header Name**, insira X-Citrix-XmlServiceKey.
   c) Em **Expression**, adicione <`XmlServiceKey1 value`> com as aspas. Você pode copiar o valor XmlServiceKey1 da configuração do Desktop Delivery Controller.



3. Adicione uma política de regravação. Para obter detalhes, consulte Configurando uma política de regravação.

   a) Navegue até **AppExpert > Rewrite > Policies**.

   b) Clique em **Add** para adicionar uma nova política.



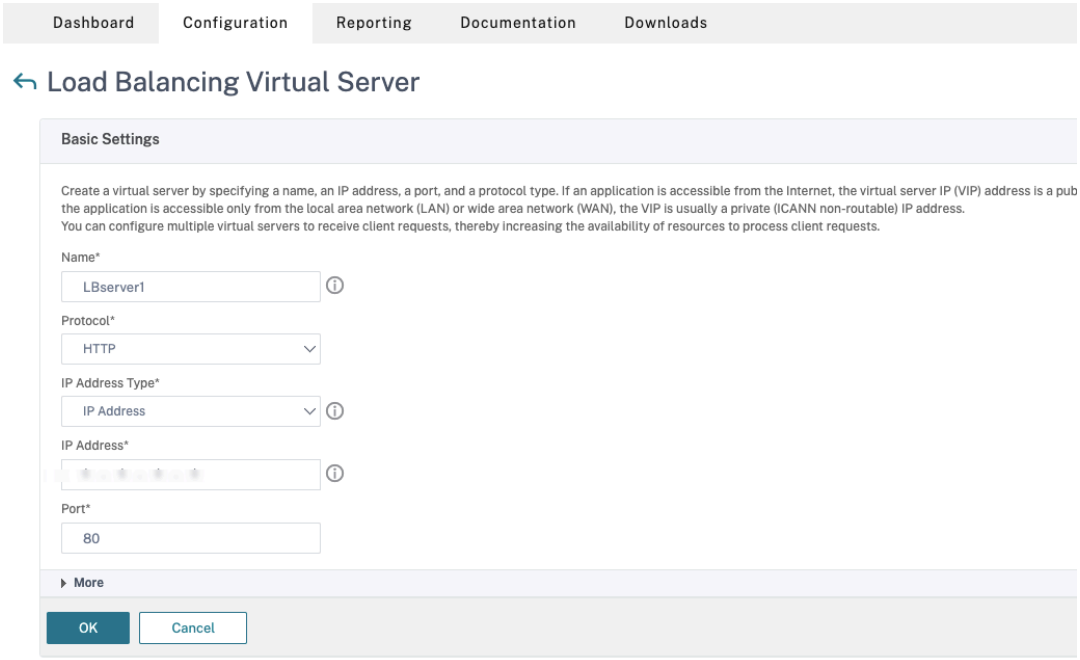
a) Em **Action**, selecione a ação criada na etapa anterior.
b) Em **Action**, adicione HTTP.REQ.IS_VALID.
c) Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões não serão iniciadas.

   Para obter detalhes, consulte Configurar o balanceamento de carga básico.

   a) Crie um servidor virtual de balanceamento de carga.

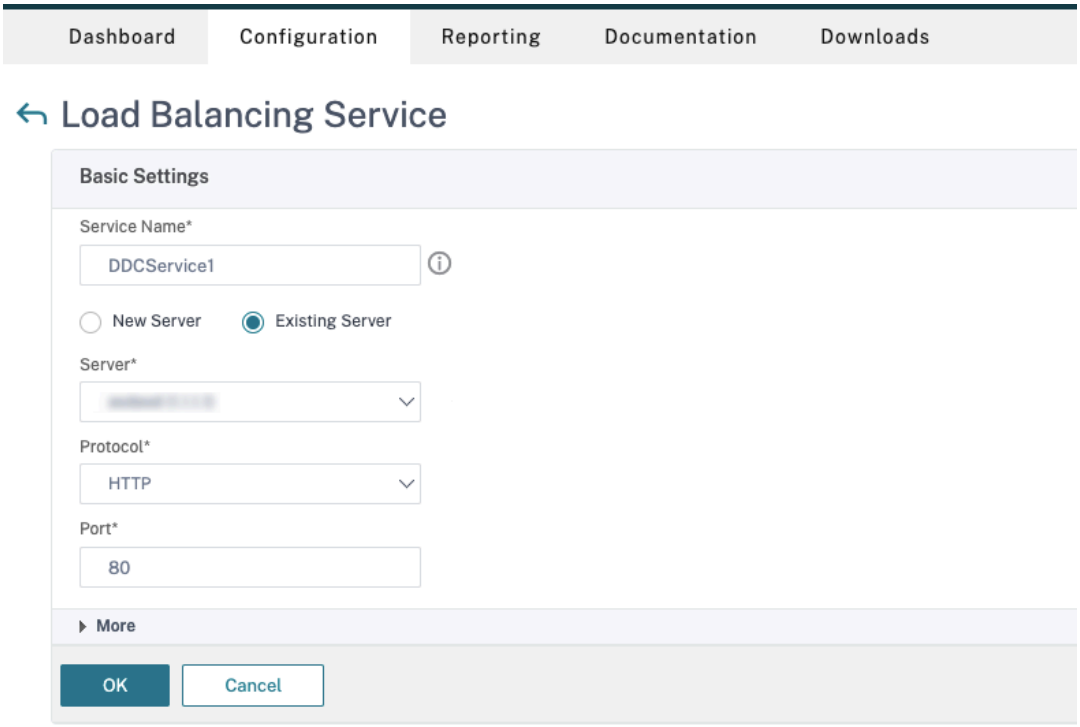
      - Navegue até **Traffic Management > Load Balancing > Servers**.
      - Na página **Virtual Servers**, clique em **Add**.



- Em **Protocol**, selecione **HTTP**.
- Adicione o endereço IP virtual de balanceamento de carga e, em **Port**, selecione **80**.
- Clique em **OK**.

b) Crie um serviço de balanceamento de carga.

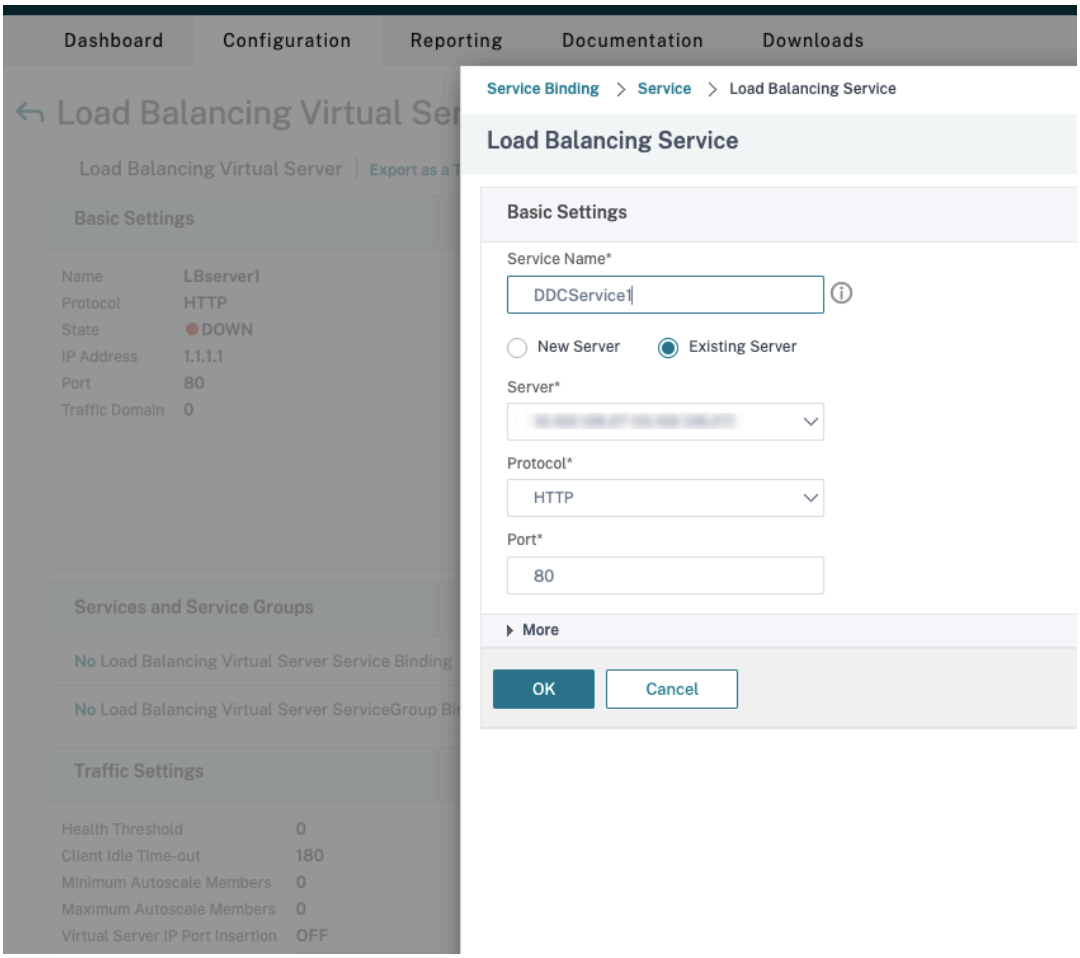
- Navegue até **Traffic Management > Load Balancing > Services**.



- Em **Existing Server**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocol**, selecione **HTTP** e, em **Port**, selecione **80**.
- Clique em **OK** e clique em **Done**.

c) Vincule o serviço ao servidor virtual.

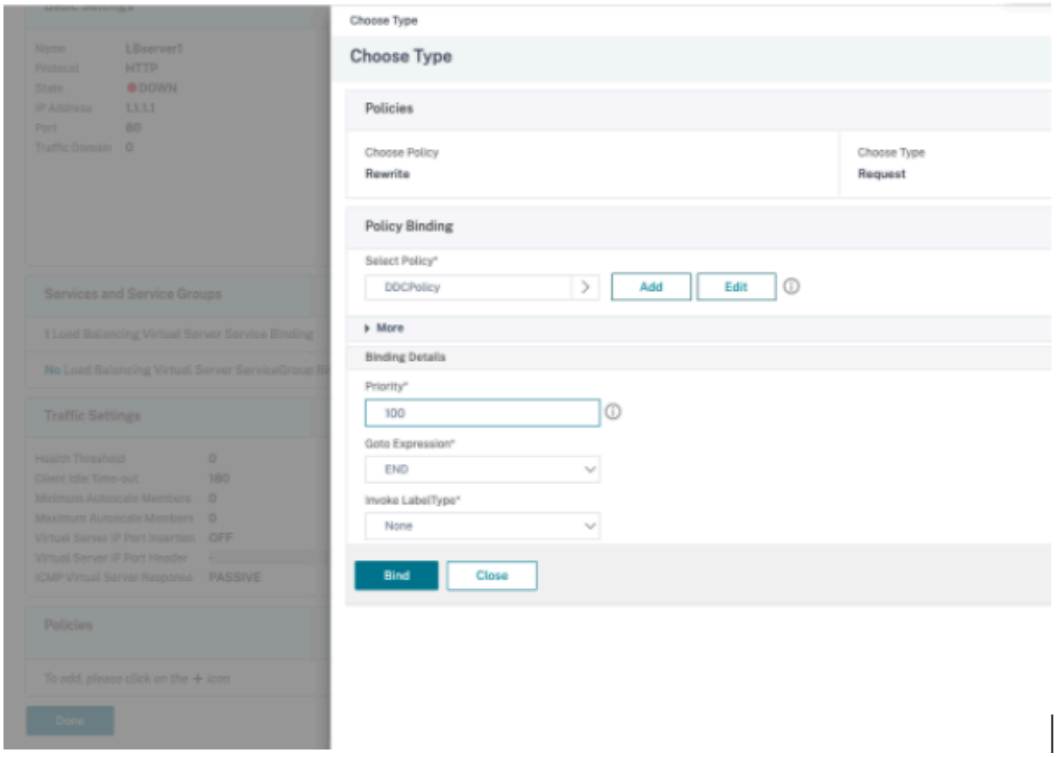
- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Services and Service Groups**, clique em **No Load Balancing Virtual Server Service Binding**.



- Em **Service Binding**, selecione o serviço criado anteriormente.
- Clique em **Bind**.

d) Vincule a política de regravação criada anteriormente ao servidor virtual.

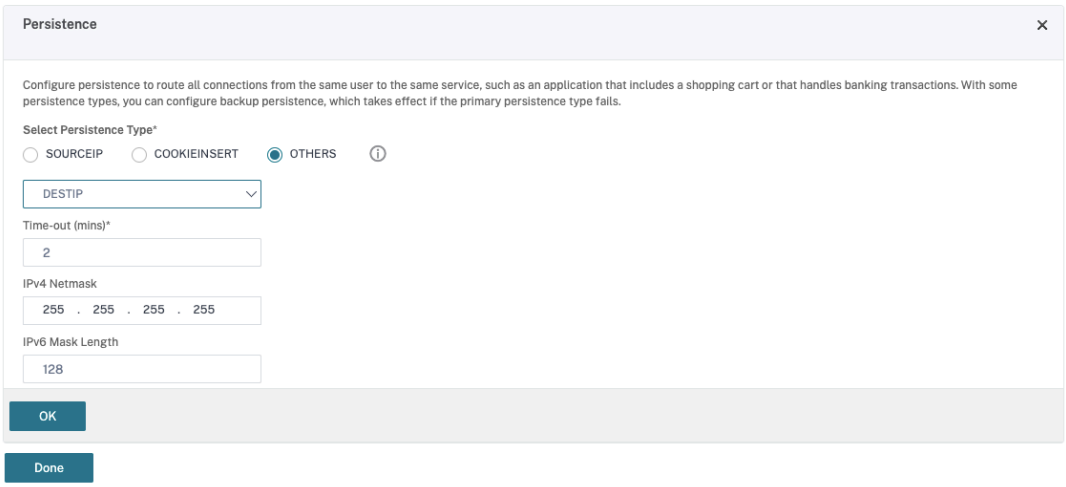
- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Advanced Settings**, clique em **Policies** e então, na sessão **Policies**, clique em **+**.



- Em **Choose Policy**, selecione **Rewrite** e em **Choose Type**, selecione **Request**.
- Clique em **Continue**.
- Em **Select Policy**, selecione a política de regravação criada anteriormente.
- Clique em **Bind**.
- Clique em **Concluído**.

e) Configure a persistência para o servidor virtual, se necessário.

- Selecione o servidor virtual criado anteriormente e clique em **Edit**.
- Em **Advanced Settings**, clique em **Persistence**.



- Selecione o tipo de persistência como **Others**.

- Selecione **DESTIP** para criar sessões de persistência com base no endereço IP do serviço selecionado pelo servidor virtual (o endereço IP de destino)
- Em **IPv4 Netmask**, adicione uma máscara de rede igual à do DDC.
- Clique em **OK**.

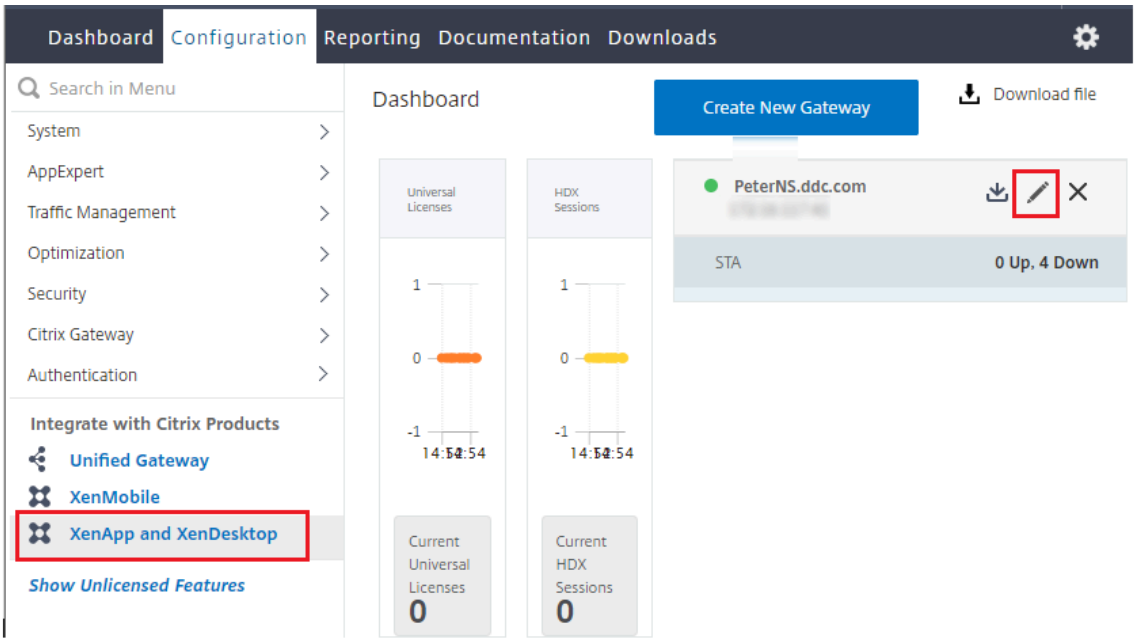
f) Repita essas etapas para o outro servidor virtual também.

Mudanças de configuração se o dispositivo Citrix ADC já estiver configurado com o Citrix Virtual Desktops

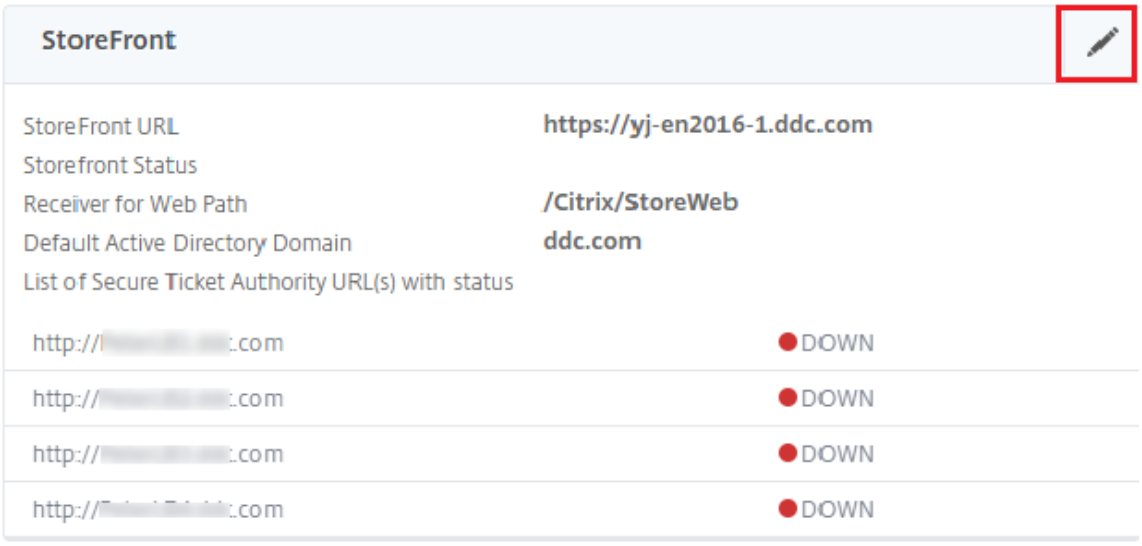
Se você já configurou o dispositivo Citrix ADC com o Citrix Virtual Desktops, para usar o recurso Secure XML, faça as seguintes alterações de configuração.

- Antes do início da sessão, altere o **Security Ticket Authority URL** do gateway para usar os FQDNs dos servidores virtuais de balanceamento de carga.
- Verifique se o parâmetro `TrustRequestsSentToTheXmlServicePort` está definido como False. Por padrão, o parâmetro `TrustRequestsSentToTheXmlServicePort` é definido como False. No entanto, se o cliente já tiver configurado o Citrix ADC para Citrix Virtual Desktops, o `TrustRequestsSentToTheXmlServicePort` está definido como Verdadeiro.

1. Na GUI do Citrix ADC, navegue até **Configuration > Integrate with Citrix Products** e clique em **XenApp and XenDesktop**.
2. Selecione a instância do gateway e clique no ícone de edição.

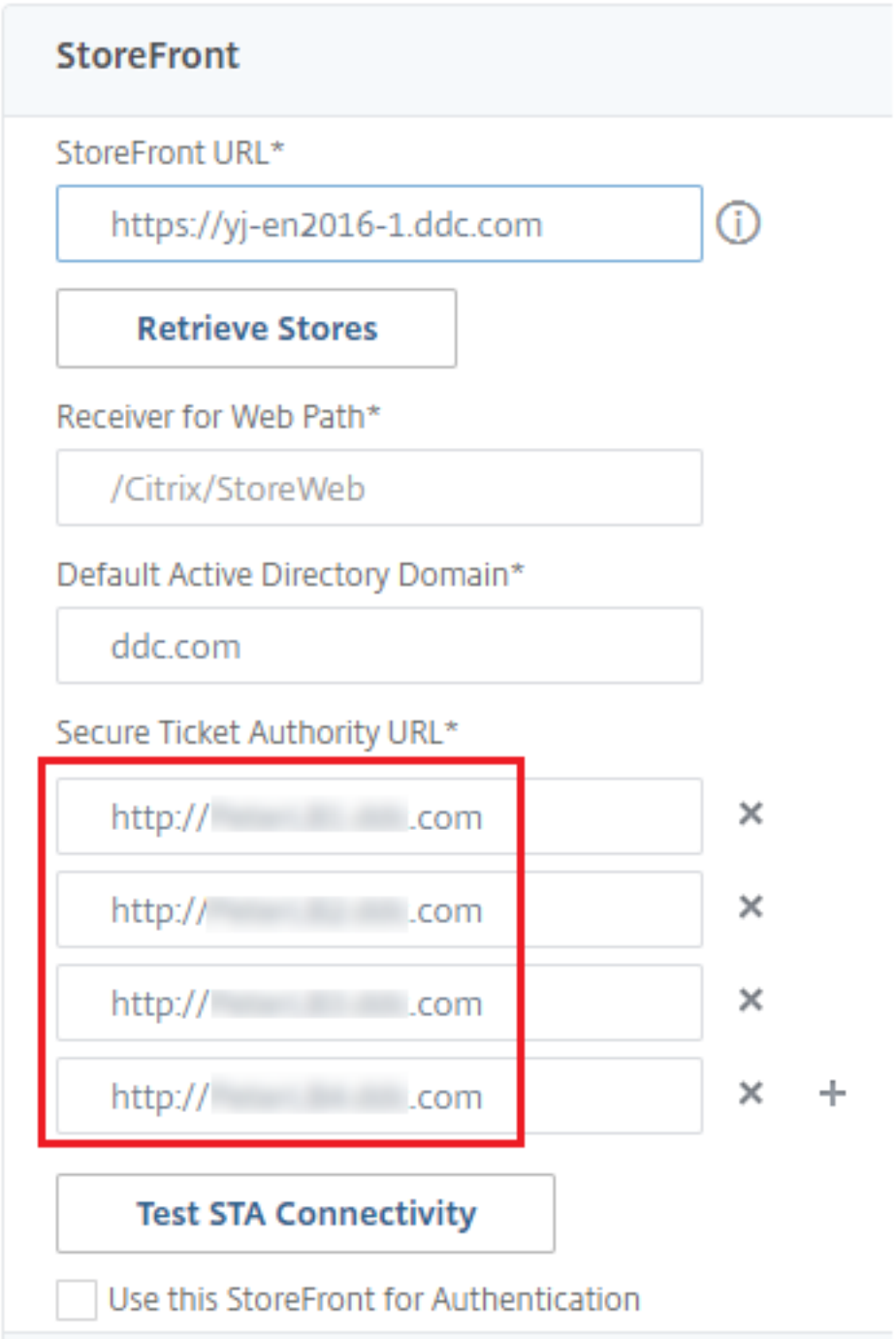


3. No painel StoreFront, clique no ícone de edição.



4. Adicione o **Secure Ticket Authority URL**.

   - Se o recurso XML seguro estiver habilitado, a URL STA deverá ser a URL do serviço de balanceamento de carga.
   - Se o recurso XML seguro estiver desativado, a URL STA deverá ser a URL do STA (endereço do DDC) e o parâmetro TrustRequestsSentToTheXmlServicePort no DDC deve ser definido como True.



Sessões

June 28, 2023

Manter a atividade da sessão é fundamental para oferecer a melhor experiência de usuário. Perder

conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode deixar o usuário tenso. Mover-se rapidamente entre dispositivos e acessar os mesmos aplicativos a cada login é uma prioridade para muitos trabalhadores móveis, como os profissionais de saúde.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões e reduzem inconvenientes, tempo de inatividade e perda de produtividade. Usando esses recursos, os usuários móveis podem mudar de forma rápida e fácil entre dispositivos.

Você também pode fazer logoff de usuário, desconectar uma sessão e configurar a pré-inicialização e a permanência da sessão; consulte Gerenciar grupos de entrega.

Confiabilidade da sessão

A opção Session Reliability mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Esse recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel e perde a conectividade momentaneamente. Normalmente, a sessão é desconectada e desaparece da tela do usuário, e o usuário precisa se reconectar à sessão desconectada. Com a Confiabilidade da Sessão, a sessão permanece ativa na máquina. Para indicar a conectividade perdida, a tela do usuário congela e o cursor muda para uma ampulheta giratória até que a conectividade seja retomada no outro lado do túnel. O usuário continua acessando a tela durante a interrupção e pode retomar a interação com o aplicativo quando a conexão de rede é restaurada. A Confiabilidade de Sessão reconecta usuários sem solicitar a reautenticação.

Os usuários do aplicativo Citrix Workspace não podem substituir a configuração do Controller.

Você pode usar a Confiabilidade da Sessão com TLS (Transport Layer Security). O TLS criptografa apenas os dados enviados entre o dispositivo do usuário e o Citrix Gateway.

Ative e configure a Confiabilidade da Sessão com as seguintes configurações de política:

- A configuração da política de conexões de confiabilidade da sessão permite ou evita a confiabilidade da sessão.
- A configuração da política de tempo limite de confiabilidade da sessão tem um padrão de 180 segundos ou três minutos. Embora você possa estender a quantidade de tempo que a confiabilidade da sessão mantém uma sessão aberta, esse recurso foi projetado para a conveniência do usuário. Consequentemente, ele não solicita que o usuário faça a reautenticação. À medida que você estende a quantidade de tempo que uma sessão é mantida aberta, as chances de que um usuário se distraia e se afaste do dispositivo aumentam. Essa ação pode deixar a sessão acessível a usuários não autorizados.

- As conexões de confiabilidade de sessão recebidas usam a porta 2598, a menos que você altere o número da porta na configuração da política de número de porta de confiabilidade da sessão.
- Para evitar que os usuários se reconectem às sessões interrompidas sem precisar se autenticar novamente, use o recurso de Reconexão automática de cliente. Você pode definir a configuração da política de autenticação de Reconexão automática de cliente para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usa a Confiabilidade da sessão e a Reconexão automática de cliente, os dois recursos funcionam em sequência. A Confiabilidade da Sessão fecha ou desconecta a sessão do usuário após o tempo especificado na configuração da política de tempo limite de confiabilidade da sessão. Depois disso, as configurações da política de Reconexão automática de cliente entram em vigor, tentando reconectar o usuário à sessão desconectada.

Reconexão automática de cliente

Com o recurso de Reconexão automática de cliente, o aplicativo Citrix Workspace pode detectar desconexões não intencionais de sessões ICA e reconectar os usuários às sessões afetadas automaticamente. Quando esse recurso está ativado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Em sessões de aplicativo, o aplicativo Citrix Workspace tenta se reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Em sessões de área de trabalho, o aplicativo Citrix Workspace tenta se reconectar à sessão por um período especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, esse período é de cinco minutos. Para alterar esse período, edite a seguinte configuração de registro no dispositivo do usuário (onde `seconds` está o número de segundos após o qual não são feitas mais tentativas para reconectar a sessão).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

Ative e configure a Reconexão automática de cliente com as seguintes configurações de política:

- **Auto Client Reconnect:** ativa ou desativa a reconexão automática pelo aplicativo Citrix Workspace após uma conexão ter sido interrompida.
- **Auto Client Reconnect authentication:** ativa ou desativa o requisito de autenticação do usuário após a reconexão automática.
- **Auto Client Reconnect logging:** ativa ou desativa o registro em log de eventos de reconexão no log de eventos. O log é desativado por padrão. Quando ativado, o log do sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e com falha. Cada servidor armazena informações sobre eventos de reconexão no log do seu próprio sistema. O site não fornece um log combinado de eventos de reconexão para todos os servidores.

A Reconexão automática de cliente incorpora um mecanismo de autenticação baseado em credenciais de usuário criptografadas. Quando um usuário faz logon inicialmente, o servidor criptografa e armazena as credenciais do usuário na memória. O servidor também cria e envia um cookie contendo a chave de criptografia para o aplicativo Citrix Workspace. O aplicativo Citrix Workspace envia a chave ao servidor para reconexão. O servidor descriptografa as credenciais e as envia ao logon do Windows para autenticação. Quando os cookies expiram, os usuários devem se autenticar novamente para se reconectar às sessões.

Os cookies não são usados se você ativar a configuração de autenticação de Reconexão automática de cliente. Em vez disso, uma caixa de diálogo solicita as credenciais aos usuários quando o aplicativo Citrix Workspace tenta se reconectar automaticamente.

Para proteção máxima das credenciais e sessões do usuário, use criptografia para toda a comunicação entre clientes e o site.

Desative a Reconexão automática de cliente no aplicativo Citrix Workspace para Windows usando o arquivo icaclient.adm. Para obter mais informações, consulte a documentação correspondente à sua versão do aplicativo Citrix Workspace para Windows.

As configurações das conexões também afetam a reconexão automática de cliente:

- Por padrão, a opção Auto Client Reconnect é ativada por meio de configurações de política no nível do site, conforme descrito anteriormente. A reautenticação do usuário não é exigida. No entanto, se a conexão ICA TCP de um servidor estiver configurada para redefinir sessões com um link de comunicação interrompido, a reconexão automática não ocorrerá. A reconexão automática de cliente só funciona se o servidor desconectar sessões quando houver uma conexão interrompida ou expirada. Nesse contexto, a conexão ICA TCP refere-se à porta virtual de um servidor (em vez de uma conexão de rede real) que é usada para sessões em redes TCP/IP.
- Por padrão, a conexão ICA TCP em um servidor é definida para desconectar sessões com conexões interrompidas ou expiradas. As sessões desconectadas permanecem intactas na memória do sistema e ficam disponíveis para reconexão pelo aplicativo Citrix Workspace.
- A conexão pode ser configurada para redefinir ou fazer o logoff de sessões com conexões interrompidas ou expiradas. Quando uma sessão é redefinida, tentar reconectar inicia uma nova sessão. Em vez de restaurar um usuário no mesmo local no aplicativo em uso, o aplicativo é reiniciado.
- Se o servidor estiver configurado para redefinir sessões, a reconexão automática de cliente criará uma nova sessão. Esse processo exige que os usuários insiram suas credenciais para fazer logon no servidor.
- A reconexão automática pode falhar se o aplicativo Citrix Workspace ou o plug-in enviar informações de autenticação incorretas, o que pode ocorrer durante um ataque ou se o servidor determinar que decorreu muito tempo desde que ele detectou a conexão interrompida.

ICA Keep-Alive

Permitir o recurso ICA Keep-Alive impede que conexões interrompidas sejam desconectadas. Quando ativado, se o servidor não detectar nenhuma atividade, esse recurso impede que os Serviços de Área de Trabalho Remota desconectem a sessão. Exemplos de falta de atividade incluem: nenhuma mudança 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 marca a sessão como desconectada.

> **Importante:**
>
> O ICA Keep-Alive funciona somente se você não estiver usando a confiabilidade da sessão. A confiabilidade da sessão tem seus próprios mecanismos para evitar que conexões interrompidas sejam desconectadas. Configure o ICA Keep-Alive somente para conexões que não usam a confiabilidade da sessão.

As configurações do ICA Keep-Alive substituem as configurações do keep-alive definidas na Política de grupo do Windows.

Ative e configure o ICA Keep-Alive com as seguintes configurações de política:

- **ICA keep alive timeout:** especifica o intervalo (1-3600 segundos) usado para enviar mensagens de ICA keep-alive. Não configure essa opção se quiser que seu software de monitoramento de rede feche conexões inativas em ambientes onde as conexões interrompidas são tão pouco frequentes que permitir que os usuários se reconectem às sessões não é uma preocupação.

  O intervalo padrão é 60 segundos: os pacotes ICA Keep-Alive são enviados aos dispositivos do usuário a cada 60 segundos. Se um dispositivo de usuário não responder em 60 segundos, o status das sessões ICA muda para Desconectado.
- **ICA keep alives:** envia ou impede o envio de mensagens ICA keep-alive.

Controle do espaço de trabalho

O controle do espaço de trabalho permite que as áreas de trabalho e os aplicativos sigam um usuário de um dispositivo para outro. Essa capacidade de movimento permite que um usuário acesse todas as áreas de trabalho ou aplicativos abertos de qualquer lugar simplesmente fazendo logon, sem ter que reinicializar as áreas de trabalho ou aplicativos em cada dispositivo. Por exemplo, o controle do espaço de trabalho pode ajudar os profissionais de saúde em um hospital que precisam se mover rapidamente entre diferentes estações de trabalho e acessar o mesmo conjunto de aplicativos sempre que fazem logon. Se você configurar as opções de controle do espaço de trabalho para permitir isso, esses trabalhadores poderão se desconectar de vários aplicativos em um dispositivo cliente e se reconectar para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle do espaço de trabalho afeta as seguintes atividades:

- **Entrar:** por padrão, o controle do espaço de trabalho permite que os usuários se reconectem automaticamente a todas as áreas de trabalho e aplicativos em execução ao fazer logon, ignorando a necessidade de reabri-los manualmente. Por meio do controle do espaço de trabalho, os usuários podem abrir áreas de trabalho ou aplicativos desconectados, além de outros que estejas ativos em outro dispositivo cliente. Desconectar-se de uma área de trabalho ou aplicativo o mantém em execução no servidor. Se tiver usuários em roaming que devem manter algumas áreas de trabalho ou aplicativos em execução em um dispositivo cliente enquanto se reconectam a um subconjunto de suas áreas de trabalho ou aplicativos em outro dispositivo cliente, você pode configurar o comportamento de reconexão de logon para abrir somente as áreas de trabalho ou aplicativos das quais o usuário se desconectou anteriormente.
- **Reconexão:** depois de fazer logon no servidor, os usuários podem se reconectar a todas as áreas de trabalho ou aplicativos a qualquer momento clicando em Reconectar. Por padrão, Reconectar abre áreas de trabalho e aplicativos que estão desconectados, além dos que estão em execução no momento em outro dispositivo cliente. Você pode configurar Reconectar para abrir apenas as áreas de trabalho ou aplicativos das quais o usuário se desconectou anteriormente.
- **Sair:** para usuários que abrem áreas de trabalho ou aplicativos pelo StoreFront, você pode configurar o comando **Logoff** para desconectar o usuário do StoreFront e de todas as sessões ativas ou somente do StoreFront.
- **Desconexão:** os usuários podem se desconectar de todas as áreas de trabalho e aplicativos em execução de uma só vez, sem precisar se desconectar de cada um individualmente.

O controle do espaço de trabalho está disponível apenas para usuários do aplicativo Citrix Workspace que acessam áreas de trabalho e aplicativos por meio de uma conexão ao Citrix StoreFront. Por padrão, o controle do espaço de trabalho está desativado para sessões de área de trabalho virtual, mas está ativado para aplicativos hospedados. O compartilhamento de sessão não ocorre por padrão entre áreas de trabalho publicadas e aplicativos publicados executados dentro dessas áreas de trabalho.

As políticas de usuário, os mapeamentos de unidade e as configurações da impressora mudam adequadamente quando um usuário se move para um novo dispositivo cliente. Políticas e mapeamentos são aplicados de acordo com o dispositivo cliente onde o usuário está conectado à sessão. Por exemplo, um profissional de saúde faz logoff de um dispositivo na sala de emergência e, em seguida, faz logon em uma estação de trabalho no laboratório de raios-x. As políticas, os mapeamentos de impressoras e os mapeamentos de unidade apropriados para a sessão no laboratório de raios-x entram em vigor na inicialização da sessão.

Você pode personalizar quais impressoras aparecem para os usuários quando eles mudam de localização. Você também pode controlar se os usuários podem imprimir em impressoras locais, quanta largura de banda é consumida quando os usuários se conectam remotamente e outros aspectos de

suas experiências de impressão.

Para obter informações sobre como ativar e configurar o controle do espaço de trabalho para usuários, consulte a documentação do StoreFront.

Roaming de sessão

> **Nota:**
>
> As informações a seguir orientam você a configurar o roaming de sessão usando o PowerShell. Mas você pode usar o Web Studio em seu lugar. Para obter mais informações, consulte Gerenciar grupos de entrega.

Por padrão, as sessões se movem entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos ficam disponíveis nos dois dispositivos. Os aplicativos seguem, independentemente do dispositivo, ou se existem ou não sessões atuais. Muitas vezes, as impressoras e outros recursos atribuídos ao aplicativo também seguem.

Embora esse comportamento padrão ofereça muitas vantagens, talvez não seja ideal em todos os casos. Você pode impedir o roaming de sessão usando o SDK do PowerShell.

Exemplo 1: um profissional de medicina está usando dois dispositivos: preenchendo um formulário de seguro em um PC desktop e olhando as informações do paciente em um tablet.

- Se o roaming de sessão estiver ativado, os dois aplicativos aparecem nos dois dispositivos (um aplicativo iniciado em um dispositivo fica visível em todos os dispositivos em uso). Isso talvez não atenda aos requisitos de segurança.
- Se o roaming da sessão estiver desativado, o prontuário do paciente não aparece no PC desktop e o formulário de seguro não aparece no tablet.

Exemplo 2: um gerente de produção inicia um aplicativo no PC no escritório. O nome e o local do dispositivo determinam quais impressoras e outros recursos estão disponíveis para a sessão. Mais tarde, ele vai a um escritório no prédio ao lado para uma reunião que exigirá o uso de uma impressora.

- Se o roaming de sessão estiver ativado, o gerente de produção provavelmente não conseguirá acessar as impressoras perto da sala de reuniões, isso porque os aplicativos que ele iniciou anteriormente em seu escritório resultaram na atribuição de impressoras e outros recursos próximos àquele local.
- Se o roaming de sessão estiver desativado, e se ele fizer logon em uma máquina diferente (usando as mesmas credenciais), uma nova sessão é iniciada e impressoras e recursos próximos ficarão disponíveis.

Configurar roaming de sessão

Para configurar o roaming de sessão, use os seguintes cmdlets de regra de política de direito com a propriedade "SessionReconnection". Opcionalmente, você também pode especificar a propriedade "LeasingBehavior".

Para sessões da área de trabalho:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões do aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Always:** as sessões sempre fazem o roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.
- **DisconnectedOnly:** reconectar-se apenas às sessões que já estão desconectadas; caso contrário, iniciar uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente primeiro desconectando-os ou usando o controle do espaço de trabalho para fazer o roaming explicitamente.) Uma sessão conectada ativa de outro dispositivo cliente nunca é usada. Em vez disso, uma nova sessão é iniciada.
- **SameEndpointOnly:** um usuário obtém uma sessão exclusiva para cada dispositivo cliente que usa. Isso desativa completamente o roaming. Os usuários podem se reconectar somente ao mesmo dispositivo que foi usado anteriormente na sessão.

A propriedade "LeasingBehavior"é descrita abaixo.

Efeitos de outra configuração:

A desativação do roaming de sessão é afetada pelo limite de aplicativo **Allow only one instance of the application per user** nas propriedades do aplicativo no grupo de entrega.

- Se você desativar o roaming de sessão, desative a opção de limite de aplicativo "Allow only one instance of the application per user".
- Se você ativar o limite de aplicativo "Allow only one instance of the application per user", não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos.

Intervalo de logon

Se uma máquina virtual contendo um VDA de área de trabalho fechar antes que o processo de logon seja concluído, você pode alocar mais tempo ao processo. O padrão para a versão 7.6 e versões posteriores é 180 segundos (o padrão para as versões 7.0 a 7.5 é 90 segundos).

Na máquina (ou na imagem mestre usada em um catálogo de máquinas), defina a seguinte chave de registro:

Chave:`HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique um período em segundos, em formato decimal, no intervalo de 0 a 3600.

Se você alterar uma imagem mestre, atualize o catálogo.

Essa configuração se aplica apenas a VMs com VDAs de área de trabalho. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor.

Marcas

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Introdução

Marcas são cadeias de caracteres que identificam itens como máquinas, aplicativos, áreas de trabalho, grupos de entrega, grupos de aplicativos e políticas. Depois de criar uma marca e adicioná-la a um item, você pode personalizar certas operações para aplicá-las apenas a itens que têm uma marca especificada.

- Personalizar as exibições de pesquisa no Web Studio.

  Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma marca chamada “test”e adicione-a (aplique-a) aos aplicativos em questão. Agora você pode filtrar a pesquisa do Web Studio com a marca “test”.

- Publique aplicativos de um grupo de aplicativos ou áreas de trabalho específicas de um grupo de entrega, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Isso é chamado de *restrição de marca*.

  Com as restrições de marcas, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando nos custos associados com a implantação e gerenciamento de

mais máquinas. Uma restrição de marca pode ser considerada como uma subdivisão (ou partição) de máquinas em um grupo de entrega. Sua funcionalidade é semelhante, mas não idêntica, a worker groups em versões do XenApp anteriores à 7.x.

Usar um grupo de aplicativos ou áreas de trabalho com uma restrição de marca pode ser útil ao isolar um subconjunto de máquinas em um grupo de entrega para solucionar problemas.

- Programe reinicializações periódicas para um subconjunto de máquinas em um grupo de entrega.

  O uso de uma restrição de marca para máquinas permite que você use novos cmdlets do PowerShell para configurar várias programações de reinicialização para subconjuntos de máquinas em um grupo de entrega. Para obter exemplos e detalhes, consulte Gerenciar grupos de entrega.

- Adapte a aplicação (atribuição) das políticas Citrix a um subconjunto de máquinas em grupos de entrega, tipos de grupo de entrega ou UOs que tenham (ou não tenham) uma marca especificada.

  Por exemplo, se você quiser aplicar uma política Citrix apenas às estações de trabalho mais poderosas, adicione uma marca chamada "high power"a essas máquinas. Em seguida, na página **Assign Policy** do assistente de criação de política, selecione a marca e a caixa de seleção **Enable**. Você também pode adicionar uma marca a um grupo de entrega e aplicar uma política Citrix a esse grupo. Para obter detalhes, consulte Criar políticas.

Você pode aplicar marcas a:

- Máquinas
- Aplicativos
- Catálogos de máquinas (somente PowerShell; consulte Marcas em catálogos de máquinas)
- Grupos de entrega
- Grupos de aplicativos

Você pode configurar uma restrição de marca que pode ser configurada ao criar ou editar o seguinte no Web Studio:

- Uma área de trabalho em um grupo de entrega compartilhado
- Um grupo de aplicativos

Restrições de marcas para uma área de trabalho ou grupo de aplicativos

Uma restrição de marca envolve várias etapas:

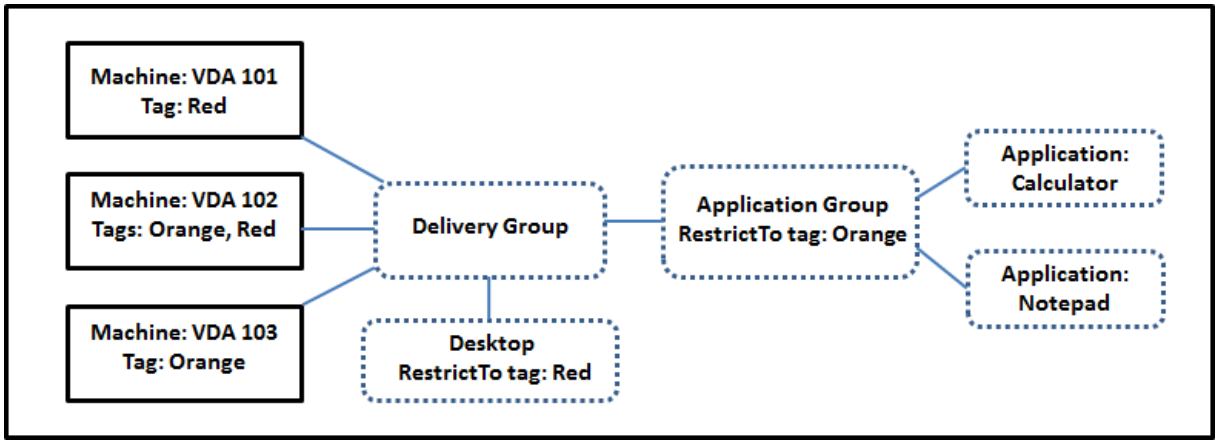
- Criar a marca e adicioná-la (aplicá-la) às máquinas.

- Criar ou editar um grupo com a restrição de marca (em outras palavras, "restringir inicializações em máquinas com a marca x").

Uma restrição de marca estende o processo de seleção da máquina do agente. O agente seleciona uma máquina de um grupo de entrega associado sujeito à política de acesso, listas de usuários configurados, preferência de zona e prontidão de inicialização, além da restrição de marca (se presente). Para aplicativos, o agente faz o fallback a outros grupos de entrega em ordem prioritária, aplicando as mesmas regras de seleção de máquina a cada grupo de entrega considerado.

Exemplo 1: layout simples

Este exemplo apresenta um layout simples que usa restrições de marca para limitar quais máquinas são consideradas para determinadas inicializações de áreas de trabalho e aplicativos. O site tem um grupo de entrega compartilhado, uma área de trabalho publicada e um grupo de aplicativos configurado com dois aplicativos.



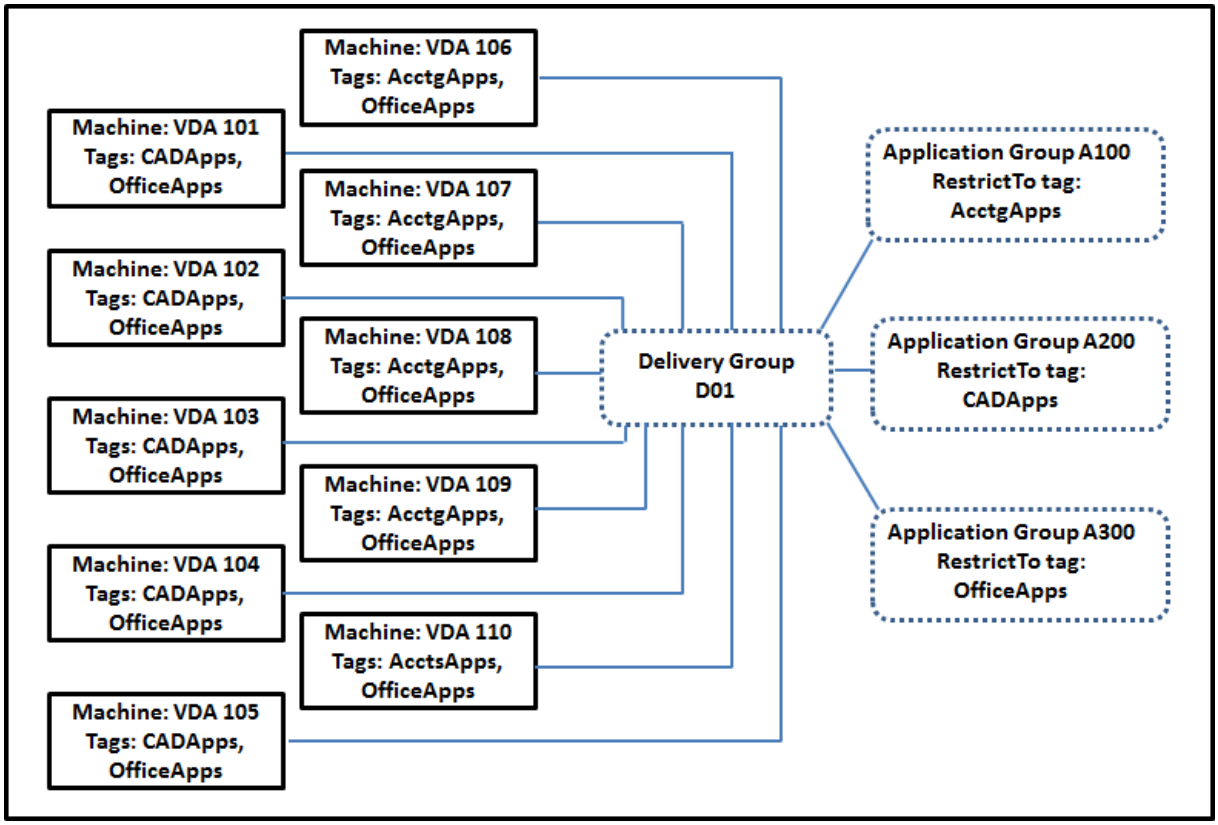
- As marcas foram adicionadas a cada uma das três máquinas (VDA 101—103).
- A área de trabalho no grupo de entrega compartilhado foi criada com uma restrição de marca chamada "Red". Uma área de trabalho só pode ser iniciada em máquinas desse grupo de entrega que tenham a marca "Red": VDA 101 e 102.
- O grupo de aplicativos foi criado com a restrição de marca "Orange", de modo que cada um de seus aplicativos (Calculadora e Bloco de Notas) só pode ser iniciado em máquinas desse grupo de entrega que tenham a marca "Orange": VDA 102 e 103.

A máquina VDA 102 tem as duas marcas (Red e Orange), por isso pode ser considerada para iniciar os aplicativos e a área de trabalho.

Exemplo 2: layout mais complexo

Este exemplo contém vários grupos de aplicativos que foram criados com restrições de marca. Isso resulta na capacidade de entregar mais aplicativos com menos máquinas do que seriam necessárias se você usasse apenas grupos de entrega.

Como configurar o exemplo 2 mostra as etapas usadas para criar e aplicar as marcas e depois configurar as restrições de marca no exemplo.



Esse exemplo usa 10 máquinas (VDA 101–110), um grupo de entrega (D01) e três grupos de aplicativos (A100, A200, A300). Ao aplicar marcas a cada máquina e especificar restrições de marca ao criar cada grupo de aplicativos:

- Os usuários de contabilidade no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 101—105)
- Os designers de CAD no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 106-110)
- Os usuários no grupo que precisam de aplicativos do Office podem acessar os aplicativos do Office em 10 máquinas (VDA 101–110)

Apenas 10 máquinas são usadas, com apenas um grupo de entrega. Usar apenas grupos de entrega (sem grupos de aplicativos) exigiria o dobro de máquinas, porque uma máquina pode pertencer a apenas um grupo de entrega.

Gerenciar marcas e restrições de marca

As marcas são criadas, adicionadas (aplicadas), editadas e excluídas dos itens selecionados por meio da ação **Manage Tags** no Web Studio.

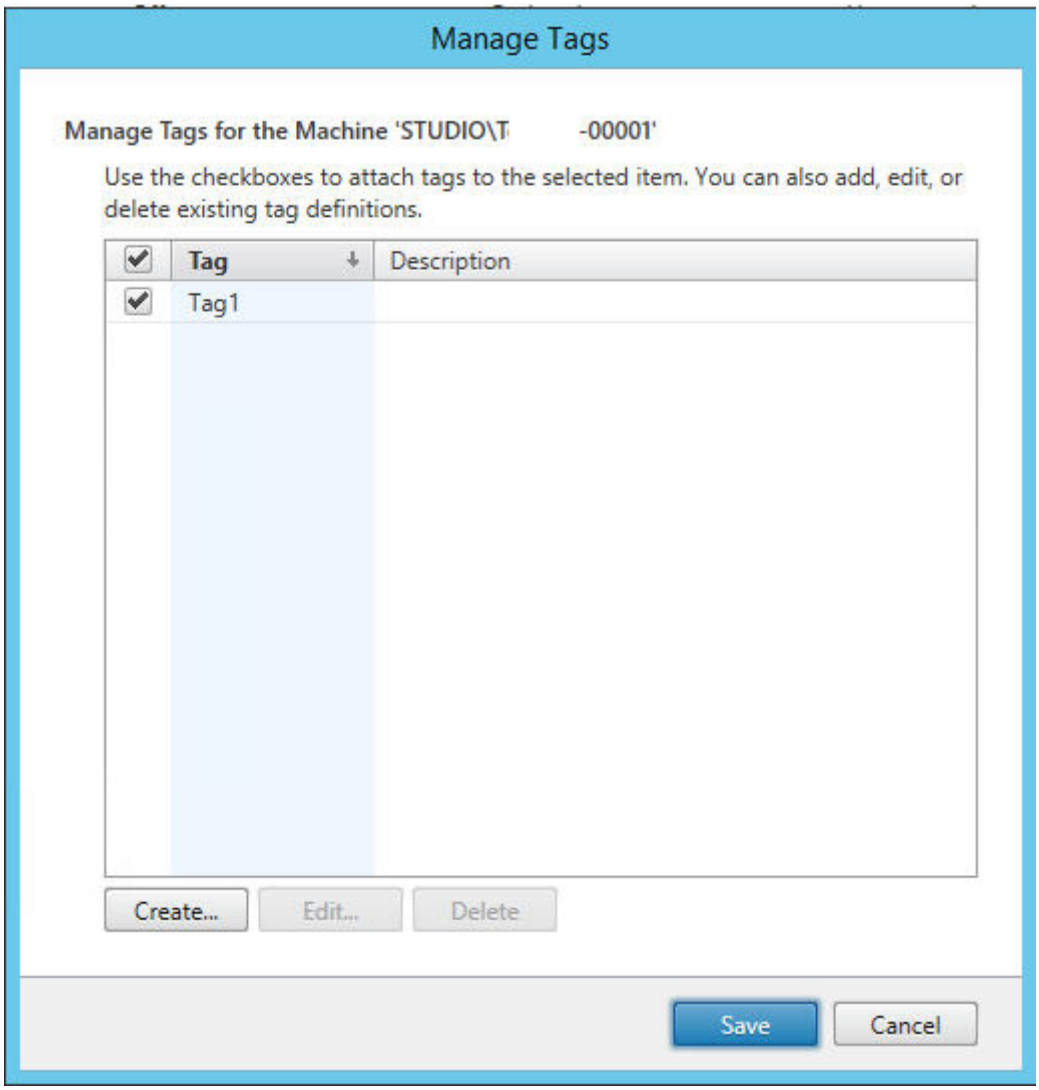
(Exceção: as marcas usadas para atribuições de política são criadas, editadas e excluídas por meio da ação **Manage Tags** no Web Studio. No entanto, as marcas são aplicadas (atribuídas) quando você cria a política. Consulte Criar políticas para obter detalhes.)

As restrições de marca são configuradas quando você cria ou edita áreas de trabalho em grupos de entrega e quando cria e edita grupos de aplicativos.

Usar a caixa de diálogo Manage Tags no Web Studio

No Web Studio, selecione os itens aos quais deseja aplicar uma marca (uma ou mais máquinas, aplicativos, uma área de trabalho, um grupo de entrega ou um grupo de aplicativos) e selecione **Manage Tags** na barra de ações. A caixa de diálogo lista todas as marcas que foram criadas no site, não apenas para os itens selecionados.

- Uma caixa de seleção contendo uma marca de seleção indica que a marca já foi adicionada aos itens selecionados. (Na captura de tela abaixo, a máquina selecionada tem a marca 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 marca adicionada.



As ações a seguir estão disponíveis na caixa de diálogo **Manage Tags**. Não deixe de consultar Cuidados ao trabalhar com tags.

- **Para criar uma marca:**

  Clique em **Create.** Insira um nome e uma descrição. O nome das marcas deve ser exclusivo, e não faz diferença entre maiúsculas e minúsculas. Em seguida, clique em **OK**. (Criar uma marca não a aplica automaticamente a itens selecionados. Use as caixas de seleção para aplicar a marca.)

- **Para adicionar (aplicar) uma ou mais marcas:**

  Ative a caixa de seleção ao lado do nome da marca. Se você selecionou vários itens e a caixa de seleção ao lado de uma marca contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a marca aplicada), alterá-lo para uma marca de seleção afeta todas as máquinas selecionadas.

Se você tentar adicionar uma marca a uma ou mais máquinas, e a marca estiver sendo usada como restrição em um grupo de aplicativos, receberá um aviso de que a ação pode resultar na disponibilização das máquinas para inicialização. Se é isso o que você quer, prossiga.

- **Para remover uma ou mais marcas:**

  Desmarque a caixa de seleção ao lado do nome da marca. Se você selecionou vários itens e a caixa de seleção ao lado de uma marca contém um hífen (indicando que alguns, mas não todos os itens selecionados já têm a marca aplicada), desmarcar a caixa de seleção remove a marca de todas as máquinas selecionadas.

  Se você tentar remover uma marca de uma máquina que está usando a marca como restrição, receberá um aviso de que a ação pode afetar quais máquinas são consideradas para inicialização. Se é isso o que você quer, prossiga.

- **Para editar uma marca:**

  Selecione uma marca e clique em **Edit**. Insira um novo nome e descrição. Você pode editar apenas uma marca de cada vez.

- **Para excluir uma ou mais marcas:**

  Selecione as marcas e clique em **Delete**. A caixa de diálogo Delete Tag indica quantos itens usam atualmente as marcas selecionadas (por exemplo, "2 machines"). Clique em um item para exibir mais informações. Por exemplo, clicar no item "2 machines"exibe o nome das duas máquinas que têm essa marca aplicada. Confirme se deseja excluir as marcas.

  Você não pode usar o Web Studio para excluir uma marca usada como restrição. Primeiro, edite o grupo de aplicativos e remova a restrição de marca ou selecione uma marca diferente.

Quando terminar de usar a caixa de diálogo **Manage Tags**, clique em **Save**.

Para ver se uma máquina tem marcas aplicadas: selecione **Delivery Groups** no painel esquerdo. Selecione um grupo de entrega no painel central e, em seguida, selecione **View Machines** na barra de ações. Selecione uma máquina no painel central e, em seguida, selecione a guia **Tags** no painel **Details**.

Gerenciar restrições de marca

Configurar uma restrição de marca é um processo de várias etapas: primeiro você cria a marca e a adiciona/aplica às máquinas. Em seguida, você adiciona a restrição ao grupo de aplicativos ou à área de trabalho.

- **Criar e aplicar uma marca:**

  Crie a marca e adicione-a (aplique-a) às máquinas afetadas pela restrição de marca, usando as ações **Manage Tags** descritas anteriormente.

- **Para adicionar uma restrição de marca a um grupo de aplicativos:**

  Crie ou edite o grupo de aplicativos. Na página **Delivery Groups**, selecione **Restrict launches to machines with the tag** e depois selecione a marca na lista.

- **Para alterar ou remover a restrição de marca em um grupo de aplicativos:**

  Edite o grupo. Na página **Delivery Groups**, selecione uma marca diferente na lista ou remova a restrição de marca completamente desmarcando **Restrict launches to machines with the tag**.

- **Para adicionar uma restrição de marca a uma área de trabalho:**

  Crie ou edite um grupo de entrega. Clique em **Add** ou **Edit** na página **Desktops**. Na caixa de diálogo Add Desktop, selecione **Restrict launches to machines with the tag** e depois selecione a marca (tag) no menu.

- **Para alterar ou remover a restrição de marca em um grupo de entrega:**

  Edite o grupo. Na página Desktops, clique em **Edit**. Na caixa de diálogo, selecione uma marca diferente nas listas ou remova a restrição de marca completamente desmarcando **Restrict launches to machines with the tag**.

Cuidados ao trabalhar com marcas

Uma marca aplicada a um item pode ser usada para diferentes propósitos, portanto, lembre-se de que adicionar, remover e excluir uma marca pode ter efeitos indesejados. Você pode usar uma marca para classificar as exibições da máquina no campo de pesquisa do Web Studio. Você pode usar a mesma marca como restrição ao configurar um grupo de aplicativos ou uma área de trabalho. A marca limita a consideração de inicialização a apenas máquinas em grupos de entrega especificados que tenham essa marca.

Quando você tenta adicionar uma marca a máquinas depois que marca é configurada como uma restrição de marca para uma área de trabalho ou um grupo de aplicativos, é exibido um aviso. Adicionar essa marca pode disponibilizar as máquinas para iniciar aplicativos ou áreas de trabalho adicionais. Se é isso o que você quer, prossiga. Caso contrário, você pode cancelar a operação.

Por exemplo, digamos que você crie um grupo de aplicativos com a restrição de marca "Red". Mais tarde, você adiciona várias outras máquinas nos mesmos grupos de entrega usados por esse grupo de aplicativos. Se você tentar adicionar a tag "Red"a essas máquinas, o Web Studio exibe uma mensagem com uma informação semelhante a: "A marca "Red"é usada como uma restrição nos seguintes grupos de aplicativos. Adicionar essa marca pode disponibilizar as máquinas selecionadas para iniciar aplicativos neste grupo de aplicativos."Você pode confirmar ou cancelar a adição da tag às máquinas adicionais.

Da mesma forma, se um grupo de aplicativos usar uma tag para restringir inicializações, o Web Studio avisa que você não pode excluir a marca até que tenha editado o grupo para removê-la como uma restrição. (Se você tiver permissão para excluir uma marca usada como restrição em um grupo de aplicativos, isso pode resultar na permissão de que os aplicativos podem ser iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição contra a exclusão de uma marca se aplica se a marca estiver sendo usada como uma restrição a inicializações de áreas de trabalho. Depois de editar o grupo de aplicativos ou áreas de trabalho no grupo de entrega para remover essa restrição de marca, você pode excluir a marca.

Nem todas as máquinas têm os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada qual com uma restrição de marca diferente e conjuntos diferentes ou sobrepostos de máquinas de grupos de entrega. A tabela a seguir ilustra como as considerações de máquina são decididas.

Quando um aplicativo é adicionado a	Estas máquinas nos grupos de entrega selecionados são consideradas para inicialização
Um grupo de aplicativos sem restrição de marca	Qualquer máquina.
Um grupo de aplicativos com restrição de marca A	Máquinas que têm a marca A aplicada.
Dois grupos de aplicativos, um com restrição de marca A e outro com restrição de marca B	Máquinas que têm a marca A e a marca B. Se nenhuma estiver disponível, as máquinas que têm a marca A ou a marca B.
Dois grupos de aplicativos, um com restrição de marca A e outro sem restrição de marca	Máquinas que têm a marca A. Se nenhuma estiver disponível, então qualquer máquina.

Se você usou uma restrição de marca em uma programação de reinicialização de máquina, quaisquer alterações feitas que afetem as aplicações ou restrições de marcas afetam o próximo ciclo de reinicialização da máquina. Isso não afeta nenhum ciclo de reinicialização que está em andamento enquanto as alterações estão sendo feitas.

Como configurar, exemplo 2

A sequência a seguir mostra as etapas para criar e aplicar marcas e depois configurar restrições de marca para os grupos de aplicativos ilustrados no segundo exemplo.

VDAs e aplicativos já foram instalados nas máquinas e o grupo de entrega foi criado.

Crie e aplique marcas às máquinas:

1. No Web Studio, selecione o grupo de entrega D01 e, em seguida, selecione **View Machines** na barra de ações.

2. Selecione as máquinas VDA 101–105 e, em seguida, selecione **Manage Tags** na barra de ações.
3. Na caixa de diálogo Manage Tags, clique em **Create** e, em seguida, crie uma marca chamada `CADApps`. Clique em **OK**.
4. Clique em **Create** novamente e crie uma marca chamada OfficeApps. Clique em **OK**.
5. Enquanto ainda estiver na caixa de diálogo **Manage Tags**, adicione (aplique) as marcas recém-criadas às máquinas selecionadas marcando as caixas de seleção ao lado do nome de cada marca (`CADApps` e `OfficeApps`). Quando terminar, feche a caixa de diálogo.
6. Selecione o grupo de entrega D01 e selecione **View Machines** na barra de ações.
7. Selecione as máquinas VDA 106–110 e, em seguida, selecione **Manage Tags** na barra de ações.
8. Na caixa de diálogo **Manage Tags**, clique em **Create**. Crie uma marca chamada `AcctgApps`. Clique em **OK**.
9. Aplique a marca `AcctgApps` recém-criada e a marca `OfficeApps` às máquinas selecionadas clicando nas caixas de seleção ao lado do nome de cada marca; feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de marca.

1. No Web Studio, selecione **Applications** no painel esquerdo, selecione a guia **Application Groups** e selecione **Create Application Group** na barra de 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 depois selecione a marca `AcctgApps` na lista.
3. Conclua o assistente, especificando os usuários de contabilidade e os aplicativos de contabilidade. (Ao adicionar o aplicativo, escolha a origem **From Start menu**, que procura o aplicativo nas máquinas que têm a marca `AcctgApps`.) Na página **Summary**, dê o nome `A100` ao grupo.
4. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando máquinas com a marca `CADApps`, além dos usuários e aplicativos apropriados.
5. Repita as etapas para criar o grupo de aplicativos `A300`, especificando máquinas com a marca `OfficeApps`, além dos usuários e aplicativos apropriados.

Marcas em catálogos de máquinas

Você pode usar marcas em catálogos de máquinas. A sequência geral de criação de uma marca e da aplicação dela a um catálogo é a mesma descrita anteriormente. No entanto, a aplicação de marcas a catálogos é suportada somente por meio da interface do PowerShell. Não é possível usar o Web Studio para aplicar uma marca a um catálogo ou remover uma marca de um catálogo. As exibições de catálogos no Web Studio não indicam se uma marca está aplicada.

Resumindo: você pode usar o Web Studio ou o PowerShell para criar ou excluir uma marca para uso em um catálogo. Para aplicar a marca ao catálogo, use o PowerShell.

Aqui estão alguns exemplos de uso de marcas com catálogos:

- Um grupo de entrega tem máquinas de vários catálogos, mas você quer que uma operação (como uma programação de reinicialização) afete apenas as máquinas em um catálogo específico. Aplicar uma marca a esse catálogo atende ao seu requisito.
- Em um grupo de aplicativos, você quer limitar as sessões de aplicativos a máquinas em um catálogo específico. Aplicar uma marca a esse catálogo atende ao seu requisito.

Cmdlets do PowerShell afetados:

- Você pode passar objetos de catálogo para cmdlets como `Add-BrokerTag` e `Remove-BrokerTag`.
- `Get-BrokerTagUsage` mostra quantos catálogos contêm marcas.
- `Get-BrokerCatalog` tem uma propriedade chamada `Tags`.

Por exemplo, os cmdlets a seguir adicionam uma tag chamada `fy2018` ao catálogo chamado `acctg`:
`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (A marca foi criada anteriormente usando Web Studio ou PowerShell.)

Consulte a ajuda do cmdlet do PowerShell para obter mais orientação e sintaxe.

Mais informações

Postagem do blog: How to assign desktops to specific servers.

Utilizar a pesquisa no Studio

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Use o recurso de pesquisa Search para exibir informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou grupos de entrega específicos. Depois de selecionar **Search** no Web Studio, você tem várias opções:

- Use guias para listar máquinas por tipo (SO de sessão única ou multissessão) ou listar todas as sessões.

- Digite o nome na caixa de pesquisa.
- Selecione o ícone de filtro para realizar uma pesquisa avançada. Selecione a seta para baixo para exibir uma lista de propriedades de pesquisa. Selecione o sinal de mais para criar uma expressão a partir das propriedades na lista.

Para salvar sua pesquisa, selecione o ícone de reticências (…) e selecione **Save As**. A pesquisa aparece na lista **Saved searches**. (Para acessar a lista, selecione a caixa de pesquisa.) Para excluir pesquisas salvas, selecione a caixa de pesquisa e selecione **Clear**.

Quando você usa filtros para realizar uma pesquisa avançada, a janela **Add filters** aparece em primeiro plano, deixando a exibição em segundo plano inalterada. Depois de selecionar **Search**, os resultados correspondentes da pesquisa são exibidos, com os critérios de filtro ao lado de **Filter**. Quando você fecha a janela **Add filters**, os resultados permanecem. Para limpar os filtros, selecione o ícone X ao lado dos critérios do filtro.

Pesquisar catálogos de máquinas ou grupos de entrega

Não é possível realizar pesquisas no nó **Machine Catalogs** ou **Delivery Groups** porque a caixa Search não está disponível. Em vez disso, use o nó **Search** para pesquisar catálogos de máquinas ou grupos de entrega. No nó **Search**, selecione o ícone de filtro, adicione filtros da seguinte forma e selecione **Search**.

Para mostrar mais critérios de pesquisa na tela, selecione o sinal de mais. Remova os critérios de pesquisa selecionando o ícone da lixeira.

Personalizar colunas para exibir

Ao personalizar colunas, você pode ver as colunas marcadas com o rótulo **Degrades performance**. Selecionar essas colunas pode prejudicar o desempenho do console. Depois de concluir a personalização, a tabela é atualizada para exibir as colunas selecionadas. A presença delas pode resultar em atrasos quando você atualizar a tabela.

Se a personalização contiver colunas que degradam o desempenho, você será solicitado a determinar se deseja preservá-las. O aviso aparece depois que você atualiza a janela do navegador ou sai do console e volta a fazer login. Esteja ciente das seguintes considerações se decidir preservar as colunas:

- Para garantir o desempenho do console, você não pode atualizar a tabela mais de uma vez por minuto. Essa restrição se aplica a todas as guias: **Single-session OS Machines**, **Multi-session OS Machines** e **Sessions**. Se você precisar de atualizações mais frequentes, remova todas as colunas que prejudicam o desempenho.

Exportar resultados da pesquisa para um arquivo CSV

Você pode exportar os resultados da pesquisa (até 10.000 itens) para um arquivo CSV. O arquivo é salvo no local de download padrão do seu navegador.

Esse recurso está disponível para máquinas e sessões. Para exportar os resultados da pesquisa, clique no ícone de exportação no canto superior direito. A exportação pode levar até 1 minuto para ser concluída.

Não é possível realizar outra exportação nas guias do nó Search enquanto uma exportação estiver em andamento.

Dicas para aprimorar uma pesquisa

Considere as dicas a seguir ao usar o recurso de pesquisa:

- No nó **Search**, selecione qualquer coluna para classificar os itens.
- Para mostrar mais características para incluir na exibição em que você pode pesquisar e classificar, selecione **Columns to Display** ou clique em qualquer coluna e selecione **Columns to Display**. Na janela **Columns to Display**, marque a caixa de seleção ao lado dos itens que deseja exibir e selecione **Save** para sair.

  > **Nota:**
  >
  > Os itens que degradam o desempenho são marcados com o rótulo **Degrades performance**.

- Para localizar um dispositivo de usuário conectado a uma máquina, use **Client (IP)** e **Is** e insira o endereço IP do dispositivo.
- Para localizar sessões ativas, use **Session State**, **Is** e **Connected**.
- Para listar todas as máquinas em um grupo de entrega, selecione **Delivery Groups** no painel esquerdo. Selecione o grupo e, em seguida, selecione **View Machines** na barra de ações ou no menu de contexto.

Tenha em mente as seguintes considerações ao realizar operações de classificação:

- Contanto que o número de itens não exceda 5.000, você pode clicar em qualquer coluna para classificar os itens nela. Quando o número excede 5.000, você pode classificar apenas por nome ou por usuário atual (dependendo da guia em que você está). Para ativar a classificação, use filtros para reduzir o número de itens para 5.000 ou menos.
- Quando o número de itens for maior que 500, mas não superior a 5.000:

- Armazenamos todos os dados localmente em cache para melhorar o desempenho da classificação. Nas guias **Single-session OS Machines** e **Multi-session OS Machines**, armazenamos os dados em cache a primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Name**) para classificar. Na guia **Sessions**, armazenamos os dados em cache a primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Current User**) para classificar. Como resultado, a classificação leva mais tempo para ser concluída. Para um desempenho mais rápido, classifique por nome ou usuário atual ou use filtros para reduzir o número de itens.
- A seguinte mensagem abaixo da tabela indica que os dados estão armazenados em cache: Last refreshed: <the time when you refreshed the table>. Nesse caso, as operações de classificação são baseadas em itens que foram carregados anteriormente. Esses itens podem não estar atualizados. Para atualizá-los, clique no ícone de atualização.

Configurações

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

Você pode usar o Web Studio para gerenciar essas configurações:

- Citrix Customer Experience Improvement Program
- Remover Delivery Controllers
- Alterar o banco de dados de log
- Definir data e hora
- Habilitar a atribuição automática de vários usuários para o acesso ao PC remoto
- Habilitar a resolução de DNS
- Habilitar a confiança em XML
- Gerenciar chave de segurança

Configurar o fuso horário

Para personalizar o formato de data e hora de acordo com suas preferências, siga estas etapas:

1. Entre no Web Studio e selecione **Settings** no painel esquerdo.
2. Localize o bloco **Date and time** e clique em **Edit** para configurar as seguintes opções:
    - **Time format:**
        - Selecione para exibir a hora usando um relógio de 12 horas (9 da noite, por exemplo) ou um relógio de 24 horas (21h, por exemplo).
    - **Date format:**
        - Configure o formato de data para corresponder às suas preferências, por exemplo, aaaa/MM/dd.
    - **Time zone:**
        - **UTC:** exibe a data e a hora em UTC em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações no seu fuso horário local.
        - **Local time zone:** exiba a data e a hora no seu fuso horário local em toda a interface do usuário. Passar o mouse sobre a data e a hora exibe as informações em UTC.

Habilitar a resolução de DNS

Para apresentar nomes de DNS em vez de endereços IP no arquivo ICA, siga estas etapas:

1. Entre no Web Studio e selecione **Settings** no painel esquerdo.
2. Ative a configuração **Enable DNS resolution**.

Perfis de usuário

June 28, 2023

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 diferentes necessidades de seus usuários, você pode usar as políticas do Citrix Virtual Apps and Desktops para aplicar um comportamento de perfil diferente às máquinas em cada grupo de entrega. Por exemplo, um grupo de entrega pode exigir perfis obrigatórios da Citrix, cujo modelo

está armazenado em um local de rede, enquanto outro grupo de entrega requer perfis de roaming da Citrix armazenados em outro local com várias pastas redirecionadas.

- Se outros administradores da sua organização forem responsáveis pelas políticas do Citrix Virtual Apps and Desktops, confirme com eles para garantir que definam as políticas relacionadas ao perfil para todos os seus grupos de entrega.
- As políticas de Profile Management também podem ser definidas na política de grupo, no arquivo .ini do Profile Management, e localmente, em máquinas virtuais individuais. Essas várias formas de definir o comportamento do perfil são lidas na seguinte ordem:

  1. Política de Grupo (arquivos .adm ou .admx)
  2. Políticas do Citrix Virtual Apps and Desktops no nó Política
  3. Políticas locais na máquina virtual à qual o usuário se conecta
  4. Arquivo .ini do Profile Management

  Por exemplo, se você configurar a mesma política na Política de Grupo e no nó Política, o sistema lê a configuração da política na Política de Grupo e ignora a configuração da política do Citrix Virtual Apps and Desktops.

Seja qual for 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 feitas no Studio, define os padrões do Profile Management de acordo.

As políticas que o Profile Management ajusta são mostradas na tabela a seguir. Todas as configurações de política não padrão são preservadas; elas não são substituídas por esse 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 principais fatores são se as máquinas são persistentes ou provisionadas e se elas são compartilhadas por vários usuários ou dedicadas a apenas um usuário.

Os sistemas persistentes têm um tipo de armazenamento local, cujo conteúdo é mantido quando o sistema desliga. Sistemas persistentes podem empregar uma tecnologia de armazenamento, como SANs, para simular um disco local. Em contraste, os sistemas provisionados são criados "dinamicamente"a partir de um disco base e um tipo de disco de identidade. O armazenamento local geralmente é simulado por um disco RAM ou disco de rede, este último geralmente fornecido por uma SAN com um link de alta velocidade. A tecnologia de provisionamento geralmente é o Citrix Provisioning

ou Machine Creation Services (ou um produto equivalente de terceiros). Às vezes, os sistemas provisionados têm armazenamento local persistente. Esses são classificados como persistentes.

Juntos, esses dois fatores definem os seguintes tipos de máquina:

- **Persistente e dedicada**. Por exemplo, máquinas com SO de sessão única com uma atribuição estática e armazenamento local persistente que são criadas com Machine Creation Services, estações de trabalho físicas e laptops.
- **Persistente e compartilhada**. Por exemplo, máquinas com SO multissessão criadas com o Machine Creation Services e servidores Citrix Virtual Apps.
- **Provisionada e dedicada**. Por exemplo, máquinas com SO de sessão única com uma atribuição estática, mas sem armazenamento persistente, criadas com Citrix Provisioning Service (no Citrix Virtual Desktops).
- **Provisionada e compartilhada**. Por exemplo, máquinas com SO de sessão única com uma atribuição aleatória criadas com o Citrix Provisioning Service (no Citrix Virtual Desktops) e servidores Citrix Virtual Apps.

As seguintes configurações de política do Profile Management são sugestões para os diferentes tipos de máquinas. Elas funcionam bem na maioria dos casos, mas você pode se desviar delas de acordo com a sua implantação.

> **Importante:**
>
> **Delete locally cached profiles on logoff**, **Profile streaming** e **Always cache** são impostas pelo recurso de configuração automática. Ajuste as outras políticas manualmente.

Máquinas persistentes

Política	Persistente e dedicada	Persistente e compartilhada
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Ativado (nota 1)	Desativado (nota 2)
Active write back	Disabled	Desativado (nota 3)
Process logons of local administrators	Enabled	Desativado (nota 4)

Máquinas provisionadas

Política	Provisionada e dedicada	Provisionada e compartilhada
Delete locally cached profiles on logoff	Desativado (nota 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Desativado (nota 6)	Disabled
Active write back	Enabled	Enabled
Process logons of local administrators	Enabled	Ativado (nota 7)

1. Como **Profile streaming** está desativado para este tipo de máquina, a configuração **Always cache** é sempre ignorada.
2. Desative **Always cache**. No entanto, você pode garantir que arquivos grandes sejam carregados em perfis o mais rápido possível após o logon, ativando essa 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 **Active write back**, exceto para salvar alterações nos perfis de usuários que fazem roaming entre os servidores do Citrix Virtual Apps. Nesse caso, ative a política.
4. Desative **Process logons of local administrators** exceto para áreas de trabalho compartilhadas hospedadas. Nesse caso, ative a política.
5. Desative **Delete locally cached profiles on logoff**. Essa configuração retém perfis armazenados localmente em cache. Como as máquinas são redefinidas no logoff, mas estão atribuídas a usuários individuais, os logons são mais rápidos se seus perfis estiverem armazenados em cache.
6. Desative **Always cache**. No entanto, você pode garantir que arquivos grandes sejam carregados em perfis o mais rápido possível após o logon, ativando essa 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 **Process logons of local administrators**, exceto para perfis de usuários que fazem roaming entre servidores do Citrix Virtual Apps and Desktops. Nesse caso, desative a política.

Redirecionamento de pastas

O redirecionamento de pastas permite armazenar dados do usuário em compartilhamentos de rede diferentes do local onde os perfis são armazenados. O redirecionamento de pastas reduz o tamanho do perfil e o tempo de carregamento, mas pode afetar a largura de banda da rede. O redirecionamento de pastas não requer o emprego dos perfis de usuário Citrix. Você pode optar por gerenciar perfis de usuário por conta própria e ainda assim redirecionar pastas.

Configure o redirecionamento de pastas usando as 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 de localização foram validadas.
- As pastas redirecionadas estão configuradas na rede e seu conteúdo preenchido a partir da área de trabalho virtual dos usuários no logon.

Configure o redirecionamento das pastas usando apenas políticas da Citrix ou objetos de política de grupo do Active Directory, não os dois métodos. Configurar o redirecionamento de pastas usando os dois mecanismos de política pode resultar em um comportamento imprevisível.

Redirecionamento avançado de pastas

Em implantações com vários sistemas operacionais (SO), digamos que você queira que alguns dos perfis de um usuário sejam compartilhados por cada SO. O restante do perfil não é compartilhado e é usado apenas por um sistema operacional. Para garantir uma experiência de usuário consistente nos sistemas operacionais, você precisa de uma configuração diferente para cada sistema operacional, ou seja, o redirecionamento avançado de pastas. Por exemplo, diferentes versões de um aplicativo em execução em dois sistemas operacionais precisam ler ou editar um arquivo compartilhado; assim você decide redirecioná-lo para um mesmo local de rede onde as duas versões podem acessá-lo. Alternativamente, como o conteúdo da pasta **Menu Iniciar** é estruturado de forma diferente nos dois sistemas operacionais, você decide redirecionar apenas uma pasta, não as duas. Essa abordagem separa a pasta **Menu Iniciar** e seu conteúdo em cada SO, garantindo uma experiência consistente para os usuários.

Se a sua implantação exigir redirecionamento avançado de pastas, você deve conhecer a estrutura dos dados de perfil de seus usuários e determinar quais partes podem ser compartilhadas entre os sistemas operacionais. A menos que o redirecionamento de pastas seja usado corretamente, podem ocorrer comportamentos imprevisíveis.

Para redirecionar pastas em implantações avançadas:

- Use um grupo de entrega separado para cada SO.
- Saiba onde seus aplicativos virtuais, incluindo aqueles em áreas de trabalho virtuais, armazenam dados e configurações do usuário e entenda como os dados estão estruturados.
- Para dados de perfil compartilhados que podem fazer roaming com segurança (porque estão estruturados de forma idêntica em cada SO), redirecione as pastas contidas em cada grupo de entrega.
- Para dados de perfil não compartilhados que não podem fazer roaming, redirecione a pasta contendo apenas um dos grupos de área de trabalho, normalmente aquele com o SO mais usado

ou aquele em que os dados são mais relevantes. Como alternativa, para dados não compartilhados que não podem fazer roaming entre sistemas operacionais, redirecione as pastas contidas nos dois sistemas para locais de rede separados.

Exemplo de implantação avançada

A implantação tem aplicativos, incluindo versões do Microsoft Outlook e do Internet Explorer, em execução em áreas de trabalho e aplicativos do Windows 10, incluindo outras versões do Outlook e do Internet Explorer, entregues pelo Windows Server 2019. Você já configurou dois grupos de entrega para os dois sistemas operacionais. Os usuários desejam acessar os mesmos dados de **Contatos** e **Favoritos** nas duas versões dos dois aplicativos.

Importante: as decisões e sugestões a seguir são válidas para os sistemas operacionais e a implantação descritos. Na sua organização, as pastas que você opta por redirecionar e a decisão de compartilhá-las dependem de vários fatores que são únicos à sua implantação específica.

- Usando políticas aplicadas aos grupos de entrega, você escolhe as seguintes pastas para redirecionar.

Pasta	Redirecionada em Windows 10?	Redirecionada em Windows Server 2019?
Meus Documentos	Sim	Sim
Dados do Aplicativos	Não	Não
Contatos	Sim	Sim
Área de Trabalho	Sim	Não
Downloads	Não	Não
Favoritos	Sim	Sim
Links	Sim	Não
Minhas Músicas	Sim	Sim
Minhas Imagens	Sim	Sim
Meus Vídeos	Sim	Sim
Pesquisas	Sim	Não
Jogos Salvos	Não	Não
Menu Iniciar	Sim	Não

- Para as pastas compartilhadas e redirecionadas:

  - Depois de analisar a estrutura dos dados salvos pelas diferentes versões do Outlook e do Internet Explorer, você decide que é seguro compartilhar as pastas **Contatos** e **Favoritos**.
  - Você sabe que a estrutura das pastas **Meus Documentos**, **Minhas Músicas**, **Minhas Imagens** e **Meus Vídeos** é padrão em todos os sistemas operacionais. Portanto, é seguro armazenar essas pastas no mesmo local de rede para cada grupo de entrega.

- Para as pastas não compartilhadas e redirecionadas:

  - Você não redireciona a pasta 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. Consequentemente, não podem ser compartilhados.
  - Para garantir o 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, nesse caso, os dados não compartilhados são mais relevantes para um ambiente de área de trabalho do que para um ambiente de aplicativo. Por exemplo, os atalhos da área de trabalho são armazenados na pasta **Área de Trabalho** e podem ser úteis se forem originários de um computador com Windows 10, mas não de um computador com Windows Server.

- Para as pastas não redirecionadas:

  - Você não quer sobrecarregar seus servidores com arquivos baixados pelos usuários, então opta por não redirecionar a pasta Downloads.
  - Dados de aplicativos individuais podem causar problemas de compatibilidade e desempenho, assim você decide não redirecionar a pasta Dados de Aplicativos.

Para obter mais informações sobre redirecionamento de pastas, consulte Visão geral de redirecionamento de pastas, arquivos offline e perfis de usuário móvel.

Redirecionamento de pastas e exclusões

No Citrix Profile Management (mas não no Studio), um aprimoramento de desempenho permite que você evite 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 de pastas de perfil e preserve a integridade dos dados se você decidir posteriormente que não quer redirecioná-los. Para obter mais informações sobre exclusões, consulte Incluir e excluir itens.

Registro de VDA

April 3, 2024

Introdução

> **Nota:**
>
> Em um ambiente local, os VDAs se registram em um Delivery Controller. Em um ambiente de serviço do Citrix Cloud, os VDAs se registram em um Cloud Connector. Em um ambiente híbrido, alguns VDAs se registram em um Delivery Controller, enquanto outros se registram em um Cloud Connector.

Antes que um VDA possa ser usado, ele deve se registrar (estabelecer comunicação) em um ou mais Controllers ou Cloud Connectors no site. O VDA encontra um Controller ou Connector consultando uma lista chamada `ListofDDCs`. A `ListOfDDCs` em um VDA contém entradas DNS que apontam o VDA a Controllers ou Cloud Connectors no site. Para o balanceamento de carga, o VDA distribui automaticamente conexões entre todos os Controllers ou Cloud Connectors na lista.

Por que o registro de VDA é tão importante?

- Do ponto de vista da segurança, o registro é uma operação confidencial. Você está estabelecendo uma conexão entre o Controller ou o Cloud Connector e o VDA. Por ser uma operação tão sigilosa, o comportamento esperado é rejeitar a conexão se algo 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, portanto, problemas de sincronização de horário e associação de domínio são inevitáveis. O Kerberos usa nomes de entidade de serviço (SPN), portanto, você não pode usar IP ou nome de host com balanceamento de carga.
- Se um VDA não tiver informações precisas e atuais do Controller ou do Cloud Connector à medida que você adiciona e remove Controllers (ou Cloud Connectors), o VDA rejeitará inicializações de sessão que sejam intermediadas por um Controller ou Cloud Connector que não esteja listado. Entradas inválidas podem atrasar a inicialização do software do sistema de área de trabalho virtual. Um VDA não aceitará uma conexão de um Controller ou Cloud Connector desconhecido e não confiável.

Além da `ListofDDCs`, a `ListOfSIDs` (IDs de segurança) indica quais máquinas na `ListofDDCs` são confiáveis. A `ListofSIDs` pode ser usada para diminuir a carga no Active Directory ou para evitar possíveis ameaças de segurança de um servidor DNS comprometido. Para obter mais informações, consulte ListOfSIDs.

Se uma `ListofDDCs` especificar mais de um Controller ou Cloud Connector, o VDA tentará se conectar a eles em ordem aleatória. Em uma implantação local, a `ListofDDCs` também pode conter grupos de Controllers. O VDA tenta se conectar a cada Controller em um grupo antes de se mover para outras entradas na `ListofDDCs`.

O Citrix Virtual Apps and Desktops testa automaticamente a conectividade com Controllers ou Cloud Connectors configurados durante a instalação do VDA. São exibidos erros se um Controller ou Cloud Connector não puder ser acessado. Se você ignorar um aviso de que um Controller ou Cloud Connector não pode ser contatado (ou quando você não especifica os endereços do Controller ou do Cloud Connector durante a instalação do VDA), serão exibidas novas mensagens.

Métodos para configurar endereços do 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 do cache local, a menos que uma alteração de configuração seja detectada.

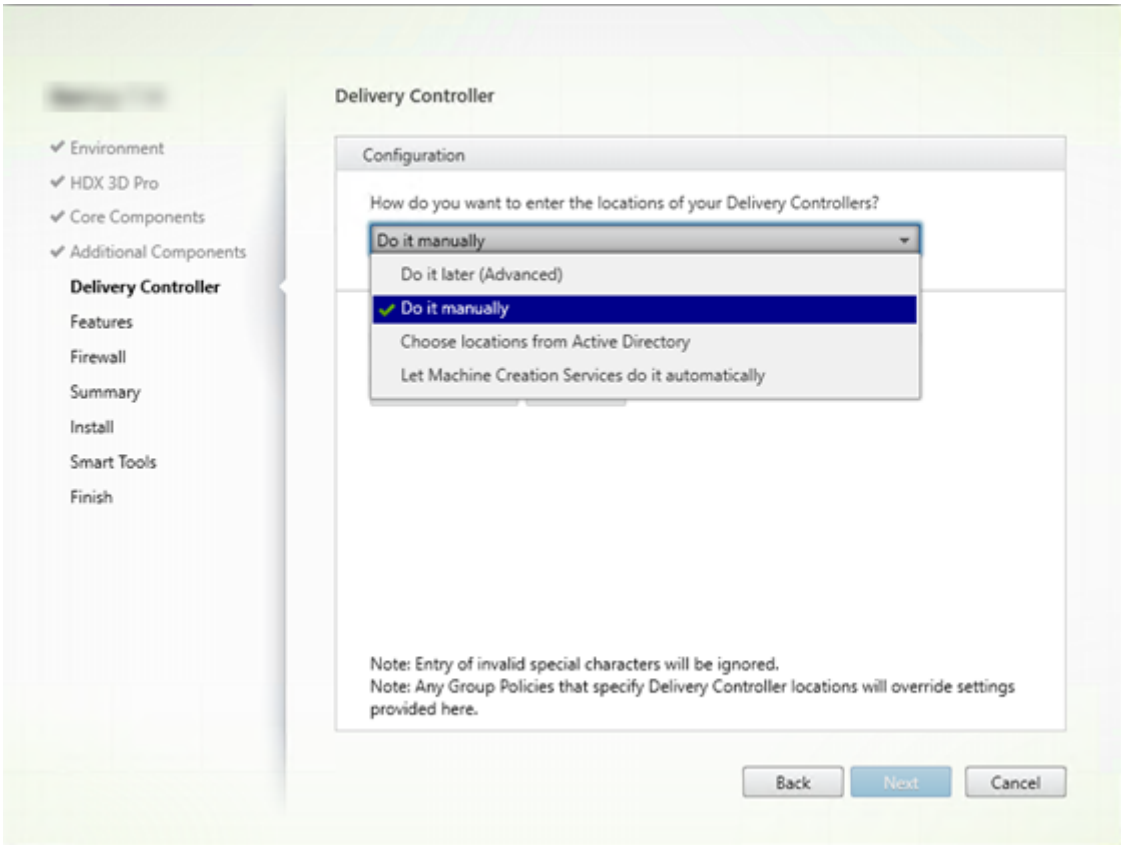
A maneira mais fácil de recuperar a lista durante os registros subsequentes é usando o recurso de atualização automática. A atualização automática está ativada por padrão. Para obter mais informações, consulte Atualização automática.

Existem vários métodos para configurar os endereços do 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 unidade organizacional 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 o uso de GPO para o registro inicial do VDA. Ele tem a maior prioridade. (Embora a atualização automática esteja listada como a prioridade mais alta, a atualização automática é usada somente após o registro inicial.) O registro baseado em política oferece a vantagem de centralizar o uso da Política de Grupo na configuração.

Para especificar esse método, realize as duas etapas a seguir:

- Na página **Delivery Controller** no assistente de instalação do VDA, selecione **Do it later (advanced)**. O assistente solicita várias vezes que você especifique os endereços do Controller, mesmo que você não os esteja especificando durante a instalação do VDA. (O registro do VDA é muito importante.)
- Ative ou desative o registro do VDA baseado em política através da política da Citrix com o parâmetro `Virtual Delivery Agent Settings > Controllers`. (Se a segurança for sua maior prioridade, use o parâmetro `Virtual Delivery Agent Settings > Controller SIDs`.)

Esta configuração é armazenada em `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

Baseado em registro

Para especificar esse método, realize uma das etapas a seguir:

- Na página **Delivery Controller** no assistente de instalação do VDA, selecione **Do it manually**. Insira o FQDN de um Controller instalado e clique em **Add**. Se você instalou mais Controllers, adicione seus endereços.
- Para uma instalação de VDA por linha de comando, use a opção /controllers e especifique o FQDNs dos Controllers ou Cloud Connectors instalados.

Essas informações são armazenadas no valor do registro `ListOfDDCs` sob a chave do registro `HKLM\Software\Citrix\VirtualDesktopAgent` ou `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

Você também pode configurar essa 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 o processamento condicional de diferentes Controllers ou Cloud Connectors, como, por exemplo, usar XDC-001 para nomes de computadores que começam com XDW-001-).

Atualize a chave do registro `ListOfDDCs`, que lista os FQDNs de todos os Controllers ou Cloud Connectors no site. (Esta chave é o equivalente à unidade organizacional (UO) do site do Active Directory.)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs` (`REG_SZ`)

Se o local do registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` contém as chaves `ListOfDDCs` e `FarmGUID`, `ListOfDDCs` é usado para a descoberta do Controller ou do Cloud Connector. `FarmGUID` estará presente se uma UO do site foi especificada durante a instalação do VDA. (Isso pode ser usado em implantações legadas.)

Opcionalmente, atualize a chave do registro `ListOfSIDs` (para obter mais informações, consulte ListOfSIDs:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (`REG_SZ`)

Lembre-se: se você também ativar o registro de VDA baseado em política através da política da Citrix, isso substituirá as configurações especificadas durante a instalação do VDA, pois esse é o método de maior prioridade.

Baseado em UO do Active Directory (legado)

Este método é suportado principalmente para compatibilidade com versões anteriores, não sendo recomendado. Se você ainda estiver usando, a Citrix sugere mudar para outro método.

Para especificar esse método, realize as duas etapas a seguir:

- Na página **Delivery Controller** no assistente de instalação do VDA, selecione **Choose locations from 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 UO correta. Esse parâmetro pode ser configurado usando a Política de Grupo.

Baseado em MCS

Se você usa o MCS para provisionar VMs, o MCS configura a lista de Controllers ou Cloud Connectors. Esse recurso funciona com a atualização automática. Ao criar o catálogo, o MCS injeta a lista de Controllers ou Cloud Connectors no arquivo `Personality.ini` durante o provisionamento inicial. A atualização automática mantém a lista em dia.

Para especificar esse método, na página **Delivery Controller** no assistente de instalação do VDA, selecione **Let Machine Creation Services do it**.

Revisão e recomendações

Como prática recomendada:

- Use o método de registro da política de grupo para o registro inicial.
- Use a atualização automática (ativada por padrão) para manter a sua lista de Controllers atualizada.
- Em uma implantação de várias zonas, use a Política de Grupo para a configuração inicial (com pelo menos dois Controllers ou Cloud Connectors). Aponte VDAs para Controllers ou Cloud Connectors locais, para dentro de suas zonas. Use a atualização automática para mantê-los atualizados. A atualização automática otimiza automaticamente a `ListofDDCs` para VDAs em zonas satélite.
- Inclua mais de um controlador na chave do registro `ListOfDDCs`, separado por um espaço ou vírgula, para evitar problemas de registro se um Controller não estiver disponível. Por exemplo:

```
1  DDC7x.xd.local DDC7xHA.xd.local
2
3  32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
       ListOfDDCs
4
5  HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
       ListOfDDCs (REG_SZ)
6  <!--NeedCopy-->
```


- Assegure-se de que todos os valores listados em `ListofDDCs` mapeiam 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 ativada por padrão. É o método mais eficiente para manter seus registros de VDA atualizados. Embora não seja usado para o registro inicial, o software de atualização automática baixa e armazena a `ListofDDCs` em um cache persistente no VDA quando o registro inicial ocorre. Esse processo é feito para cada VDA. O cache também contém informações da política da máquina, o que garante que as configurações da política sejam mantidas em todas as reinicializações.

A atualização automática é suportada usando o MCS ou o 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:

- Ative ou desative a atualização automática através de uma política da Citrix contendo o parâmetro `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`. Essa configuração é ativada por padrão.

Como funciona:

- Cada vez que um VDA se registra novamente (por exemplo, após uma reinicialização da máquina), o cache é atualizado. Cada Controller ou Cloud Connector também verifica o banco de dados do site a cada 90 minutos. Se um Controller ou Cloud Connector tiver sido adicionado ou removido desde a última verificação, ou se ocorreu uma alteração de política que afeta o registro do VDA, o Controller ou o Cloud Connector envia uma lista atualizada para seus VDAs registrados e o cache é atualizado. O VDA aceita conexões de todos os Controllers ou Cloud Connectors na sua lista armazenada em cache mais recentemente.
- Se um VDA receber uma lista que não inclui o Controller ou o Cloud Connector no qual está registrado (em outras palavras, o Controller ou o Cloud Connector foi removido do site), o VDA se registra novamente, escolhendo entre os Controllers ou Cloud Connectors na `ListofDDCs`.

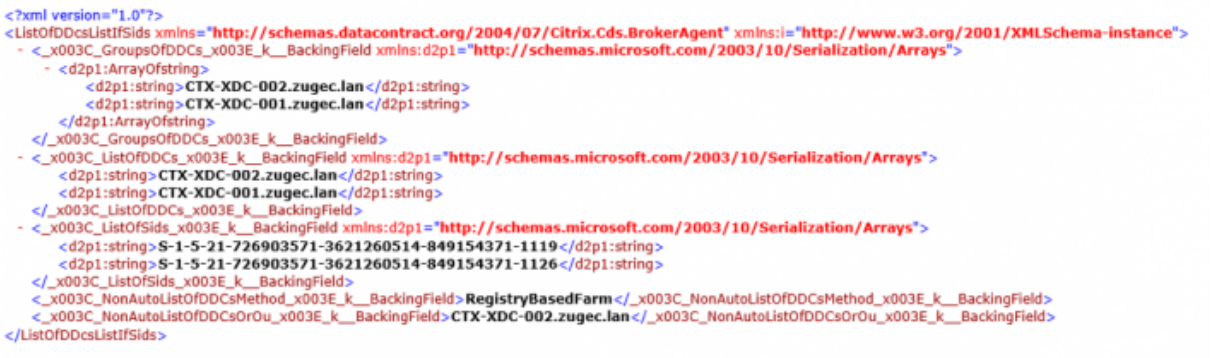
Exemplo:

- Uma implantação tem três Controllers: A, B e C. Um VDA se registra no Controller B (que foi especificado durante a instalação do VDA).
- Mais tarde, dois Controllers (D e E) são adicionados ao site. Dentro de 90 minutos, os VDAs recebem listas atualizadas e aceitam as conexões dos Controllers A, B, C, D e E. (A carga não é distribuída uniformemente a todos os Controllers até que os VDAs sejam reiniciados.)

- Mais tarde, o Controller B é movido para outro site. Dentro de 90 minutos, os VDAs no site original recebem listas atualizadas porque houve uma alteração no Controller desde a última verificação. O VDA que se registrou originalmente no 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 automaticamente armazena em cache 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, tenta-se realizar o registro em Controllers na zona primária.

Como mostrado no exemplo a seguir, o arquivo de cache contém nomes de host e uma lista de IDs de segurança (`ListofSIDs`). O VDA não consulta os SIDs, o que reduz a carga do Active Directory.



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 de esclarecimento. 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 precisa configurar a `ListofSIDs` manualmente por motivos de segurança (não para reduzir a carga do Active Directory), não é possível usar o recurso de atualização automática. Para obter detalhes, consulte ListOfSIDs.

Exceção à prioridade de atualização automática

Embora a atualização automática geralmente tenha a prioridade mais alta de todos os métodos de registro de VDA e substitua as configurações de outros métodos, há uma exceção. Os elementos

`NonAutoListOfDDCs` no cache especificam o método de configuração inicial do VDA. A atualização automática monitora essas informações. Se o método de registro inicial mudar, o processo de registro ignora a atualização automática e usa o próximo método configurado de prioridade mais alta. Esse processo é útil quando você move um VDA para outro site (por exemplo, durante a recuperação de desastres).

Considerações de configuração

Visualize uma configuração comum de registro do VDA.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

Veja as etapas de registro do VDA.

Este é um vídeo incorporado. Clique no link para assistir ao vídeo

Considere o seguinte ao configurar itens que podem afetar o registro do VDA.

Endereços do Controller ou Cloud Connector

Independentemente do método usado para especificar Controllers ou Cloud Connectors, a Citrix recomenda usar um endereço FQDN. Um endereço IP não é considerado uma configuração confiável, porque é mais fácil comprometer um IP do que um registro DNS. Se você preencher o `ListofSIDs` manualmente, poderá usar um IP em um `ListofDDCs`. Contudo, o FQDN continua a ser o recomendado.

Balanceamento de carga

Como observado anteriormente, o VDA distribui conexões automaticamente a todos os Controllers ou Cloud Connectors na `ListofDDCs`. A funcionalidade de failover e balanceamento de carga é incorporada ao Citrix Brokering Protocol (CBP). Se você especificar vários Controllers ou Cloud Connectors na sua configuração, o registro fará o failover entre eles automaticamente, 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 de VDA usa a autenticação mútua Kerberos, onde o cliente (VDA) deve provar sua identidade para o serviço (Controller). No entanto, o Controller ou Cloud Connector devem provar sua identidade para o VDA. Isso significa que o VDA e o Controller ou Cloud Connector estão atuando como servidor e cliente ao mesmo tempo. Como observado no início deste artigo, existem dois canais de comunicação: VDA para Controller/Cloud Connector e Controller/Cloud Connector para VDA.

Um componente nesse processo é chamado SPN (nome de entidade de serviço), que é armazenado como uma propriedade em um objeto de computador do Active Directory. Quando seu VDA se conecta

a um Controller ou Cloud Connector, ele deve especificar com quem ele deseja se comunicar. Esse endereço é um SPN. Se você usar um IP com balanceamento de carga, a autenticação mútua Kerberos reconhece corretamente que o IP não pertence ao Controller ou Cloud Connector esperado.

Para obter mais informações, consulte:

- Introdução ao Kerberos
- Autenticação mútua usando Kerberos

A atualização automática substitui CNAME

O recurso de atualização automática substitui a função CNAME (alias DNS) das versões XenApp e XenDesktop anteriores à 7.x. A funcionalidade CNAME foi desativada, começando com o XenApp e XenDesktop 7. Use a atualização automática em vez de CNAME. (Se você precisar usar o CNAME, consulte CTX137960. Para que o alias de DNS funcione consistentemente, não use atualização automática e CNAME ao mesmo tempo.)

Grupos de Controllers/Cloud Connectors

Em determinados cenários, você pode processar Controllers ou Cloud Connectors em grupos, sendo um grupo o preferencial e o outro grupo usado para failover, se todos os Controllers/Cloud Connectors falharem. Lembre-se de que Controllers ou Cloud Connectors são selecionados aleatoriamente na lista, portanto, o agrupamento pode ajudar a forçar um uso preferencial.

Esses grupos são destinados ao uso em um único site (não em vários sites).

Use parênteses para especificar grupos de Controllers/Cloud Connectors. Por exemplo, com quatro Controllers (dois primários e dois backups), um agrupamento pode ser:

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

Neste exemplo, os Controllers no primeiro grupo (001 e 002) são processados primeiro. Se os dois falharem, os Controllers no segundo grupo (003 e 004) são processados.

Para o XenDesktop 7.0 ou superior, há uma etapa extra que você precisa executar para usar o recurso de **Grupos de registro**. Você precisa proibir a política **Enable Auto Update of Controller** do Studio usando **Prohibit**.

ListOfSIDs

A lista de Controllers que um VDA pode contatar para o registro é a `ListofDDCs`. Um VDA também deve saber em quais Controllers confiar: os VDAs não confiam automaticamente nos Controllers na

ListofDDCs. A ListofSIDs (IDs de segurança) identifica os Controllers confiáveis. Os VDAs tentam se registrar somente em Controllers confiáveis.

Na maioria dos ambientes, a ListofSIDs é gerado automaticamente a partir da ListofDDCs. Você pode usar um rastreamento CDF para ler a ListofSIDs.

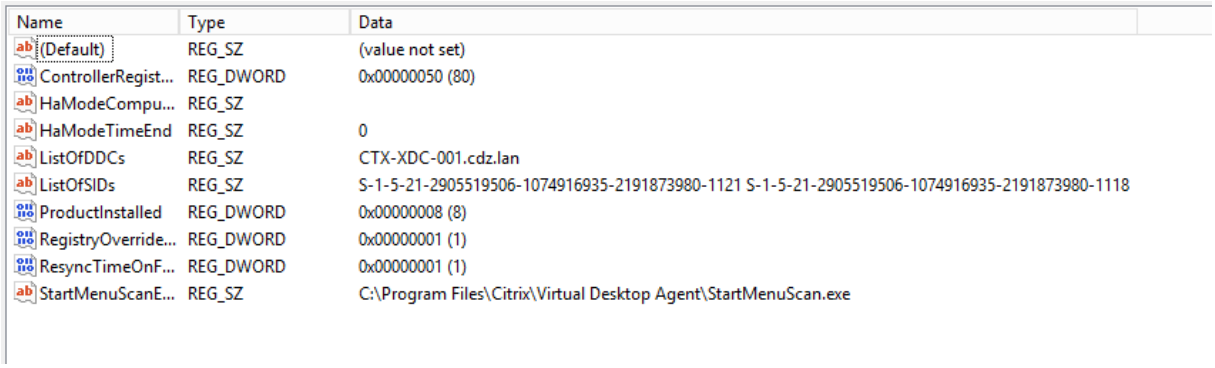
Geralmente, não há necessidade de modificar manualmente a ListofSIDs. Existem várias exceções. As duas primeiras exceções não são mais válidas porque há tecnologias mais recentes disponíveis.

- **Funções separadas para Controllers:** antes de as zonas serem introduzidas no XenApp e XenDesktop 7.7, a ListofSIDs era configurada manualmente quando apenas um subconjunto de Controllers era usado para o registro. Por exemplo, se estivesse usando XDC-001 e XDC-002 como agentes XML, e XDC-003 e XDC-004 para o registro do VDA, você especificaria todos os Controllers na ListofSIDs, e XDC-003 e XDC-004 na ListofDDCs. Esa não é uma configuração típica ou recomendada. Não use em ambientes mais novos. Em vez disso, use zonas.
- **Reduzir a carga do Active Directory:** antes de o recurso de atualização automática ser introduzido no XenApp e XenDesktop 7.6, a ListofSIDs era usada para reduzir a carga nos controladores de domínio. Ao preencher previamente a ListofSIDs, pode-se ignorar a resolução de nomes DNS para SIDs. No entanto, o recurso de atualização automática elimina a necessidade desse trabalho, porque o cache persistente contém SIDs. A Citrix recomenda manter o recurso de atualização automática ativado.
- **Segurança:** em alguns ambientes altamente protegidos, os SIDs dos Controllers confiáveis foram configurados manualmente para evitar possíveis ameaças à segurança por um servidor DNS comprometido. No entanto, se fizer isso, você também deve desativar o recurso de atualização automática. Caso contrário, a configuração do cache persistente é usada.

Portanto, a menos que você tenha um motivo específico, não modifique a ListofSIDs.

Se precisar modificar a 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 espaço, se houver mais de um.

No exemplo a seguir, um Controller é usado para o registro do VDA (ListofDDCs), e dois Controllers são usados para intermediar (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 Controller durante o registro do VDA

Quando um VDA tenta se registrar, o Broker Agent executa primeiramente uma pesquisa de DNS no domínio local para assegurar que o Controller especificado pode ser acessado.

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 é repetida frequentemente. Se o endereço do Controller for inválido (por exemplo, o administrador inseriu um FQDN incorreto ao instalar o VDA), a atividade da consulta pode levar a uma possível condição de negação de serviço distribuído (DDoS) no controlador de domínio.

A chave de registro a seguir 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\Policies\Citrix\VirtualDesktopAgent`

- Nome: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valor: `1` (padrão) ou `0`

Quando definida como `1`, a pesquisa de fallback é desativada. Se a pesquisa inicial do Controller falhar, o Broker Agent para de procurar. Essa é a configuração padrão.
Quando definida como `0`, a pesquisa de fallback é ativada. Se a pesquisa inicial do Controller falhar, a pesquisa de fallback de cima para baixo é iniciada.

Sequenciamento de associação LDAP durante o registro do VDA usando um controlador de domínio somente leitura

Quando um VDA se registra em um controlador de domínio somente leitura (RODC), o Broker Agent deve selecionar quais associações ou associações do Light Directory Access Protocol (LDAP) ignorar. Para fazer essa seleção, o Broker Agent requer uma chave de registro adequada.

Se uma chave de registro não for fornecida ou o campo da chave de registro estiver vazio, o registro do VDA no RODC demorará mais, pois é necessário passar pela sequência de associação do LDAP original.

Para modificar a sequência de associação do LDAP, a chave de registro `ListofIgnoredBindings` foi adicionada a `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. O uso de `ListofIgnoredBindings` permite modificar a sequência de associação do LDAP conforme necessário, e, assim, acelerar o registro do VDA em um RODC.

- Nome: `ListofIgnoredBindings`
- Tipo: `REG_SZ`
- Valores: `DefaultPath`, `DomainPath`, `PDCPath`

O valor é uma lista de opções de caminho de associação, cada uma separada por uma vírgula. A chave de registro ignorará quaisquer valores que não reconheça como válidos.

Solucionar problemas de registro do VDA

Como observado anteriormente, um VDA deve ser registrado em um Delivery Controller ou Cloud Connector para ser considerado ao iniciar sessões intermediadas. Os VDAs não registrados podem resultar na subutilização de recursos disponíveis. Há várias razões para que um VDA não possa ser registrado, muitas das quais um administrador pode resolver. O Studio fornece informações sobre 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 você adicionar as máquinas existentes, a lista de nomes de contas de computador indica se as máquinas são adequadas para adicionar ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre a máquina.

  Se a mensagem identificar uma máquina problemática, você pode remover essa máquina (usando o botão **Remove**) ou adicionar a máquina. Por exemplo, se uma mensagem indicar que as informações sobre uma máquina não puderam ser obtidas (talvez porque ela nunca foi registrada), você pode optar por adicionar a máquina.

  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 de produtos pode exigir um novo VDA. Definir um nível funcional disponibiliza todos os recursos introduzidos nessa versão (e posterior, se o nível funcional não for alterado) para as máquinas no catálogo. No entanto, as máquinas nesse catálogo com uma versão anterior do VDA não podem 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 ao grupo.

O painel de detalhes de um grupo de entrega indica o número de máquinas que deveriam estar registradas, mas que não estão. Em outras palavras, pode haver uma ou mais máquinas que estão ligadas e não estão no modo de manutenção, mas que não estão registradas atualmente em um Controller. Ao visualizar uma máquina "não registrada, mas que deveria estar", consulte a guia **Troubleshoot** no painel de detalhes para ver as possíveis causas e as ações corretivas recomendadas.

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 VDA, consulte CTX136668.
- Você também pode usar verificações de integridade do Citrix Scout para solucionar problemas de registro de VDA e início de sessão. Para obter detalhes, consulte Sobre verificações de integridade.

IP virtual e loopback virtual

June 28, 2023

> **Importante:**
>
> O Windows 10 Enterprise multissessão não suporta Virtualização IP de Área de Trabalho Remota (IP Virtual) e não oferecemos suporte a IP virtual nem loopback virtual em Windows 10 Enterprise multissessão.

Os recursos de IP virtual e loopback virtual são suportados em máquinas Windows Server 2016. Esses recursos não se aplicam a máquinas com SO Windows Desktop.

O recurso de endereço IP virtual da Microsoft fornece um aplicativo publicado com um endereço IP atribuído dinamicamente e exclusivo para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem das comunicações com o localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo do localhost (127.*).

Certos aplicativos, como CRM e Computer Telephony Integration (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros fins que exigem um endereço IP exclusivo ou um endereço de loopback. Outros aplicativos podem se associar a uma porta estática, portanto, as tentativas de iniciar instâncias adicionais de um aplicativo em um ambiente multiusuário falham

porque a porta está em uso. Para que esses aplicativos funcionem corretamente em um ambiente Citrix Virtual Apps, é necessário um endereço IP exclusivo para cada dispositivo.

IP virtual e loopback virtual são recursos independentes. Você pode usar apenas um ou os dois.

Sinopse da ação do administrador:

- Para usar o IP virtual da Microsoft, ative-o e configure-o no Windows Server. (As configurações de política Citrix não são necessárias.)
- Para usar o loopback virtual do Citrix, configure dois parâmetros em uma política Citrix.

IP virtual

Quando o IP virtual está ativado e configurado no Windows Server, cada aplicativo configurado em execução em uma sessão parece ter um endereço exclusivo. Os usuários acessam esses aplicativos em um servidor Citrix Virtual Apps da mesma forma que acessam qualquer outro aplicativo publicado. Um processo requer IP virtual em um dos seguintes casos:

- O processo usa um número de porta TCP codificado
- O processo usa soquetes do Windows e requer um endereço IP exclusivo ou um número de porta TCP especificado

Para determinar se um aplicativo precisa usar endereços IP virtuais:

1. Obtenha a ferramenta TCPView da Microsoft. Essa ferramenta lista todos os aplicativos que associam endereços IP específicos e portas.
2. Desative o recurso Resolver endereços IP para ver endereços em vez de nomes de host.
3. Inicie o aplicativo e use o TCPView para ver quais endereços IP e portas o aplicativo abre e quais nomes de processo abrem essas portas.
4. Configure todos os processos que abrem o endereço IP de um servidor, 0.0.0.0 ou 127.0.0.1.
5. Para garantir que um aplicativo não abra o mesmo endereço IP em uma porta diferente, inicie outra instância do aplicativo.

Como funciona a virtualização de IP de Área de Trabalho Remota (RD) da Microsoft

- O endereçamento de IP virtual deve estar ativado no Microsoft Server.

  Por exemplo, em um ambiente Windows Server 2016, a partir do Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões de Host da Sessão da Área de Trabalho Remota** para ativar a funcionalidade de Virtualização de IP de Área de Trabalho Remota e configurar as definições para atribuir endereços IP dinamicamente utilizando o servidor DHCP (Dynamic Host Configuration Protocol) por sessão ou por programa. Consulte a documentação da Microsoft para obter instruções.

- Depois que o recurso é ativado, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente a partir do servidor DHCP.
- O recurso de Virtualização de IP de Área de Trabalho Remota atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilham um endereço IP por sessão.
- Depois que um endereço é atribuído a uma sessão, a sessão usa o endereço virtual em vez do endereço IP principal para o sistema sempre que as seguintes chamadas são feitas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Ao usar o recurso de virtualização de IP da Microsoft dentro da configuração de host da sessão de Área de Trabalho Remota, os aplicativos são associados a endereços IP específicos inserindo um componente "filter"entre as chamadas de função do aplicativo e do Winsock. O aplicativo então vê somente o endereço IP correto a ser usado. Qualquer tentativa do aplicativo de escutar comunicações TCP ou UDP é associada automaticamente ao seu endereço IP virtual (ou endereço de loopback) alocado. Quaisquer conexões de origem abertas pelo aplicativo são originárias do endereço IP associado ao aplicativo.

Em funções que retornam um endereço (como `GetAddrInfo()`, que uma política do Windows controla), se o endereço IP do host local for solicitado, o IP virtual examina o endereço IP retornado e o altera para o endereço IP virtual da sessão. Os aplicativos que tentam obter o endereço IP do servidor local através de tais funções de nome veem apenas o endereço IP virtual exclusivo atribuído à sessão. Esse endereço IP é frequentemente usado em chamadas subsequentes do soquete, tais como associação ou conexão. Para obter mais informações sobre as políticas do Windows, consulte RDS IP Virtualization in Windows Server.

Muitas vezes, um aplicativo solicita associar-se a uma porta para escuta no endereço 0.0.0.0. Quando um aplicativo faz isso e usa uma porta estática, você não pode iniciar mais de uma instância do aplicativo. O recurso de endereço IP virtual também procura por 0.0.0.0 nesses tipos de chamada e altera a chamada para escutar no endereço IP virtual específico, o que permite que mais de um aplicativo escute na mesma porta no mesmo computador porque estão todos escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço IP virtual estiver ativado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentam se associar a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas são associadas a VIPAddress1:9000 e VIPAddress2:9000, sem haver conflito.

Loopback virtual

Ativar as configurações de política de loopback de IP virtual da Citrix permite que cada sessão tenha o seu próprio endereço de loopback para comunicação. Quando um aplicativo usa o endereço localhost

(padrão = 127.0.0.1) em uma chamada Winsock, o recurso de loopback virtual simplesmente substitui 127.0.0.1 por 127.X.X.X, onde X.X.X é uma representação do ID de sessão + 1. Por exemplo, um ID de sessão de 7 é 127.0.0.8. No caso improvável de o ID da sessão exceder o quarto octeto (mais de 255), o endereço passa para o octeto seguinte (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em um dos seguintes casos:

- O processo usa o endereço (localhost) de loopback do soquete do Windows (127.0.0.1)
- O processo usa um número de porta TCP codificado

Use as configurações de política de loopback virtual para aplicativos que usam um endereço de loopback para comunicação entre processos. Nenhuma configuração adicional é necessária. O loopback virtual não tem dependência do IP virtual, portanto, você não precisa configurar o servidor Microsoft.

- Suporte a loopback de IP virtual. Quando ativada, essa configuração de política permite que cada sessão tenha o seu próprio endereço de loopback virtual. Essa configuração é desativada por padrão. O recurso se aplica apenas a aplicativos especificados com a configuração de política de lista de programas de loopback virtual de IP virtual.
- Lista de programas de loopback virtual de IP virtual. Essa configuração de política especifica os aplicativos que usam o recurso de loopback de IP virtual. Essa configuração se aplica somente quando a configuração de política de suporte de loopback de IP virtual está ativada.

Recurso relacionado

Você pode usar as seguintes configurações de registro para garantir que o loopback virtual tenha preferência sobre o IP virtual. Esse recurso é chamado de loopback preferencial. No entanto, proceda com cautela:

- Use o loopback preferencial somente se o IP virtual e o loopback virtual estiverem ativados. Caso contrário, os resultados podem ser inesperados.
- Editar o registro incorretamente pode causar sérios problemas e exigir que você reinstale seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Execute regedit nos servidores onde os aplicativos residem.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nome: PreferLoopback, Tipo: REG_DWORD, Dados: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dados: <lista de processos>

Zonas

June 28, 2023

> **Nota:**
>
> Você pode gerenciar a implantação do seu Citrix Virtual Apps and Desktops usando dois consoles de gerenciamento: Web Studio (baseado na Web) e Citrix Studio (baseado no Windows). Este artigo abrange somente o Web Studio. Para obter informações sobre o Citrix Studio, consulte o artigo equivalente no Citrix Virtual Apps and Desktops 7 2212 ou anterior.

As implantações que abrangem locais amplamente dispersos conectados por uma WAN podem ter problemas devido à latência e à confiabilidade da rede. Há duas opções que atenuam esses problemas:

- Implantar vários sites, cada um com seu próprio banco de dados do site SQL Server.

  Essa opção é recomendada para implantações em grandes empresas. Vários sites são gerenciados separadamente e cada um requer seu próprio banco de dados do site SQL Server. Cada site é uma implantação separada do Citrix Virtual Apps.

- Configurar várias zonas em um único site.

  A configuração de zonas pode ajudar os usuários em regiões remotas a se conectarem aos recursos sem necessariamente forçar que as conexões atravessem grandes segmentos da WAN. O uso de zonas permite o gerenciamento eficaz do site a partir de um único console Web Studio, Citrix Director e do banco de dados do site. Isso economiza nos custos de implantação, equipes, 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 áreas de trabalho mais próximos dos usuários finais, o que melhora o desempenho. Uma zona pode ter um ou mais Controllers instalados localmente para redundância e resiliência, mas não é necessário.

  O número de Controllers configurados no site pode afetar o desempenho de algumas operações, como adicionar novos Controllers ao site. Para evitar isso, recomendamos que você limite o número de zonas no site Citrix Virtual Apps ou Citrix Virtual Desktops a um máximo de 50.

  Quando a latência de rede das 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 sobre a qual estamos falando. Por exemplo, "Um VDA se registra em um Controller local"significa que o 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, nessa implementação de zonas, não há coletores de dados. Todos os Controllers no site se comunicam com um banco de dados na zona primária. Além disso, as zonas preferencial e de failover funcionam de forma diferente nessa versão.

Tipos de zona

Um site sempre tem uma zona primária. Ele também pode opcionalmente ter uma ou mais zonas satélite. Zonas de 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". Essa zona contém o banco de dados do site SQL Server (e servidores SQL de alta disponibilidade, se usados), Web Studio, Director, Citrix StoreFront, Citrix License Server e Citrix Gateway. Mantenha sempre o banco de dados do site na zona primária.

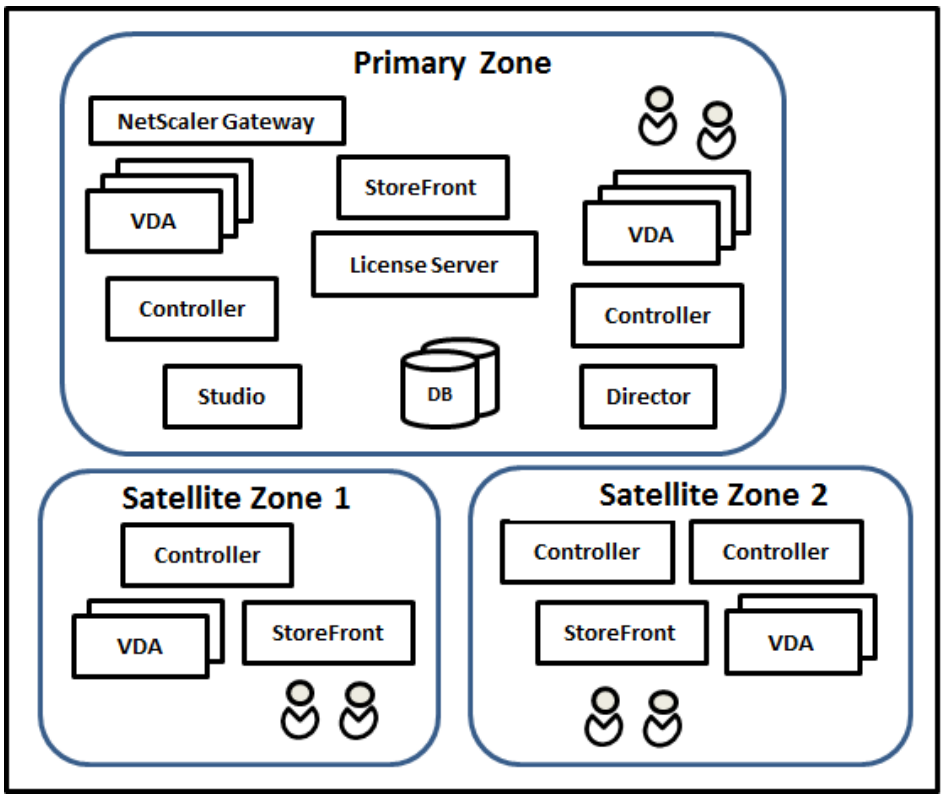
A zona primária deve ter pelo menos dois Controllers para redundância. A zona primária pode ter VDAs com aplicativos que estão intrinsecamente ligados ao banco de dados e infraestrutura.

Zona satélite:

Uma zona satélite contém um ou mais VDAs, Controllers, servidores StoreFront e servidores Citrix Gateway. Em operações normais, os Controllers em uma zona satélite se comunicam diretamente com o banco de dados na zona primária.

Uma zona satélite, particularmente as grandes, também pode conter um hipervisor que é usado para provisionar e armazenar máquinas para essa zona. Quando configura 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 de diferentes configurações, com base em seu ambiente e necessidades únicas. A figura a seguir ilustra uma zona primária e exemplos de zonas satélite.



Na ilustração:

- **Zona primária:** contém dois Controllers, Web Studio, Director, StoreFront, License Server e o banco de dados do site (além de implantações SQL Server de alta disponibilidade). A zona primária também contém vários VDAs e um Citrix Gateway.
- **Zona satélite 1: VDAs com Controller:** zona satélite 1 contém um Controller, VDAs e um servidor StoreFront. VDAs nesta zona satélite registram-se no Controller local. O Controller local se comunica com o banco de dados do site e o servidor de licenças na zona primária.

  Se a WAN falhar, o recurso de Cache de host local permite que o Controller na zona satélite continue intermediando conexões com VDAs nessa zona. Essa implantação é eficiente em um escritório onde os funcionários usam um site StoreFront local e o Controller local para acessar seus recursos locais.
- **Zona satélite 2: VDAs com Controllers redundantes:** zona satélite 2 contém dois Controllers, VDAs e um servidor StoreFront. Esse é o tipo de zona mais resiliente, oferecendo proteção contra uma falha simultânea da WAN e de um dos Controllers locais.

Onde os VDAs se registram e onde os Controllers fazem failover

Em um site que contém zonas primária e satélite, com VDAs com 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. (Esse 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 fique disponível outra vez. Um VDA em uma zona satélite nunca tenta se registrar em um Controller em outra zona satélite.
- Quando a atualização automática está ativada para a descoberta pelo VDA de Controllers, e você especifica uma lista de endereços de Controllers durante a instalação do VDA, um Controller é selecionado aleatoriamente nessa lista para o registro inicial (independentemente da zona em que o Controller reside). Depois que a máquina com esse VDA é reinicializada, o VDA começa a se registrar dando preferência a um Controller em sua zona local.
- Se um Controller em uma zona satélite falhar, é feito o failover para outro Controller local, se possível. Se nenhum Controller local estiver disponível, o failover é feito para um Controller na zona primária.
- Se você mover um Controller para dentro ou para fora de uma zona e a atualização automática estiver ativada, os VDAs nas duas zonas recebem 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 no catálogo se registram novamente nos Controllers na zona para onde você moveu o catálogo. (Quando você move um catálogo para outra zona, verifique se essa zona e a zona com a conexão de host associada estão bem conectadas. Se houver largura de banda limitada ou alta latência, mova a conexão do host para a mesma zona que contém o catálogo de máquina associado.)

Se todos os Controllers na zona primária falharem:

- O Web Studio não pode se conectar ao site.
- Conexões com VDAs na zona primária não podem ser estabelecidas.
- O desempenho do site se degrada até que os Controllers na zona primária fiquem disponíveis.

Para sites que contêm versões de VDA anteriores à 7.7:

- Um VDA em uma zona satélite aceita solicitações de Controllers em sua zona local e na zona primária. (VDAs com versão mínima 7.7 podem aceitar solicitações do Controller de outras zonas satélite.)
- Um VDA em uma zona satélite se registra em um Controller na zona primária ou na zona local aleatoriamente. (VDAs com versão mínima 7.7 dão preferência à zona local.)

Preferência de zona

Para usar o recurso de preferência de zona, você deve usar, no mínimo, o StoreFront 3.7 e o Citrix Gateway 11.0-65.x.

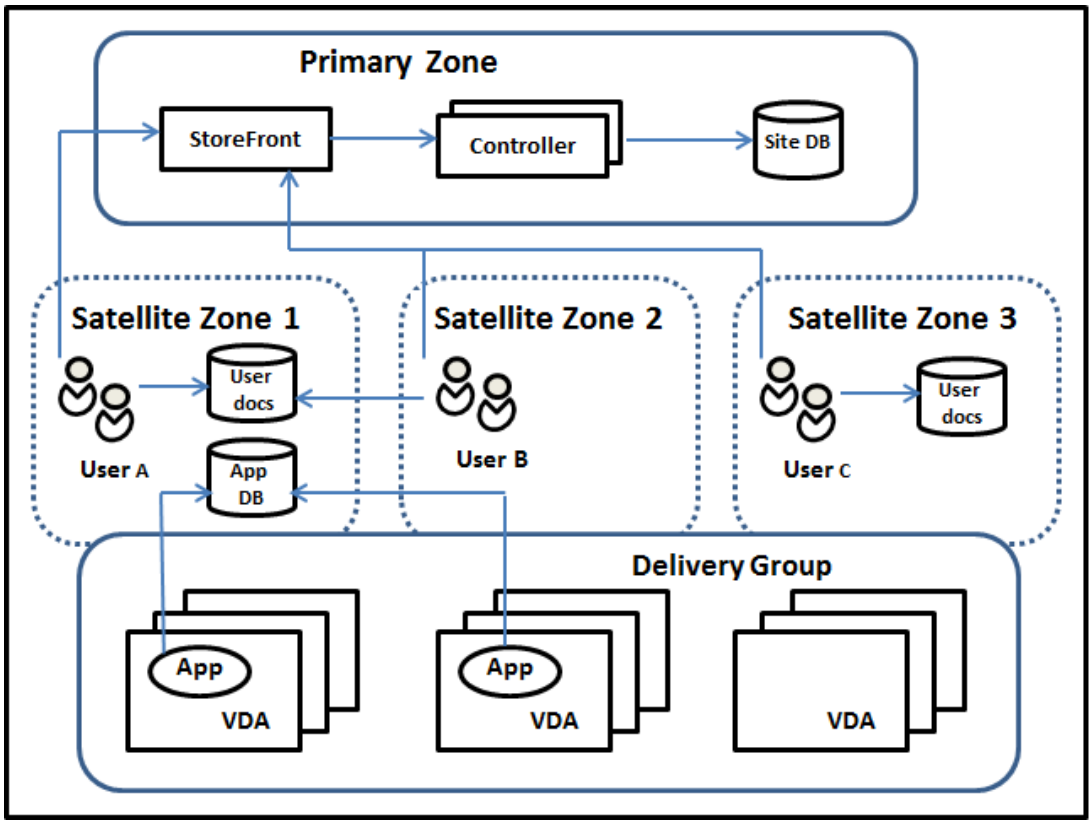
Em um site de várias zonas, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou área de trabalho.

Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma determinada zona com base em:

- Onde os dados do aplicativo são armazenados. Essa é a origem do aplicativo.
- A localização dos dados de origem do usuário, como um perfil ou compartilhamento. Essa é a origem do usuário.
- O local atual do usuário (onde o aplicativo Citrix Workspace está sendo executado). Essa é a localização do usuário.

O gráfico a seguir mostra um exemplo de configuração de várias zonas.



Neste exemplo, os VDAs estão distribuídos entre três zonas satélite, mas estão todos no mesmo grupo de entrega. Portanto, o agente pode ter a opção de qual VDA usar para uma solicitação de inicialização

do usuário. Esse exemplo indica que existem várias localizações onde os usuários podem executar seus pontos de extremidade com o 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 de origem para o usuário ou aplicativo. O agente no Delivery Controller usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se os recursos estiverem disponíveis. Você pode:

- Configura a zona de origem de um usuário adicionando um usuário a uma zona.
- Configurar a zona de origem de um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona de origem por vez. (Pode ocorrer uma exceção a usuários quando várias associações de zona ocorrem devido à associação a grupos de usuários; consulte a seção "Outras considerações". No entanto, mesmo nesse caso, o agente usa apenas uma zona de origem.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o agente seleciona apenas uma zona preferencial para uma inicialização. A ordem de prioridade padrão para selecionar a zona preferencial é origem do aplicativo > origem do usuário > localização do usuário. Você pode restringir a sequência; consulte Adaptação da preferência de zona. Quando um usuário inicia um aplicativo:

- Se o aplicativo tiver uma associação de zona configurada (uma origem de aplicativo), a zona preferencial é a zona de origem do aplicativo.
- Se o aplicativo não tiver uma associação de zona configurada, mas o usuário tiver uma associação de zona configurada (uma origem de usuário), a zona preferencial é a zona de origem desse usuário.
- Se nem o aplicativo nem o usuário tiverem uma associação de zona configurada, a zona preferencial será a zona em que o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, será usada uma seleção aleatória de VDA e zona. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver uma zona preferencial, o balanceamento de carga será aplicado a todos os VDAs no grupo de entrega.

Adaptar as preferências de zona

Quando você configura (ou remove) uma zona de origem para um usuário ou um aplicativo, você também pode restringir como a preferência de zona é usada.

- **Uso obrigatório da zona de origem do usuário:** em um grupo de entrega, você pode especificar que uma sessão seja iniciada na zona de origem do usuário (se configurada), sem o failover para outra zona se a zona de origem não tiver recursos disponíveis. Essa restrição é útil quando você precisa evitar o risco de copiar grandes perfis ou arquivos de dados entre zonas. Em outras palavras, você prefere negar um início de sessão a iniciar a sessão em uma zona diferente.
- **Uso obrigatório da zona de origem do aplicativo:** da mesma forma, quando você configura uma zona de origem para um aplicativo, você pode indicar que o aplicativo seja iniciado somente naquela zona, sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona de origem do aplicativo.
- **Sem zona de origem do aplicativo, e ignora a zona de origem do usuário configurada:** se você não especificar uma zona de origem para um aplicativo, também pode indicar que nenhuma zona de usuário configurada será considerada ao iniciar o aplicativo. Por exemplo, você quer que os usuários executem um aplicativo em um VDA perto de seus dispositivos, usando a preferência de zona de localização do usuário, mesmo que alguns usuários tenham uma zona de origem diferente.

Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia um aplicativo ou área de trabalho, o agente prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário iniciando um aplicativo ou área de trabalho já tem uma sessão adequada para o recurso que está sendo iniciado (por exemplo, que pode usar compartilhamento de sessão para um aplicativo, ou uma sessão que já está executando o recurso sendo iniciado), mas essa sessão está sendo executada em um VDA em uma zona diferente da zona preferencial do usuário/aplicativo, o sistema pode criar uma nova sessão. Isso permite o início na zona correta (se tiver capacidade disponível), antes de se reconectar a uma sessão em uma zona menos preferida para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não possa mais ser acessada, a reconexão é permitida às sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem preferencial para o início das sessões é:

1. Reconectar-se a uma sessão existente na zona preferencial.
2. Reconectar-se a uma sessão desconectada existente em uma zona diferente da zona preferencial.

3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar-se a uma sessão existente conectada em uma zona diferente da zona preferencial.
5. Iniciar uma nova sessão em uma zona diferente da zona preferencial.

Outras considerações de preferência de zona

- Se você configurar uma zona de origem para um grupo de usuários (como um grupo de segurança), os usuários desse grupo (por meio de associação direta ou indireta) serão associados à zona especificada. No entanto, um usuário pode ser um membro de vários grupos de segurança e, portanto, pode ter uma zona de origem diferente configurada por meio de outra associação de grupo. Nesses casos, a determinação da zona de origem desse usuário pode ser ambígua.

Se um usuário tem uma zona de origem configurada que não foi adquirida através da associação de grupo, essa zona é usada para a preferência de zona. Todas as associações de zona adquiridas por meio da associação de grupo são ignoradas.

Se o usuário tem várias associações de zonas diferentes adquiridas exclusivamente por meio da associação ao grupo, o agente escolhe entre as zonas aleatoriamente. Assim que o agente faz essa escolha, a zona é usada para inícios de sessão subsequentes, até que a associação do grupo do usuário mude.

- A preferência da zona de localização do usuário exige a detecção do aplicativo Citrix Workspace no dispositivo de ponto de extremidade pelo Citrix Gateway através do qual o dispositivo está se conectando. O Citrix Gateway deve ser configurado para associar intervalos de endereços IP a zonas específicas, e a identidade de zona descoberta deve ser passada para o Controller através do StoreFront.

Para obter mais informações sobre a preferência de zona, consulte Zone preference internals.

Considerações, requisitos e práticas recomendadas

- 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 estão na mesma zona. (No entanto, com uma conexão de alta largura de banda e baixa latência 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, pressupõe-se que as máquinas têm boa conectividade (local) com os hipervisores e VDAs na mesma zona. Os Controllers nessa zona satélite são usados preferencialmente aos Controllers na zona primária para lidar com esses hipervisores e máquinas VDA.

  - Quando uma conexão de hipervisor é colocada em uma zona satélite, pressupõe-se que todos os hipervisores gerenciados por meio dessa conexão de hipervisor também residem nessa zona satélite. Os Controllers nessa zona satélite são usados preferencialmente aos Controllers na zona primária ao se comunicar com essa conexão de hipervisor.
  - Quando um catálogo de máquinas é colocado em uma zona de satélite, presume-se que todas as máquinas VDA nesse catálogo estão na zona satélite. Os Controllers locais são usados preferencialmente aos Controllers na zona primária ao tentar se registrar no site, depois que o mecanismo da atualização automática da lista do Controller 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 do roteamento Optimal HDX Routing do StoreFront em vez de, como acontece para os outros elementos descritos aqui, como parte da configuração do site. Quando um Citrix Gateway está associado a uma zona, é preferível que ele seja usado quando são usadas conexões HDX com máquinas VDA nessa zona.

- Quando você cria um site de produção e depois cria o primeiro catálogo e grupo de entrega, todos os itens ficam na zona primária —você não pode criar zonas satélite até concluir essa configuração inicial. (Se você criar um site vazio, a zona primária conterá inicialmente apenas um Controller. Você pode criar zonas satélite antes ou depois de criar um catálogo e um grupo de entrega.)
- Quando você cria a primeira zona de satélite contendo um ou mais itens, todos os outros itens em seu site permanecem na zona primária.
- A zona primária é chamada de 'Primary'por padrão; você pode alterar esse nome. Embora o Web Studio indique qual zona é a zona primária, é prática recomendada usar um nome facilmente identificável para a zona primária. Você pode reatribuir a zona primária (ou seja, transformar outra zona na zona primária), mas ela deve sempre conter o banco de dados do site e todos os servidores de alta disponibilidade.
- Mantenha sempre 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 estreita 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 desejados 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, através de uma rede de baixa latência e alta largura de banda).
- Para um desempenho ideal, instale o Web Studio e o Director apenas na zona primária. Você pode acessar o Web Studio e o Director de uma zona satélite (por exemplo, uma zona satélite contendo Controllers para usar como failover se a zona primária ficar inacessível) porque eles

são um aplicativo da web.

- O ideal é que o Citrix Gateway em uma zona satélite seja usado para conexões de usuários que entram nessa zona a partir de outras zonas ou localizações externas, embora você possa usá-lo para conexões dentro da zona.
- Lembre-se: para usar o recurso de preferência de zona, você deve usar, no mínimo, o StoreFront 3.7 e o 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 nos VDAs implantados na zona satélite. Assim, zonas satélite com apenas alguns VDAs e sessões podem funcionar com uma conexão de baixa qualidade ao banco de dados em comparação a zonas satélite com um grande número de VDAs e sessões.

Para obter mais informações, consulte Latency and SQL Blocking Query Improvements.

O impacto da latência no desempenho da intermediação

Embora as zonas permitam que os usuários fiquem em links de maior latência, desde que haja um agente local, a latência adicional inevitavelmente afeta a experiência do usuário final. Na maioria dos trabalhos, os usuários experimentam lentidão causada por viagens de ida e volta entre Controllers na zona satélite e no banco de dados do site.

Na inicialização de aplicativos, ocorrem atrasos extras enquanto o processo de intermediação da sessão identifica VDAs adequados para enviar solicitações de início de sessão.

Criar e gerenciar zonas

Um administrador completo pode executar 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. A movimentação de 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 Citrix Provisioning não reconhece zonas, portanto, recomendamos usar o Web Studio para criar catálogos para zonas satélite. Crie o catálogo no Web Studio, especificando a zona satélite correta. Depois use o console Citrix Provisioning para provisionar

máquinas no catálogo. (Se você criar o catálogo usando o assistente do Citrix Provisioning, o catálogo será colocado na zona primária. Você deve usar o Web Studio para movê-lo para a zona de satélite posteriormente.)

Criar uma zona

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo.
3. Selecione **Create Zone** na barra de ações.
4. Insira um nome para a zona e uma descrição (opcional). O nome deve ser exclusivo dentro do site.
5. Selecione os itens a serem colocados na nova zona. Você pode filtrar ou pesquisar a lista de itens a partir da qual você pode selecionar. Você também pode criar uma zona vazia; simplesmente não selecione nenhum item.
6. Clique em **Salvar**.

Como alternativa a esse método, você pode selecionar um ou mais itens no Web Studio e, em seguida, selecionar **Create Zone** na barra de ações.

Alterar o nome ou a descrição de uma zona

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo.
3. Selecione uma zona no painel central e, em seguida, selecione **Edit Zone** na barra de ações.
4. Altere o nome da zona, a descrição ou os dois. Se você alterar o nome da zona primária, confirme que a zona permanece facilmente identificável como a zona primária.
5. Clique em **Save** ou **Apply**.

Mover itens de uma zona para outra zona

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo.
3. Selecione uma zona no painel central e, em seguida, selecione um ou mais itens.
4. Arraste os itens para a zona de destino ou selecione **Move Items** na barra de ações e 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 para poder ser excluída. Não é possível excluir a zona primária.

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo.
3. Selecione uma zona no painel central.
4. Selecione **Delete Zone** na barra de ações. Se a zona não estiver vazia (contiver itens), você será solicitado a escolher a zona para onde os itens serão movidos.
5. Confirme a exclusão.

Adicionar uma zona de origem para um usuário

Configurar a zona de origem de um usuário é o mesmo que *adicionar um usuário a uma zona*.

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo e, em seguida, selecione uma zona no painel central.
3. Selecione **Add Users to Zone** na barra de ações.
4. Na caixa de diálogo **Add Users to Zone**, clique em **Add** e selecione os usuários e grupos de usuários a serem adicionados à zona. Se você especificar usuários que já têm uma zona de origem, uma mensagem oferece duas opções: **Yes** = adicionar apenas os usuários que você especificou que não têm uma zona de origem; **No** = retornar à caixa de diálogo de seleção do usuário.
5. Clique em **OK**.

Para usuários com uma zona de origem configurada, você pode exigir que as sessões sejam iniciadas somente a partir de sua zona de origem:

1. Crie ou edite um grupo de entrega.
2. Na página **Users**, marque a caixa de seleção **Sessions must launch in a user's home zone, if configured**.

Todas as sessões iniciadas por um usuário nesse grupo de entrega devem ser iniciadas a partir de máquinas na zona de origem desse usuário. Se um usuário no grupo de entrega não tiver uma zona de origem configurada, esse parâmetro não terá efeito.

Remover uma zona de origem de um usuário

Este procedimento é o mesmo que remover um usuário de uma zona.

1. Faça login no Web Studio.
2. Selecione **Zones** no painel esquerdo e, em seguida, selecione uma zona no painel central.
3. Selecione **Remove Users from Zone** na barra de ações.
4. Na caixa de diálogo **Add Users to Zone**, clique em **Remove** e selecione os usuários e grupos a serem removidos da zona. Essa ação remove os usuários somente da zona; os usuários permanecem nos grupos de entrega e nos grupos de aplicativos aos quais pertencem.
5. Confirme a remoção quando solicitado.

Gerenciar zonas de origem para aplicativos

Configurar a zona de origem de um aplicativo é o mesmo que adicionar um aplicativo a uma zona. Por padrão, em um ambiente de várias zonas, um aplicativo não tem uma zona de origem.

A zona de origem de um aplicativo é especificada nas propriedades do aplicativo. Você pode configurar as propriedades do aplicativo ao adicionar o aplicativo a um grupo ou posteriormente.

- Ao criar um Grupo de Entrega, criar um Grupo de Aplicativos ou adicionar aplicativos a grupos existentes, selecione **Properties** na página **Applications** do assistente.
- Para alterar as propriedades de um aplicativo depois que o aplicativo for adicionado, selecione **Applications** no painel esquerdo. Selecione um aplicativo e, em seguida, selecione **Edit Application Properties** na barra de ações.

Na página **Zones** das propriedades/configurações do aplicativo:

- Se quiser que o aplicativo tenha uma zona de origem:
  - Selecione o botão de opção **Use the selected zone to decide** e selecione a zona.
  - Se quiser que o aplicativo seja iniciado apenas a partir da zona selecionada (e não de outras zonas), marque a caixa de seleção na área de seleção de zona.
- Se não quiser que o aplicativo tenha uma zona de origem:
  - Selecione o botão de opção **Do not configure a home zone**.
  - Se você não quiser que o agente considere nenhuma zona de usuário configurada ao iniciar o aplicativo, marque a caixa de seleção sob o botão de opção. Nesse caso, não serão usadas zonas de origem do aplicativo nem do usuário para determinar onde iniciar o aplicativo.

Outras ações que incluem a especificação de zonas

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 o padrão. Quando usar o Machine Creation Services para criar um catálogo, a zona configurada para a conexão do host é selecionada automaticamente.

Se o site não contiver zonas satélite, a zona primária é presumida e a caixa de seleção de zona não é exibida.

Monitoramento

June 28, 2023

Administradores e funcionários do suporte técnico podem monitorar os sites do Citrix Virtual Apps and Desktops usando uma variedade de recursos e ferramentas. Usando essas ferramentas, você pode monitorar:

- Sessões do usuário e o uso de sessões
- Desempenho de logon
- Conexões e máquinas, incluindo falhas
- Avaliação de carga
- Tendências históricas
- Infraestrutura

Citrix Director

O Director é uma ferramenta da Web em tempo real que você pode usar para monitorar e solucionar problemas e para executar tarefas de suporte para usuários finais.

Para obter detalhes, consulte os artigos do Director .

Log de configuração

O log de configuração permite que os administradores acompanhem as alterações administrativas em um site. O log de configuração pode ajudar os administradores a diagnosticar e solucionar problemas depois que são feitas alterações na configuração, auxiliar no gerenciamento de mudanças e rastreio de configurações, e informar as atividades de administração.

Você pode exibir e gerar relatórios sobre as informações do log no Studio. Você também pode exibir os itens do log no Director com o Trend View para fornecer notificações de alterações de configuração. Esse recurso é útil para administradores que não têm acesso ao Studio.

A exibição de Tendências fornece dados históricos de alterações de configuração durante um período de tempo para que os administradores possam avaliar quais alterações foram feitas no site, quando foram feitas e quem as fez encontrar a causa de um problema. Essa exibição 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 ativar e configurar o log de configuração, consulte Configuration Logging. Os artigos do Director descrevem como exibir as informações do log da ferramenta.

Logs de eventos

Os serviços dentro do Citrix Virtual Apps and Desktops registram no log os eventos que ocorrem. Os logs de eventos são usados para monitorar e solucionar problemas de operação.

Para obter detalhes, consulte Registros de eventos. Artigos de recursos individuais também podem conter informações sobre eventos.

Log de configuração

June 28, 2023

O log de configuração é um recurso que captura alterações na configuração do site e atividades administrativas no banco de dados. O recurso é ativado por padrão. Você pode usar o conteúdo no log para:

- Diagnosticar e solucionar problemas após fazer alterações de configuração. O log fornece uma trilha de localização.
- Auxiliar no gerenciamento de mudanças e rastrear as configurações.
- Informar atividades administrativas.

Você define as preferências de log de configuração, exibe os logs de configuração e gera relatórios HTML e CSV no Citrix Studio. Você pode filtrar as exibições do log de configuração por intervalos de datas e resultados de pesquisa de texto. O log obrigatório, quando ativado, impede que alterações

de configuração sejam feitas, a menos que possam ser registradas em log. Com a permissão apropriada, você pode excluir entradas do log de configuração. Você não pode usar o recurso de log de configuração para editar o conteúdo do log.

O log de configuração usa um SDK do PowerShell e o Configuration Logging Service. O Configuration Logging Service é executado em todos os Controllers do site. Se um Controller falhar, o serviço em outro Controller lida automaticamente com as solicitações de log.

Por padrão, o recurso de registro de configuração está ativado e usa o banco de dados 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 do log 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 da administração delegada, com as permissões Edit Logging Preferences e View Configuration Logs.

Os logs de configuração são localizados quando são criados. Por exemplo, um registro criado em inglês é lido em inglês, independentemente da localidade do leitor.

O que é registrado no log

As alterações de configuração e as atividades administrativas iniciadas no Studio, Director e por scripts PowerShell são registradas em log. Exemplos de alterações de configuração em log incluem trabalhar com (criar, editar, excluir, atribuir):

- Catálogos de máquinas
- Grupos de entrega (incluindo a alteração das configurações de gerenciamento de energia)
- Funções e escopos do administrador
- Recursos e conexões do host
- Políticas Citrix através do Studio

Exemplos de alterações administrativas em log incluem:

- Gerenciamento de energia de uma máquina virtual ou área de trabalho do usuário
- Quando o Studio ou Director envia uma mensagem para um usuário

As seguintes operações não são registradas em log:

- Operações autônomas, como a ativação do gerenciamento em pool de máquinas virtuais.
- Ações de políticas implementadas por meio do Console de Gerenciamento de Política de Grupo (GPMC); use as ferramentas da Microsoft para ver os logs dessas ações.
- Alterações feitas por meio do registro, acesso direto do banco de dados ou a partir de outras fontes que não o Studio, Director ou PowerShell.

- Quando a implantação é inicializada, o log de configuração fica disponível quando a primeira instância do Configuration Logging Service é registrada no Configuration Service. Portanto, os estágios iniciais da configuração não são registrados em log (por exemplo, quando o esquema do banco de dados é obtido e aplicado, quando um hipervisor é inicializado).

Gerenciar o log de configuração

Por padrão, o log 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 log de configuração (e o banco de dados de monitoramento) pelos seguintes motivos:

- A estratégia de backup do banco de dados de log de configuração provavelmente será diferente da estratégia de backup do banco de dados de configuração do site.
- O volume de dados coletados do log de configuração (e o Monitoring Service) pode afetar negativamente o espaço disponível para o banco de dados de configuração do site.
- Ele divide o ponto único de falha entre os três bancos de dados.

As edições de produtos que não oferecem suporte ao log de configuração não têm um nó Logging no Studio.

Ativar e desativar o log de configuração e o log obrigatório

Por padrão, o log de configuração está ativado e o log obrigatório está desativado.

1. Entre no Web Studio e selecione **Logging** no painel esquerdo.
2. Selecione **Preferences** na barra de ações. A caixa de diálogo do log de configuração contém informações do banco de dados e indica se o log de configuração e o log obrigatório estão ativados ou desativados.
3. Selecione a ação desejada:

   Para ativar o registro em log de configuração, selecione **Enable**. Essa é a configuração padrão. Se o banco de dados não puder ser gravado, as informações de log são descartadas, mas a operação continua.

   Para desativar o log de configuração, selecione **Disable**. Se o registro em log tiver sido ativado anteriormente, os registros existentes permanecem legíveis com o SDK do PowerShell.

   Para ativar o log obrigatório, selecione **Prevent changes to the site configuration when the database is not available**. Nenhuma alteração de configuração ou atividade administrativa que é normalmente registrada em log é permitida, a menos que possa ser gravada no banco de dados de log de configuração. Você pode ativar o log obrigatório somente quando o log

de configuração está ativado (quando **Enable** está selecionado). Se o Configuration Logging Service falhar e a alta disponibilidade não estiver em uso, o log obrigatório passa a ser o padrão. Nesses casos, as operações que normalmente seriam registradas em log não são realizadas.

Para desativar o log obrigatório, selecione **Allow changes when to the site configuration when the database is not available**. Alterações de configuração e atividades administrativas são permitidas, mesmo que o banco de dados de log de configuração não possa ser acessado. Essa é a configuração padrão.

Alterar a localização do banco de dados de log de configuração

Você não pode alterar a localização do banco de dados quando o log obrigatório está ativado, pois a alteração da localização inclui um breve intervalo de desconexão que não pode ser registrado no log.

1. Crie um servidor de banco de dados usando uma versão compatível do SQL Server.
2. Entre no Web Studio e selecione **Logging** no painel esquerdo.
3. Selecione **Preferences** na barra de ações.
4. Na caixa de diálogo Logging Preferences, selecione **Change logging database**.
5. Na caixa de diálogo Change Logging Database, especifique a localização do servidor que contém o novo servidor de banco de dados. Consulte Formatos de endereço de banco de dados para formatos válidos
6. Para permitir que o Studio crie o banco de dados, clique em **OK**. Quando solicitado, clique em **OK** e o banco de dados é criado automaticamente. O Studio tenta acessar o banco de dados usando as credenciais do usuário atual do Studio. Se isso falhar, você será solicitado a fornecer as credenciais do usuário do banco de dados. Em seguida, o Studio carrega o esquema do banco de dados para o banco de dados. (As credenciais são retidas somente durante a criação do banco de dados.)
7. Para criar o banco de dados manualmente, clique em **Generate database script**. O script gerado inclui instruções para criar o banco de dados manualmente. Confirme que o banco de dados está vazio e que pelo menos um usuário tem permissão para acessar e alterar o banco de dados antes de carregar o esquema.

Os dados no log de configuração de dados anterior não são importados para o novo banco de dados. Os logs não podem ser agregados de ambos os bancos de dados quando recuperados. A primeira entrada de log no novo banco de dados de log de configuração indica que ocorreu uma alteração no banco de dados, 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 pelo Director são listadas no painel central superior do Studio. Uma operação de alto nível resulta em uma ou mais chamadas de serviço e SDK, que são operações de baixo nível. Quando você seleciona uma operação de alto nível no painel superior, o painel inferior exibe as operações de nível baixo.

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 o registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Quando você exibe logs com base em intervalos de tempo, os registros incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se todos os logs dos últimos cinco dias forem solicitados e houver um log com uma hora de início nos últimos cinco dias, mas não houver hora 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 cria uma operação de alto nível substituta.

Para exibir o conteúdo do log de configuração, selecione **Logging** 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:

- Ordenar a exibição pelo cabeçalho da coluna.
- Filtre a exibição especificando um intervalo de dia, ou insira um texto na caixa **Search**. Para retornar à exibição padrão depois de usar a pesquisa, apague o texto na caixa **Search**.

Gerar relatórios

Você pode gerar relatórios CSV e HTML contendo dados do log de configuração.

- O relatório CSV contém todos os dados do log de um intervalo de tempo especificado. Os dados hierárquicos no banco de dados são dispostos em uma única tabela CSV. Nenhum aspecto dos dados tem precedência no arquivo. Nenhuma formatação é usada e não se pressupõe legibilidade humana. O arquivo (chamado MyReport) contém os dados em um formato universalmente consumível. Os arquivos CSV geralmente são usados para arquivamento de dados ou como fonte de dados para uma ferramenta de geração de relatórios ou manipulação de dados, como o Microsoft Excel.
- O relatório HTML fornece uma forma legível por humanos dos dados de log para um intervalo de tempo especificado. Ele fornece uma visualização estruturada e navegável para revisar as alterações. Um relatório HTML é composto por dois arquivos, denominados Summary e Details.

O Summary lista operações de alto nível: quando cada operação ocorreu, por quem e o resultado. Clicar em um link **Details** ao lado de cada operação leva você às operações de baixo nível no arquivo Details, que fornece informações adicionais.

Para gerar um relatório de log de configuração, selecione **Logging** no painel de navegação do Studio e, em seguida, selecione **Create custom report** na barra de ações.

- Selecione o intervalo de datas para o relatório.
- Selecione o formato do relatório: CSV, HTML ou ambos.
- Navegue até o local onde você deseja salvar o relatório.

Excluir conteúdo do log de configuração

Para excluir o log de configuração, você deve ter certas permissões de administração delegada e do banco de dados do SQL Server.

- **Delegated administration:** você deve ter uma função de administração delegada que permita que a configuração de implantação seja lida. A função Full Administrator tem essa permissão. Uma função personalizada deve ter Read Only ou Manage selecionado na categoria Other permissions.

  Para criar um backup dos dados de log de configuração antes de excluí-los, a função personalizada também deve ter Read Only ou Manage selecionado na categoria Logging Permissions.

- **SQL Server database:** você deve ter um login do SQL Server 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 executar qualquer atividade no servidor de banco de dados. Como alternativa, as funções de servidor `serveradmin` ou `setupadmin` permitem que você execute operações de exclusão.
  - Se a sua implantação exigir mais segurança, use um login de banco de dados não sysadmin mapeado para um usuário do banco de dados que tenha permissão para excluir registros do banco de dados.

    1. No SQL Server Management Studio, crie um login do SQL Server com uma função de servidor diferente de "sysadmin".
    2. 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.
    3. Em Database role membership, 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. Entre no Web Studio e selecione **Logging** no painel esquerdo.
2. Selecione **Delete logs** na barra de ações.
3. Você é indagado se deseja criar um backup dos logs antes que eles sejam excluídos. Se você optar por criar um backup, navegue até o local onde o arquivo de backup é salvo. O backup é criado como um arquivo CSV.

Depois que os logs de configuração são eliminados, a exclusão do log é a primeira atividade lançada no log vazio. Essa entrada fornece detalhes sobre quem excluiu os logs e quando.

Logs de eventos

June 28, 2023

Os artigos a seguir listam e descrevem eventos que podem ser registrados em log por serviços dentro do Citrix Virtual Apps and Desktops.

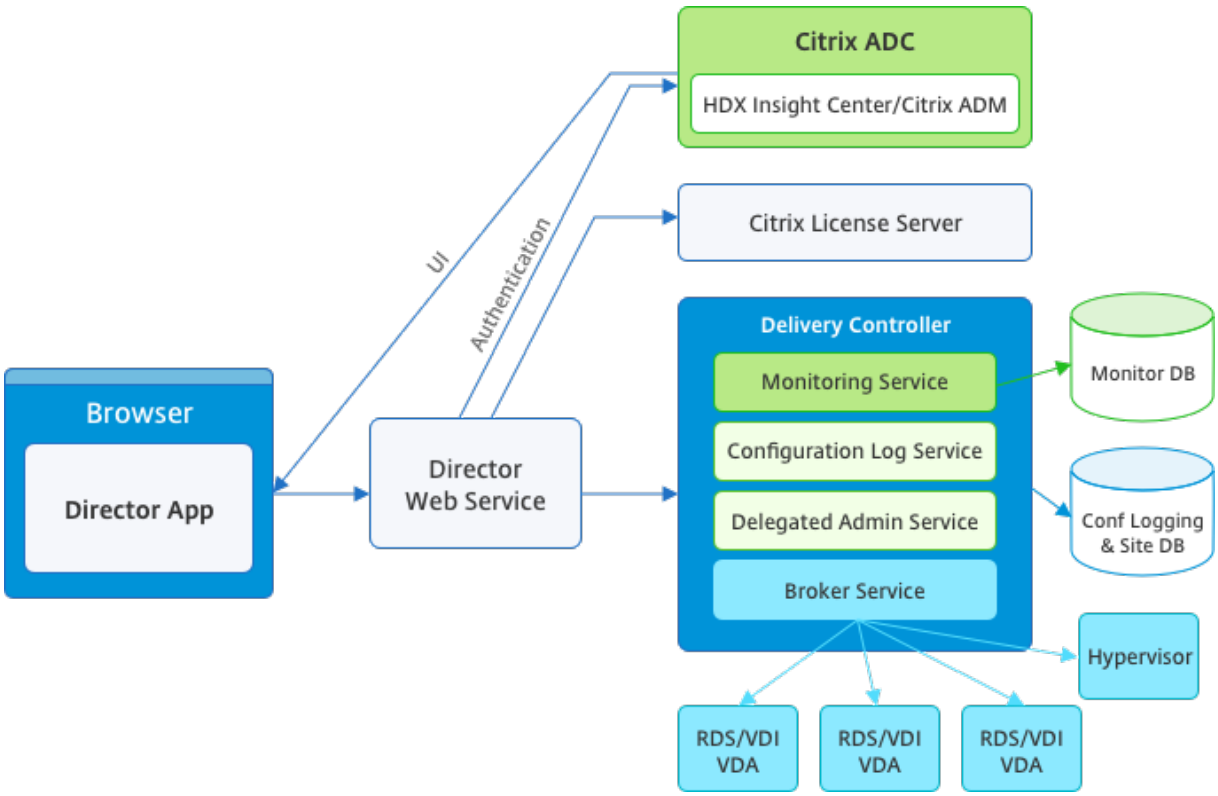
Essas informações não são completas. Os leitores devem verificar artigos sobre os recursos individuais para obter informações adicionais sobre os eventos.

- Eventos do Citrix Broker Service
- Eventos do Citrix FMA Service SDK
- Eventos do Citrix Configuration Service
- Eventos do Citrix Delegated Administration Service

Director

June 28, 2023

O Director é um console de monitoramento e solução de problemas para o Citrix Virtual Apps and Desktops.



O Director pode acessar:

- Dados em tempo real do Broker Agent usando um console unificado integrado ao Analytics, Performance Manager e Network Inspector. As seguintes análises são alimentadas pelo Citrix ADM para identificar gargalos devidos à rede em seu ambiente Citrix Virtual Apps ou Desktops:
  - Gerenciamento de desempenho para garantia de integridade e capacidade
  - Tendências históricas e análise de rede
- Dados históricos armazenados no banco de dados do Monitor para acessar o banco de dados de log de configuração.
- Dados ICA a partir do Citrix Gateway usando o Citrix ADM.
  - Obter visibilidade da experiência do usuário final para aplicativos virtuais, desktops e usuários do Citrix Virtual Apps ou Desktops.
  - Correlacionar dados de rede com dados de aplicativos e métricas em tempo real para solução de problemas eficaz.
  - Integrar com a ferramenta de monitoramento Citrix Virtual Desktop 7 Director.

O Director usa um painel de solução de problemas que fornece monitoramento de integridade histórico e em tempo real do Site Citrix Virtual Apps ou Desktops. Esse recurso permite que você veja falhas em tempo real, dando uma ideia melhor do que os usuários finais estão passando.

Para obter mais informações sobre a compatibilidade de recursos do Director com Delivery Controller

(DC), VDA e quaisquer outros componentes dependentes, consulte Matriz de compatibilidade de recursos.

> **Nota:**
>
> Com a divulgação das vulnerabilidades de canal paralelo de execução especulativa Meltdown e Spectre, a Citrix recomenda que você instale os patches de mitigação relevantes. Esses patches podem afetar o desempenho do SQL Server. Para obter mais informações, consulte o artigo de suporte da Microsoft, Orientação do SQL Server para proteção contra as vulnerabilidades Spectre, Meltdown e Micro-architectural Data Sampling. A Citrix recomenda que você teste a escala e planeje suas cargas de trabalho antes de implantar os patches em seus ambientes de produção.

O Director é instalado por padrão como um site no Delivery Controller. Para ver os pré-requisitos e outros detalhes, consulte a documentação de Requisitos do sistema desta versão. Para obter 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 de vários sites estiver inativo, o logon demora um pouco mais enquanto tenta se conectar ao site que está inativo.

Usar o Director com autenticação por cartão inteligente PIV

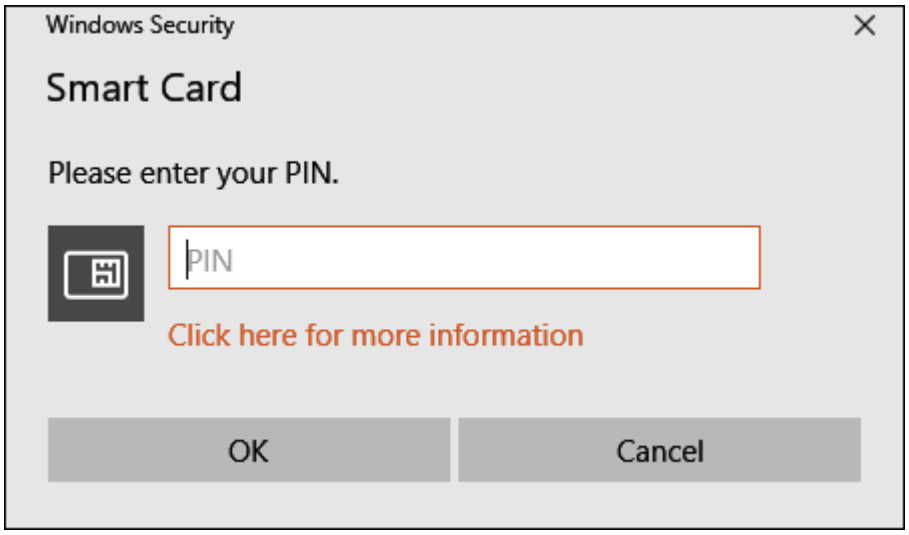
O Director agora oferece suporte à autenticação por cartão inteligente baseada em verificação de identidade pessoal (PIV) para fazer logon. Esse recurso é útil para organizações e agências governamentais que usam autenticação baseada em cartões inteligentes para controle de acesso.
A autenticação por cartão inteligente requer configuração específica no servidor do Director e no Active Directory. As etapas de configuração são detalhadas em Configurar a autenticação por cartão inteligente PIV.

> **Nota:**
>
> A autenticação por cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

Depois de realizar a configuração necessária, você pode fazer logon no Director usando um cartão inteligente:

1. Insira seu cartão inteligente no leitor de cartão inteligente.
2. Abra um navegador e vá para a URL do Director, `https://<directorfqdn>/Director`.

3. Selecione um certificado de usuário válido na lista exibida.
4. Digite seu token de cartão inteligente.



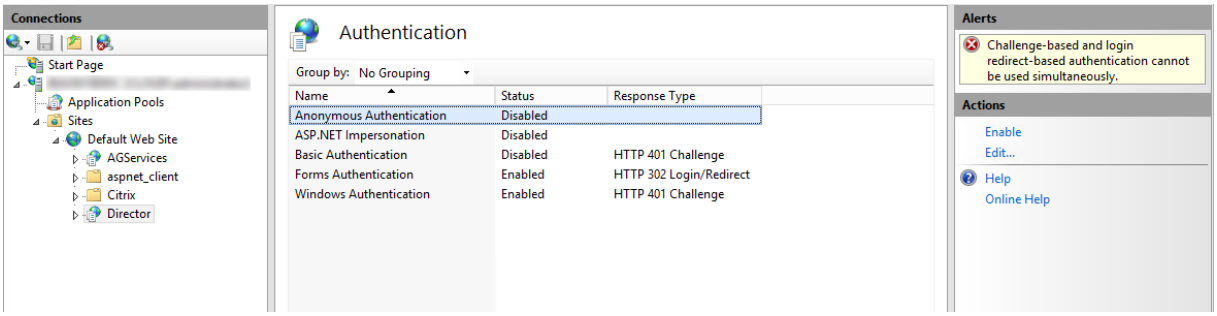
5. Depois de autenticado, você pode acessar o Director sem digitar credenciais extras na página de logon do Director.

Usar Director com Autenticação Integrada do Windows

Com a Autenticação Integrada do Windows (IWA), os usuários ingressados no domínio obtêm acesso direto ao Director sem redigitar suas credenciais na página de logon do Director. Os pré-requisitos para trabalhar com Autenticação Integrada do Windows e Director são:

- Ativar a Autenticação Integrada do Windows no site do IIS que hospeda o Director. Quando você instala o Director, as autenticações anônimas e de formulários são ativadas. Para dar suporte ao Director e à Autenticação Integrada do Windows, desative a Autenticação Anônima e ative a Autenticação do Windows. A Autenticação de Formulários deve permanecer definida como Ativado para a autenticação de usuários sem domínio.

  1. Inicie o gerenciador do IIS.
  2. Vá para **Sites** > **Site Padrão** > **Director**.
  3. Selecione **Autenticação**.
  4. Clique com o botão direito em **Autenticação anônima** e selecione **Desativar**.
  5. Clique com o botão direito em **Autenticação do Windows** e selecione **Ativar**.



- Configurar a permissão de delegação do Active Directory para o computador do Director. A configuração só é necessária se o Director e o Delivery Controller estiverem instalados em computadores separados.

    1. No computador do Active Directory, abra o Console de Gerenciamento do Active Directory.
    2. No Console de Gerenciamento do Active Directory, navegue até **Nome de domínio** > **Computadores.** Selecione o computador do Director.
    3. Clique com o botão direito e selecione **Propriedades**.
    4. Em Propriedades, selecione a guia **Delegação**.
    5. Selecione a opção **Confiar no computador para delegação a qualquer serviço (apenas Kerberos)**.

- O navegador usado para acessar o Director deve suportar a Autenticação Integrada do Windows. Podem ser necessárias etapas de configuração adicionais 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 suportada posterior 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 expirar, 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**.

Exibições de interface

O Director fornece diferentes exibições da interface adaptadas a administradores específicos. As permissões do produto determinam o que é exibido e os comandos disponíveis.

Por exemplo, os administradores do suporte técnico veem uma interface personalizada para tarefas de suporte técnico. O Director permite que os administradores do suporte técnico pesquisem o usuário que relata um problema e exibe a atividade associada a esse usuário. Por exemplo, o status dos aplicativos e processos do usuário. Eles podem resolver problemas rapidamente executando ações como encerrar um aplicativo ou processo que não responde, acompanhando operações no computador do usuário, reiniciando o computador ou redefinindo o perfil do usuário.

Em contraste, os administradores totais veem e gerenciam todo o site e podem executar comandos para vários usuários e computadores. O Painel oferece uma visão geral dos principais aspectos de uma implantação, como o status das sessões, logons de usuário e a infraestrutura do site. As informações são atualizadas a cada minuto. Se ocorrerem problemas, os detalhes serão exibidos automaticamente sobre o número e o tipo de falhas ocorridas.

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 Director Service começa usando o Google Analytics para coletar dados de uso após a instalação do Director. São coletadas estatísticas sobre o uso das páginas de Tendências e da análise de chamadas da API OData. A coleção do Analytics está em conformidade com a Política de Privacidade da Citrix. A coleta de dados é ativada por padrão quando você instala o Director.

Para recusar a coleta de dados do Google Analytics, edite a chave do registro no computador em que o Director está instalado. Se a chave do registro não existir, crie e defina-a com o valor desejado. Atualize a instância do Director depois de alterar o valor da chave do registro.

Cuidado: Usar o Editor do Registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. A Citrix recomenda que você faça backup do Registro do Windows antes de alterá-lo.

Localização: 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:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2
3 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
     DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

Guia de novos recursos

O Director tem um guia dentro do produto que usa o Pendo para dar um insight sobre os novos recursos contidos na versão atual do Director. Uma visão geral rápida acrescida de mensagens apropriadas no produto ajuda você a entender o que há de novo no produto.

Para recusar esse recurso, edite a chave do registro, conforme descrito abaixo, no computador em que o Director está instalado. Se a chave do registro não existir, crie e defina-a com o valor desejado. Atualize a instância do Director depois de alterar o valor da chave do registro.

> **Cuidado:**
>
> Usar o Editor do Registro incorretamente pode causar sérios problemas que exigirão que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. 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
```

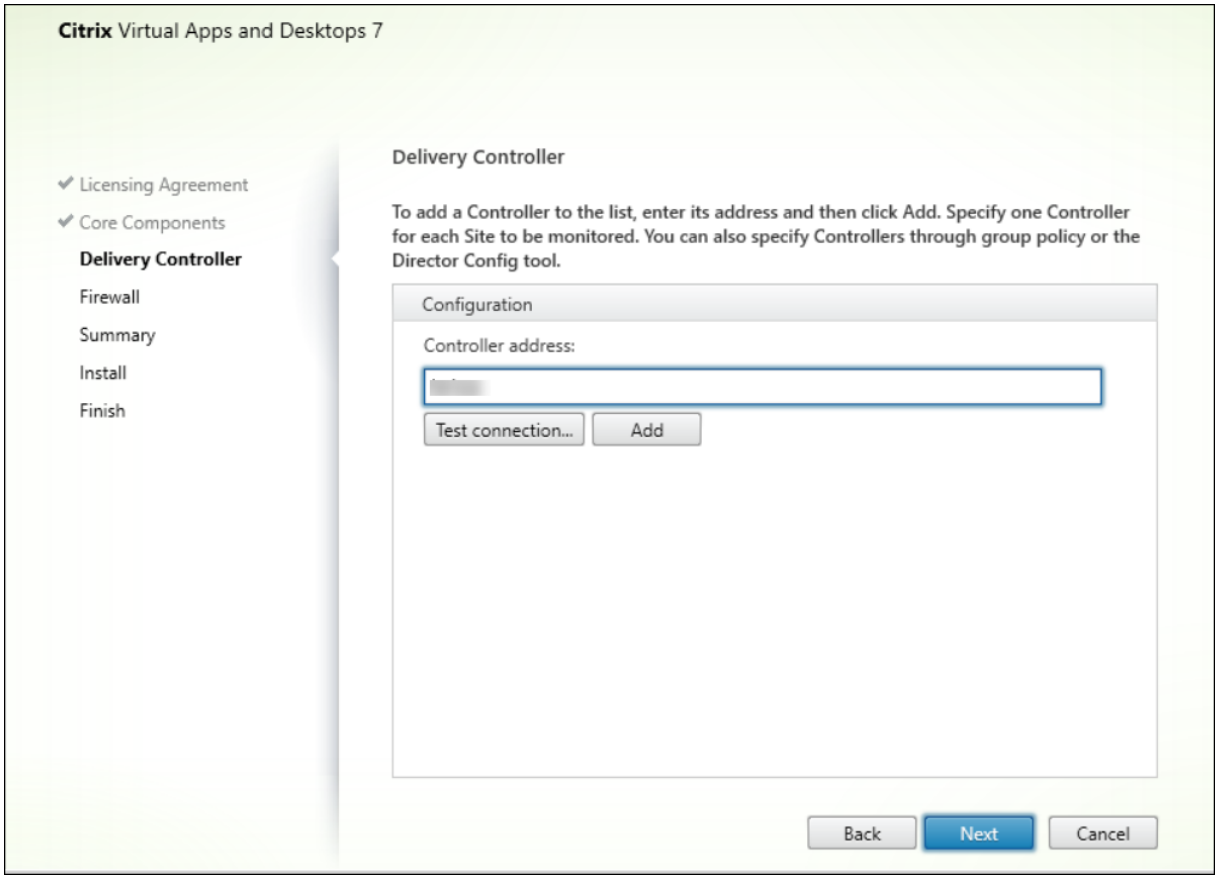
Instalar e configurar

September 13, 2023

Instalar o Director

Instale o Director usando o instalador ISO do produto completo para Citrix Virtual Apps and Desktops, que verifica os pré-requisitos, instala os componentes ausentes, configura o site do Director e executa a configuração básica. Para ver os pré-requisitos e outros detalhes, consulte a documentação de Requisitos do sistema desta versão. Esta versão do Director não é compatível com implantações do Virtual Apps anteriores à versão 6.5 ou implantações do Virtual Desktops anteriores à versão 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 outros componentes, 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 realize a instalação usando apenas o instalador ISO do produto completo, 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 distante de um Controller, você será solicitado a inserir o FQDN ou o endereço IP do Controller.



> **Nota:**
>
> Clique em **Adicionar** para adicionar o Controller a ser monitorado.

O Director se comunica com o Controller especificado por padrão. Especifique o endereço de apenas um Controller para cada site que você monitora. O Director detecta automaticamente todos os outros Controllers no mesmo site e faz o fallback para esses outros Controllers se o Controller especificado falhar.

> **Nota:**
>
> O Director não faz o balanceamento de carga entre os Controllers.

Para proteger as comunicações entre o navegador e o servidor Web, a Citrix recomenda que você implemente o 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 for usado em um ambiente que contém mais de um site, certifique-se de sincronizar os relógios do sistema em todos os servidores em que 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 pela rede usando texto simples, permita conexões do Director usando somente HTTPS, 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 de segurança potencial 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 o 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 de Assistência Remota do Windows está ativado 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, por padrão, ela é desativada no servidor. O recurso não precisa ser ativado para que o Director forneça assistência aos usuários finais. A Citrix recomenda deixar o recurso desativado para melhorar a segurança no servidor.
  - Para permitir que os administradores iniciem a Assistência Remota do Windows, concedalhes as permissões necessárias usando as configurações apropriadas da Política de Grupo da Microsoft para Assistência Remota. Para obter informações, consulte CTX127388: How to Enable Remote Assistance for Desktop Director.

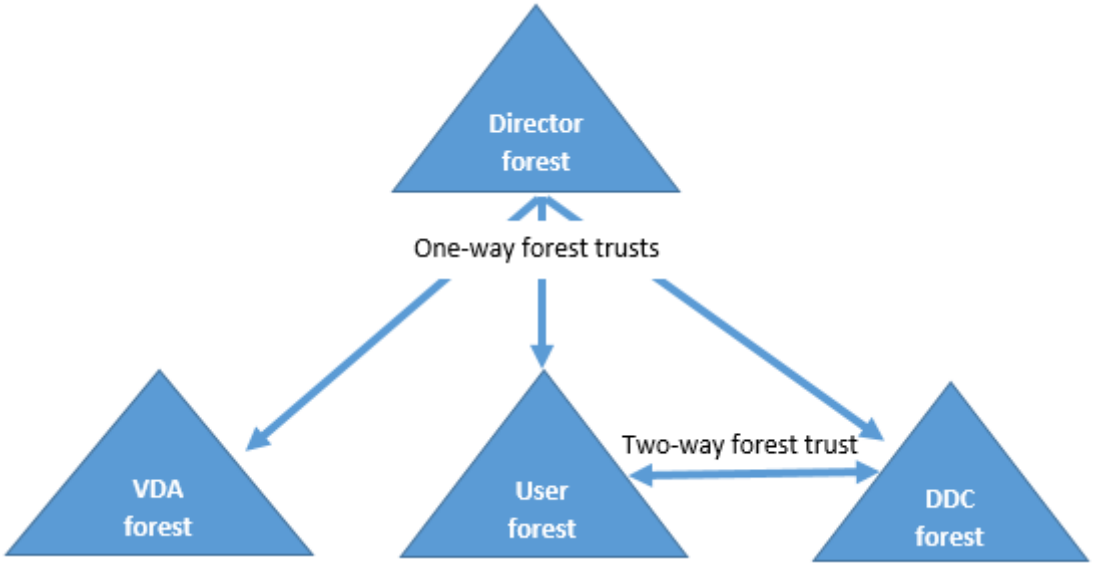
Configuração avançada

June 28, 2023

O Director pode oferecer suporte a ambientes multifloresta, cobrindo uma configuração de floresta em que usuários, Delivery Controllers (DCs), VDAs e Directors estão localizados em diferentes florestas. Isso requer a definição adequada das relações de confiança entre as florestas e os parâmetros de configuração.

Configuração recomendada em um ambiente multifloresta

A configuração recomendada requer a criação de relações de confiança da floresta de saída e 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 diferentes florestas.

A configuração avançada necessária para que o Director ofereça suporte a várias florestas é controlada por meio de configurações definidas no Gerenciador de Serviços de Informações da Internet (IIS).

> **Importante:**
>
> Quando você altera uma configuração no IIS, o Director Service automaticamente reinicia e faz o logoff dos usuários.

Para definir configurações avançadas usando o IIS:

1. Abra o console do Gerenciador de Serviços de Informações da Internet (IIS).

2. Acesse o site do Director sob o site padrão.
3. Clique duas vezes em **Application Settings**.
4. Clique duas vezes em uma configuração para editá-la.
5. Clique em **Add** para adicionar uma nova configuração.

O Director usa o Active Directory para pesquisar usuários e procurar mais informações sobre usuários e computadores. Por padrão, o Director pesquisa no domínio ou floresta em que:

- A conta do administrador é um membro.
- O servidor Web Director é um membro (se diferente).

O Director tenta realizar pesquisas no nível da floresta usando o catálogo global do Active Directory. Se você não tiver permissões para pesquisar no nível da floresta, somente o domínio é pesquisado.

Pesquisar ou procurar dados de outro domínio ou floresta do Active Directory requer 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 usuário e servidor 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:

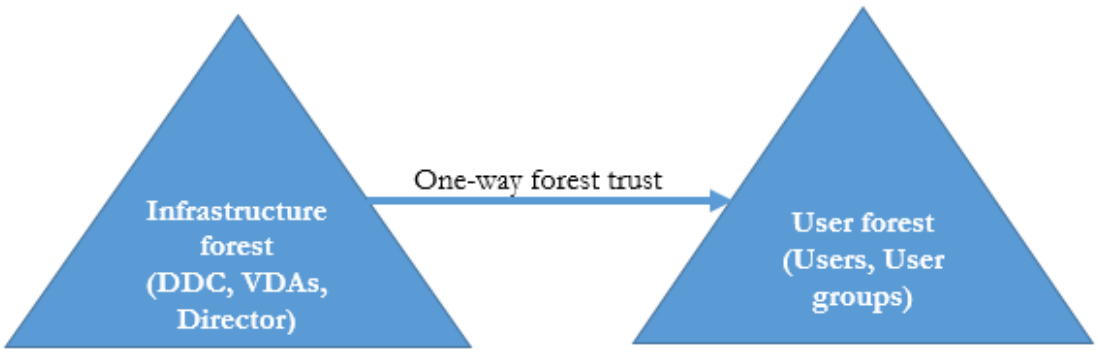
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

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, somente o domínio é pesquisado.

Configuração de grupo local de domínio

A maioria dos Citrix Service Providers (CSPs) tem configurações de ambiente semelhantes, consistindo em VDAs, DCs e Director na floresta de infraestrutura. Os registros de usuários ou grupos de usuários pertencem à floresta do cliente. Existe uma confiança de saída unidirecional da floresta de infraestrutura à floresta do cliente.

Os administradores CSP geralmente criam um grupo local de domínio na floresta de infraestrutura e adicionam os usuários ou grupos de usuários na floresta do cliente a esse grupo local de domínio.



O Director pode oferecer suporte a uma configuração multifloresta como essa 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= \<domain1\>,\<domain2\>
```

   <domain1><domain2> são os nomes das florestas nas quais o grupo local de domínio existe.

2. Atribua o grupo local de domínio aos grupos de entrega no Web Studio.
3. Reinicie o IIS e faça logon no Director novamente para que as alterações entrem em vigor. Agora, o Director pode monitorar e mostrar as sessões desses usuários.

Adicionar sites ao Director

Se o Director já estiver instalado, configure-o para trabalhar 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
<!--NeedCopy-->
```

SiteAController e SiteBController são os endereços de Delivery Controllers de dois sites diferentes.

Desativar a visibilidade de aplicativos em execução no Activity Manager

Por padrão, o Activity Manager no Director exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Essas informações são visualizadas por todos os administradores que têm

acesso ao recurso Activity Manager no Director. Para funções de administrador delegado, inclui administrador completo, administrador de grupo de entrega e administrador de assistência técnica.

Para proteger a privacidade dos usuários e os aplicativos que estão executando, você pode desativar a guia **Applications** para listar aplicativos em execução.

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

1. No VDA, modifique a chave de registro em HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDat
   Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, portanto, não são exibidas no Activity Manager.
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 de aplicativos em execução na guia Applications. Altere o valor para "false", o que desativa a visibilidade. Essa opção afeta apenas o Activity Manager no Director, não o VDA.
   Modifique o valor do seguinte parâmetro:
   UI.TaskManager.EnableApplications = false

> **Importante:**
>
> Para desativar a exibição de aplicativos em execução, faça as duas alterações para garantir que os dados não sejam exibidos no Activity Manager.

Configurar a autenticação por cartão inteligente PIV

June 28, 2023

Este artigo lista a configuração necessária no Director Server e no Active Directory para habilitar o recurso de autenticação por cartão inteligente.

> **Nota:**
>
> A autenticação por cartão inteligente é suportada apenas para usuários do mesmo domínio do Active Directory.

Configuração do servidor do Director

Execute as seguintes etapas de configuração no servidor do Director:

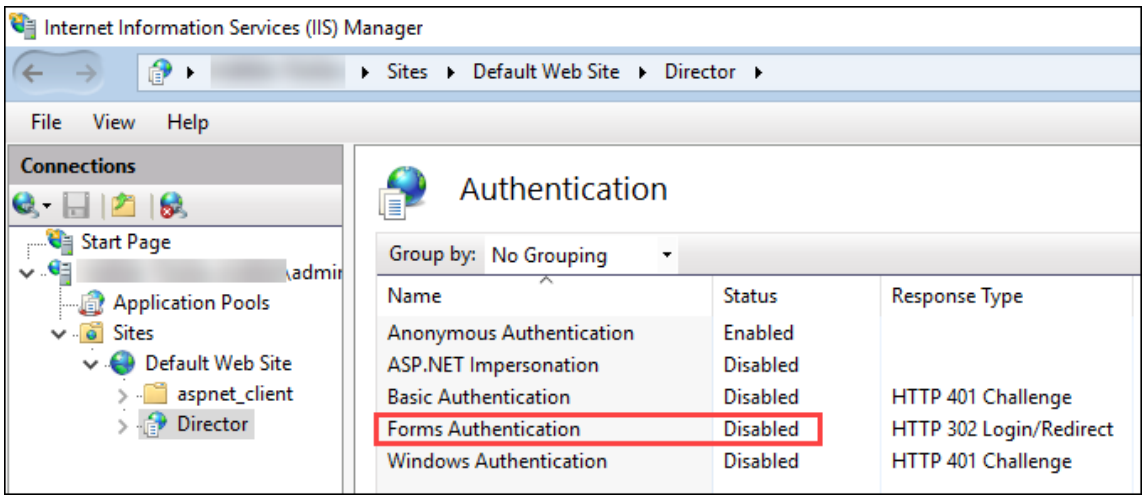
1. Instale e ative a autenticação de mapeamento de certificado de cliente. Siga as instruções em **Client Certificate Mapping authentication using Active Directory** no documento da Microsoft, Client Certificate Mapping Authentication.
2. Desabilite a autenticação de formulários no site do Director.

   Inicie o Gerenciador do IIS.

   Vá para **Sites** > **Site Padrão** > **Director**.

   Selecione **Autenticação**.

   Clique com o botão direito em **Autenticação de formulários** e selecione **Desativar.**



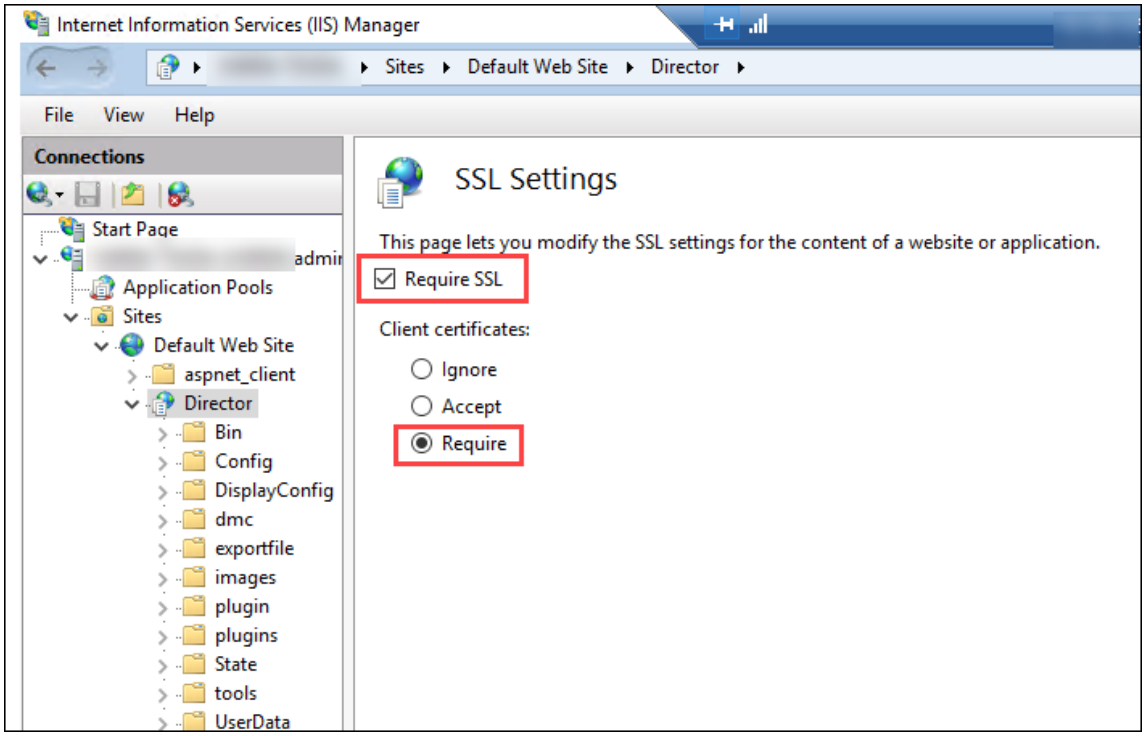
3. Configure a URL do Director com o protocolo https mais seguro (em vez de HTTP) para autenticação de certificado de cliente.

   a) Inicie o Gerenciador do IIS.

   b) Vá para **Sites** > **Site Padrão** > **Director**.

   c) Selecione **Configurações de SSL.**

   d) Selecione **Exigir SSL** e **Certificados de cliente** > **Exigir.**



4. Atualize web.config. Abra o arquivo web.config (disponível em c:\inetpub\wwwroot\Director) usando um editor de texto.

Sob o elemento pai <system.webServer>, adicione o seguinte trecho como o primeiro elemento filho:

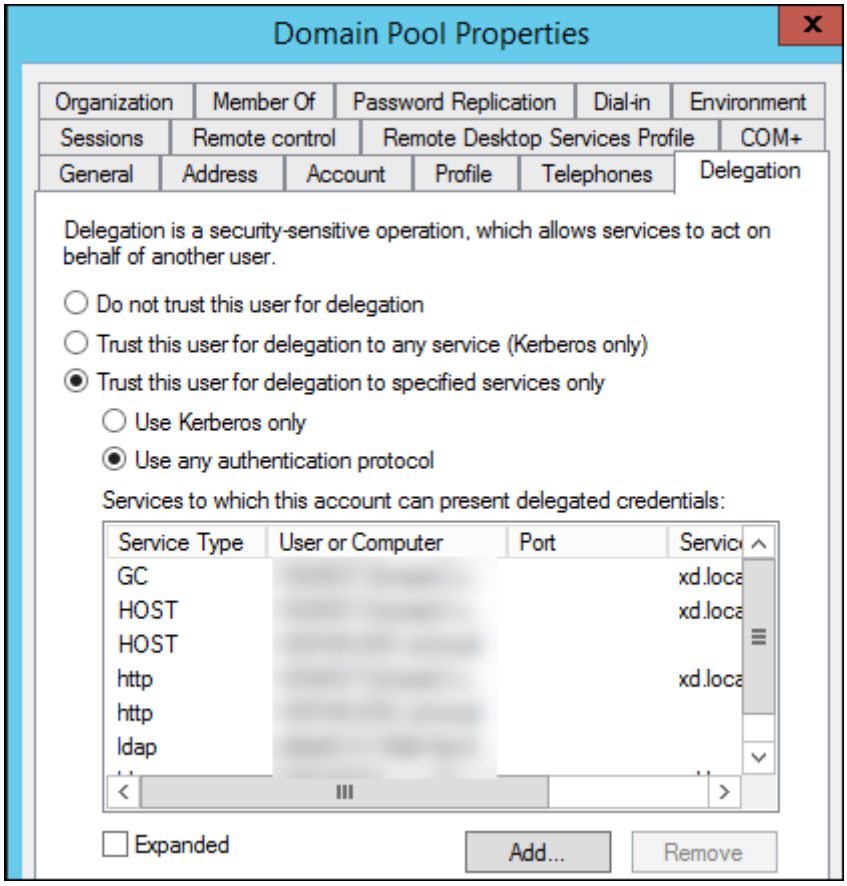
```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

Configuração do Active Directory

Por padrão, o aplicativo Director é executado com a propriedade de identidade **Pool de aplicativos**. A autenticação por cartão inteligente requer delegação para a qual a identidade do aplicativo do Director deve ter privilégios de Base Computacional Confiável (TCB) no host de serviço.

A Citrix recomenda que você crie uma conta de serviço separada para a identidade do Pool de Aplicativos. Crie a conta de serviço e atribua privilégios TCB de acordo com as instruções no artigo do MSDN Microsoft, 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.

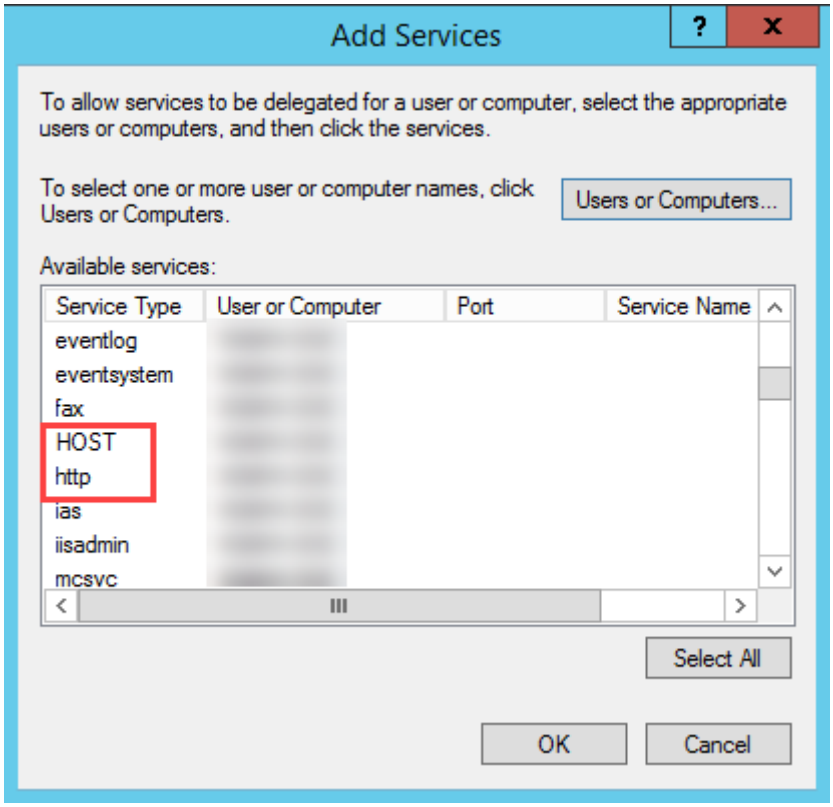


Configure os seguintes serviços para essa conta:

- 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 o **Tipo de serviço** HOST e HTTP.



Da mesma forma, adicione Tipos de serviço para os hosts do **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 Installing OpenSC PKCS#11 Module in Firefox, Step by Step. Para obter informações sobre o uso do recurso de autenticação por cartão inteligente no Director, consulte a seção Usar o Director com autenticação por cartão inteligente PIV no artigo Director.

Configurar análise de rede

June 28, 2023

> **Nota:**
> A disponibilidade desse recurso depende da licença da sua organização e das 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 de aplicativos e áreas de trabalho na rede. Com esse recurso, o Director fornece análises avançadas do tráfego ICA em sua implantação.
- O gerenciamento de desempenho fornece relatórios de tendências e retenção histórica. Com a retenção histórica de dados comparada com a avaliação em tempo real, você pode criar relatórios de tendências, incluindo tendências de capacidade e integridade.

Depois de habilitar esse recurso no Director, os relatórios do HDX Insight fornecem ao Director informações adicionais:

- A guia Network na página Trends mostra os efeitos de latência e largura de banda para aplicativos, áreas de trabalho e usuários em toda a sua implantação.
- A página User Details mostra informações de latência e largura de banda específicas para uma determinada sessão de usuário.

Limitações:

- Na visualização Trends, os dados de logon da conexão HDX não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.

Para habilitar a análise de rede, você deve instalar e configurar o Citrix ADM no Director. O Director requer o Citrix ADM versão 11.1 compilação 49.16 ou posterior. O MAS é um dispositivo virtual executado no Citrix Hypervisor. Usando a análise de rede, o Director comunica e reúne as informações relacionadas à sua implantação.

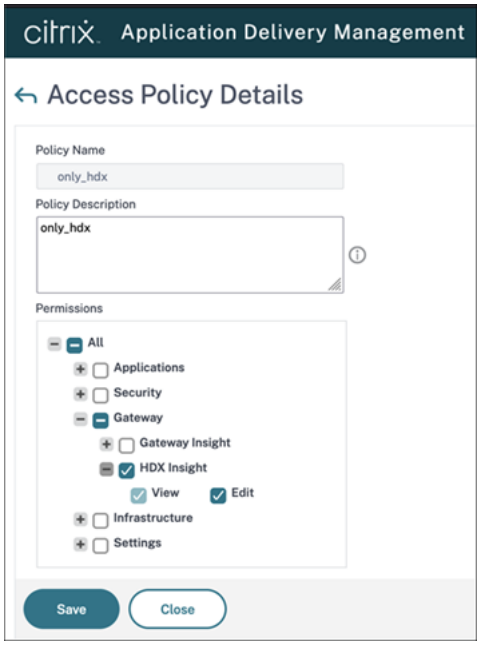
Para obter mais informações, consulte a documentação do Citrix ADM.

> **Nota:**
>
> O Citrix NetScaler Insight Center atingiu a data de Fim da Manutenção em 15 de maio de 2018. Consulte a Citrix Product Matrix. Integre o Director com o Citrix ADM para análise de rede. Para migrar o seu NetScaler Insight Center para o Citrix ADM, consulte Migrate from NetScaler Insight Center to Citrix ADM.

1. No servidor em que 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 do que HTTP) e escolha a integração Citrix ADM.
3. Para verificar as alterações, faça logoff e logon novamente.

> **Nota:**
>
> Por motivos de segurança, é recomendável criar uma função personalizada para a integração do

ADM ao Director com permissão suficiente para acessar somente o HDX Insight.



Para obter mais informações, consulte Configurar políticas de acesso.

Administração delegada e o Director

June 28, 2023

A administração delegada usa três conceitos: administradores, funções e escopos. As permissões são baseadas em uma função de administrador e no escopo dessa função. Por exemplo, um administrador pode receber uma função de administrador de assistência técnica em que o escopo envolve a responsabilidade pelos usuários finais em apenas um site.

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 chamadas de exibição.
- As áreas de trabalho, máquinas e sessões as quais o administrador pode visualizar e com elas interagir.
- Os comandos que o administrador pode executar, como sombrear a sessão de um usuário ou ativar o modo de manutenção.

As permissões e funções internas também determinam como os administradores usam o Director:

Função do administrador	Permissões no Director
Full Administrator	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, ativar o modo de manutenção e exportar dados de tendências.
Delivery group Administrator	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, ativar o modo de manutenção e exportar dados de tendências.
Read Only Administrator	Pode acessar todas as exibições e ver todos os objetos em escopos especificados e informações globais. Pode baixar relatórios de canais HDX e exportar dados de tendências usando a opção Export na exibição Trends. Não é possível executar nenhum outro comando nem alterar nada nas exibições.
Help Desk Administrator	Pode acessar somente as exibições Help Desk e User Details e pode exibir somente objetos que o administrador foi delegado para gerenciar. Pode sombrear a sessão de um usuário e executar comandos para esse usuário. Pode realizar operações no modo de manutenção. Pode usar opções de controle de energia para máquinas com SO de sessão única. Não pode acessar as exibições Dashboard, Trends, Alerts ou Filters. Não pode usar opções de controle de energia para máquinas com SO multissessão.
Administrador de catálogo de máquinas	Pode acessar somente a página Machine Details (pesquisa baseada em máquina).
Host Administrator	Nenhum acesso. Este administrador não é compatível com o Director e não pode exibir dados.

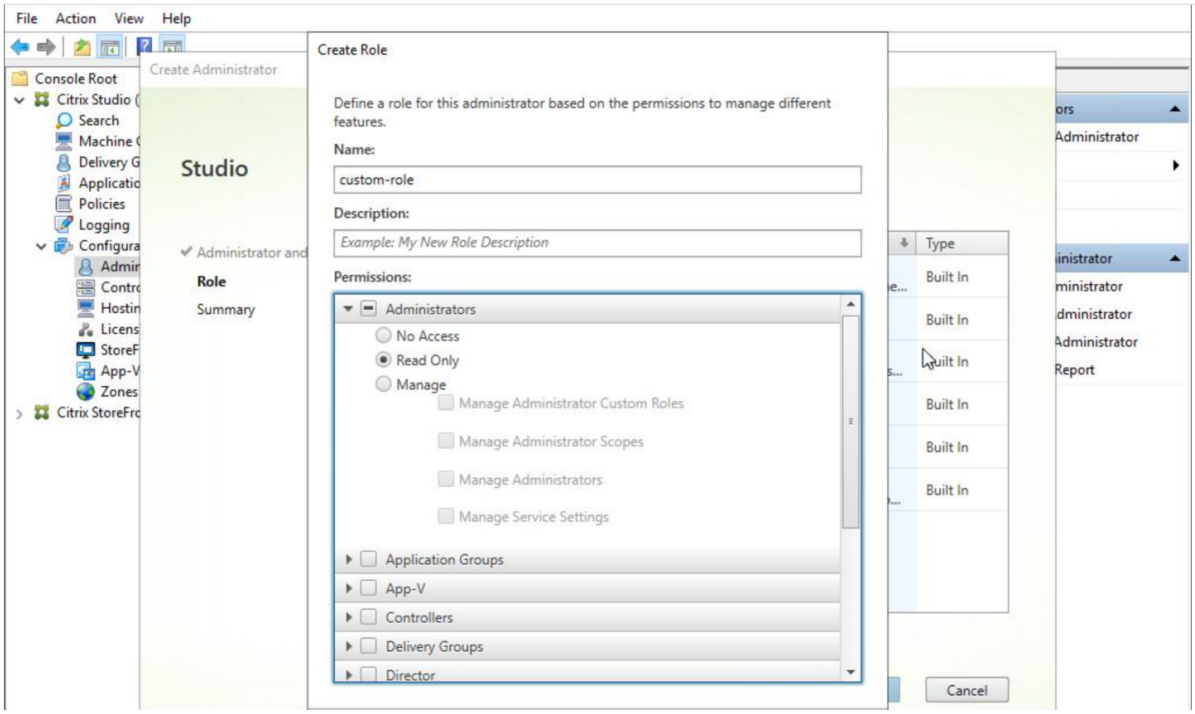
Configurar funções personalizadas para administradores do Director

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 interna de administrador de assistência técnica para que

esse administrador não possa fazer logoff das sessões.

Se você criar uma função personalizada com permissões do Director, também deverá dar a essa função outras permissões genéricas:

- Permissão de Delivery Controller para fazer logon no Director –pelo menos acesso somente leitura no nó Administrador
- Permissões para grupos de entrega para exibir os dados relacionados aos grupos de entrega no Director –pelo menos acesso somente leitura



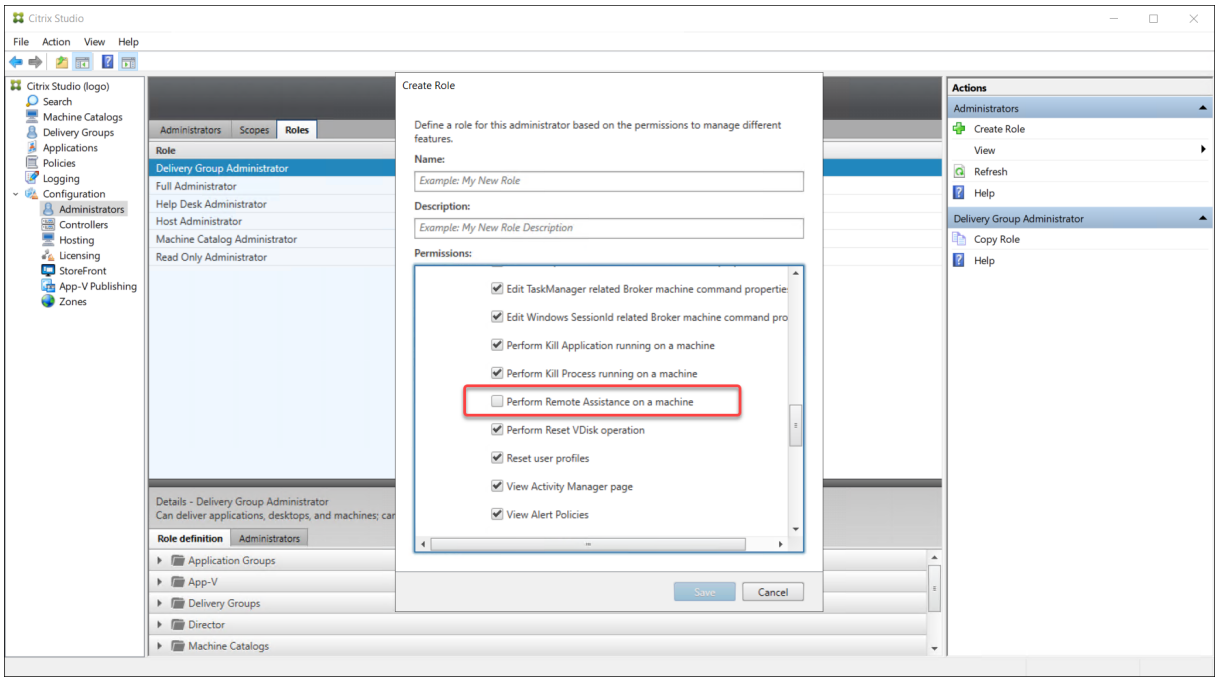
Como alternativa, você pode criar uma função personalizada copiando uma função existente e incluir permissões extras para outras exibições. Por exemplo, você pode copiar a função de assistência técnica Help Desk e incluir permissões para exibir as páginas Dashboard ou Filters.

Selecione as permissões do Director para a função personalizada, que incluem:

- Perform Kill Application running on a machine
- Perform Kill Process running on a machine
- Perform Remote Assistance on a machine
- Reset user profiles
- View Client Details page
- View Dashboard page
- View Filters page
- View Machine Details page
- Exibir a página de tendências

- View User Details page

Neste exemplo, o sombreamento (Perform Remote Assistance on a machine) está desativado.



Uma permissão pode depender de outras permissões para ser aplicável à interface do usuário. Por exemplo, selecionar a permissão **Perform Kill Application running on a machine** ativa a funcionalidade **End Application** somente nos painéis aos quais a função tem permissão. Você pode selecionar as seguintes permissões de painel:

- View Filters page
- View User Details page
- View Machine Details page
- View Client Details page

Além disso, na lista de permissões para outros componentes, considere essas permissões de grupos de entrega:

- Ativar/desativar o modo de manutenção de uma máquina usando a associação de grupo de entrega.
- Executar operações de energia em computadores Windows Desktop usando a associação de grupo de entrega.
- Executar o gerenciamento de sessões em máquinas usando a associação de grupo de entrega.

Implantação segura do Director

June 28, 2023

Este artigo destaca áreas que podem ter impacto na segurança do sistema ao implantar e configurar o Director.

Configurar Serviços de Informações da Internet (IIS) da Microsoft

Você pode configurar o Director com uma configuração restrita do IIS.

Limites de reciclagem do pool de aplicativos

Você pode definir os seguintes limites de reciclagem do pool de aplicativos:

- Limite de memória virtual: 4.294.967.295
- Limite de memória privada: o tamanho da memória física do servidor StoreFront
- Limite de solicitação: 4.000.000.000

Extensões de nome de arquivo

Você pode cancelar a permissão de extensões de nome de arquivo não listadas.

O Director requer estas extensões de nome de arquivo na Filtragem de Solicitações:

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

O Director requer os seguintes verbos HTTP na Filtragem de Solicitações. Você pode cancelar a permissão de verbos não listados.

- GET

- POST
- HEAD

O Director não requer:

- Filtros ISAPI
- Extensões ISAPI
- Programas CGI
- Programas FastCGI

> **Importante:**
>
> - O Director requer Confiança Total. Não defina o nível de confiança .NET global como Alto ou inferior.
> - O Director mantém um pool de aplicativos separado. Para modificar as configurações do Director, selecione o site do Director e modifique.

Configurar direitos de usuário

Quando o Director é instalado, seus pools de aplicativos recebem o seguinte:

- Direito de logon **Log on as a service**
- Privilégios **Adjust memory quotas for a process**, **Generate security audits** e **Replace a process level token**

Os direitos e privilégios mencionados são um comportamento normal de instalação quando os pools de aplicativos são criados.

Você não precisa alterar esses direitos de usuário. Esses privilégios não são usados pelo Director e são desativados automaticamente.

Comunicações do Director

Em um ambiente de produção, use os protocolos IPsec (Internet Protocol security) ou HTTPS para proteger a passagem de dados entre o Director e seus servidores.

O IPsec é um conjunto de extensões padrão para o protocolo de internet que fornece comunicações autenticadas e criptografadas com integridade de dados e proteção contra reprodução. Como o IPsec é um conjunto de protocolos de camada de rede, os protocolos de nível superior podem usá-lo sem modificação. O HTTPS usa os protocolos TLS (Transport Layer Security) para fornecer criptografia de dados forte.

> **Nota:**
>
> - A Citrix recomenda que você restrinja o acesso ao console do Director na rede intranet.
> - A Citrix recomenda que você não ative conexões não seguras ao Director em um ambiente de produção.
> - Para a segurança das comunicações do Director, é necessária uma configuração para cada conexão separadamente.
> - O protocolo SSL não é recomendado. Em vez disso, use o protocolo TLS mais seguro.
> - Proteja suas comunicações com o Citrix ADC usando TLS, não IPsec.

Para proteger as comunicações entre servidores do Citrix Virtual Apps and Desktops e Director (para monitoramento e relatórios), consulte Data Access Security.

Para proteger as comunicações entre o Director e o Citrix ADC (para Citrix Insight), consulte Configurar análise de rede.

Para proteger as comunicações entre o Director e o servidor de licenças, consulte Secure the License Administration Console.

Separação de segurança do Director

Você pode implantar qualquer aplicativo Web no mesmo domínio da Web (nome de domínio e porta) que o Director. No entanto, quaisquer riscos de segurança nesses aplicativos Web podem reduzir potencialmente a segurança da sua implantação do Director. Quando um maior grau de separação de segurança é necessário, a Citrix recomenda que você implante o Director em um domínio da Web separado.

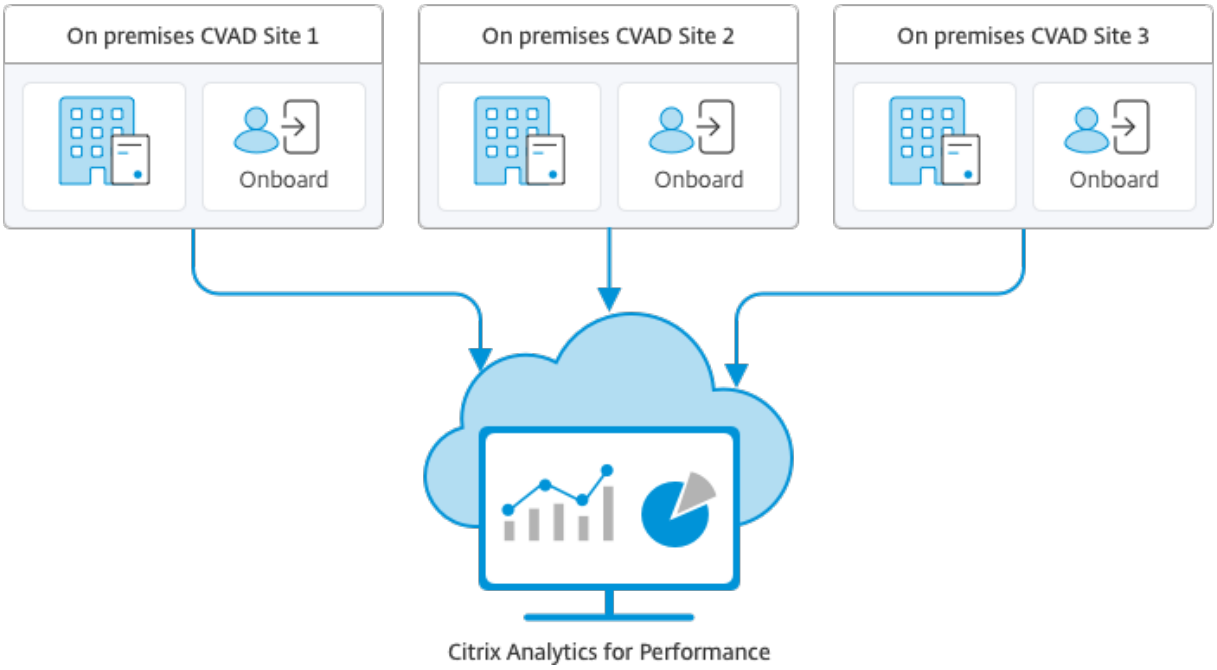
Configurar sites locais com o Citrix Analytics for Performance

September 13, 2023

O Citrix Analytics for Performance (Performance Analytics) é uma solução abrangente de monitoramento de desempenho do Citrix Analytics Cloud Service. A análise de desempenho fornece análises e insights avançados baseados em métricas de desempenho. O Performance Analytics ajuda você a monitorar e visualizar as métricas de uso e desempenho de um ou mais sites do Citrix Virtual Apps and Desktops na sua organização.

Para obter mais informações sobre o Performance Analytics, consulte o artigo Performance Analytics.

Você pode enviar dados de desempenho do seu site para o Citrix Analytics for Performance no Citrix Cloud para utilizar seus recursos avançados de análise de desempenho. Para exibir 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 no Director, não é necessário instalar novos componentes. Certifique-se de que os seguintes requisitos sejam atendidos:

- Seu Delivery Controller e Director sejam da versão 1912 CU2 ou posterior. Para obter mais informações, consulte Matriz de compatibilidade de recursos.

> **Nota:**
>
> - Configurar 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.
> - Quando você configura o 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 Citrix Monitor Service

> no Delivery Controller. Nesse caso, a guia Analytics exibe o status Not Connected. 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 com controle total à pasta Encryption. Reinicie o Citrix Monitor Service.DIR-14324.

- O acesso à guia **Analytics** para realizar essa configuração esteja disponível apenas para administradores completos.
- Para que o Performance Analytics acesse métricas de desempenho, o acesso de saída à Internet esteja disponível em todos os Delivery Controllers e nas máquinas nas quais o Director está instalado. Especificamente, garanta acessibilidade às seguintes URLs:
  - Registro de chave da Citrix: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`
    No caso de os Delivery Controllers e as máquinas do Director estarem dentro de uma intranet e o acesso de saída à Internet ser por meio de um servidor proxy, assegure-se do seguinte:
- O servidor proxy deve permitir a lista anterior de URLs.
- Adicione a seguinte configuração aos arquivos web.config e citrix.monitor.exe.config do Director: Certifique-se de adicionar essa configuração nas marcas de **configuration**:

```
1  <system.net>
2      <defaultProxy>
3          <proxy  usesystemdefault = "false"  proxyaddress = "http
               ://<your_proxyserver_address>:80" bypassonlocal = "
               true"  />
4      </defaultProxy>
5  </system.net>
```

  - O web.config do Director está localizado em `C:\inetpub\wwwroot\Director\web.config` na máquina em que o Director está instalado.
  - O citrix.monitor.exe.config está localizado em `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` na máquina em que o Delivery Controller está instalado.

  Esse parâmetro é fornecido pela Microsoft no IIS. Para obter mais informações, consulte `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.
  O campo **defaultproxy** no arquivo de configuração controla o acesso de saída do Director e do Monitor Service. A configuração e a comunicação com o Performance Analytics exigem que

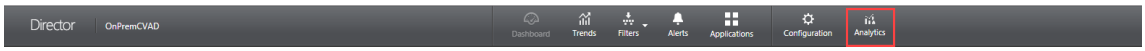
o campo **defaultproxy** seja definido como **true**. É possível que as políticas em vigor definam esse campo como false. Nesse caso, você deve definir manualmente o campo como true. Faça um backup dos arquivos de configuração antes de fazer as alterações. Reinicie o serviço Monitoring no Delivery Controller para que as alterações tenham efeito.

- 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 sobre a experiência de registro de produto. Para obter mais informações sobre permissões de administrador, consulte Modify Administrator Permissions.

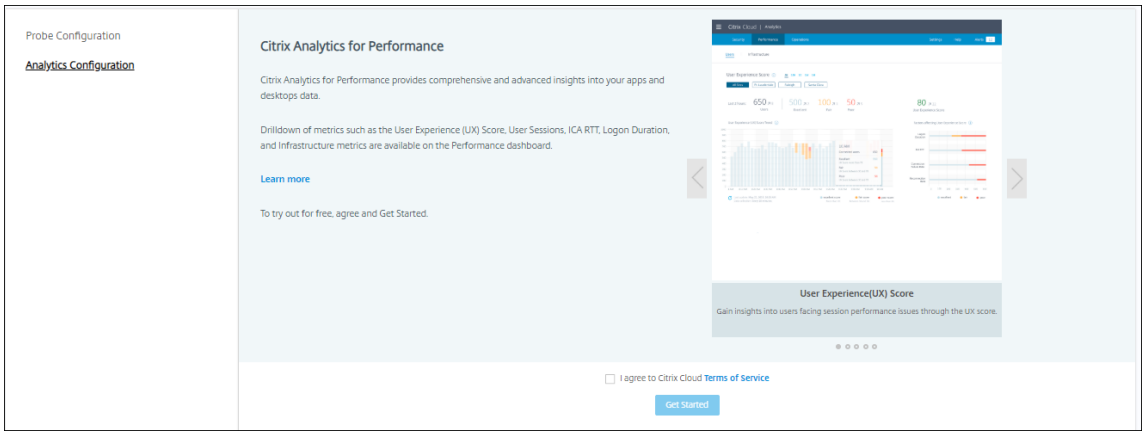
Etapas de configuração

Depois de verificar os pré-requisitos, faça o seguinte:

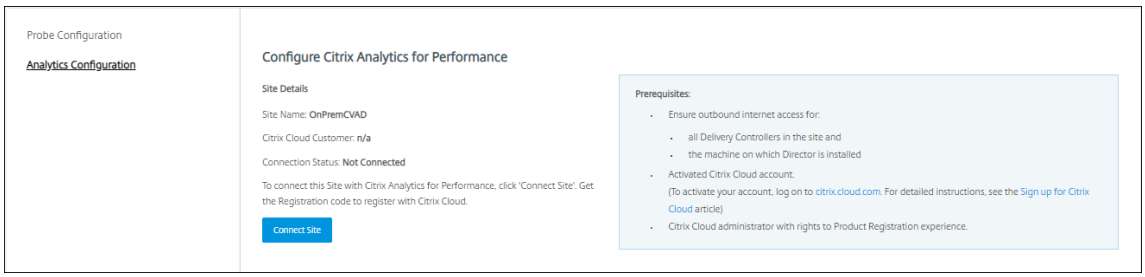
1. Faça logon no Director como administrador completo e selecione o site que deseja configurar com o Performance Analytics.
2. Clique na guia **Analytics**. A página **Configuration** é exibida.



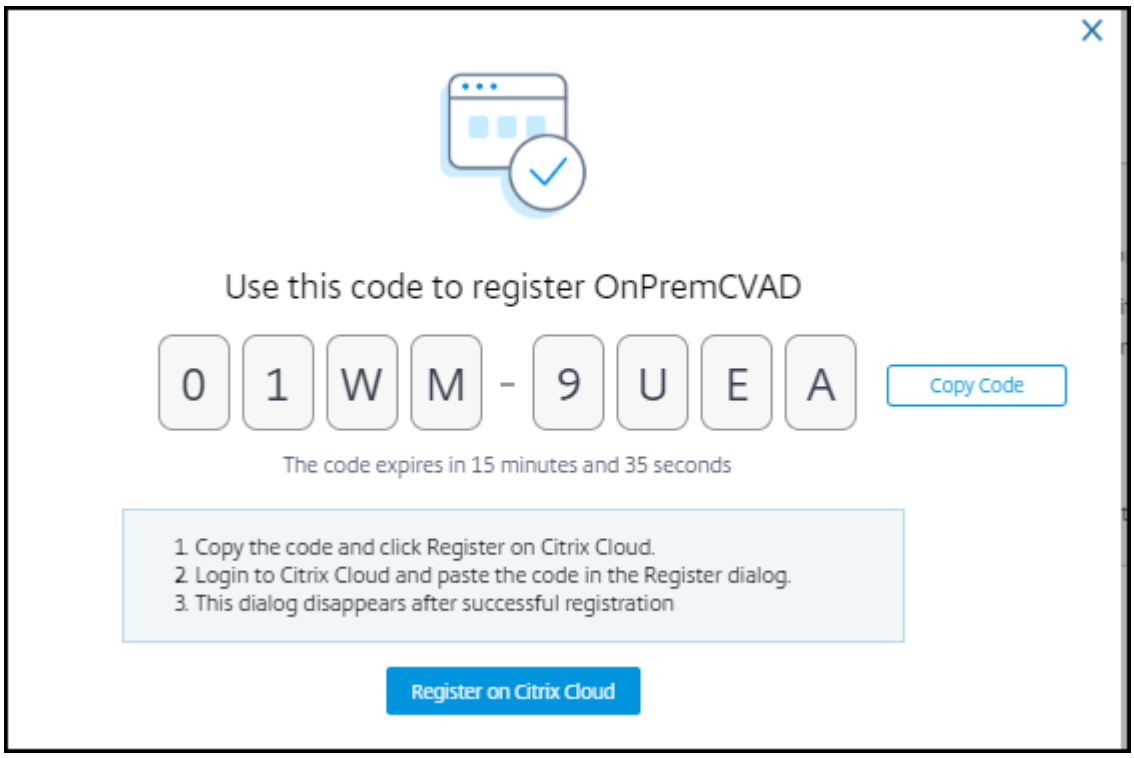
3. Revise as etapas, selecione os termos de serviço e clique em **Get Started**.



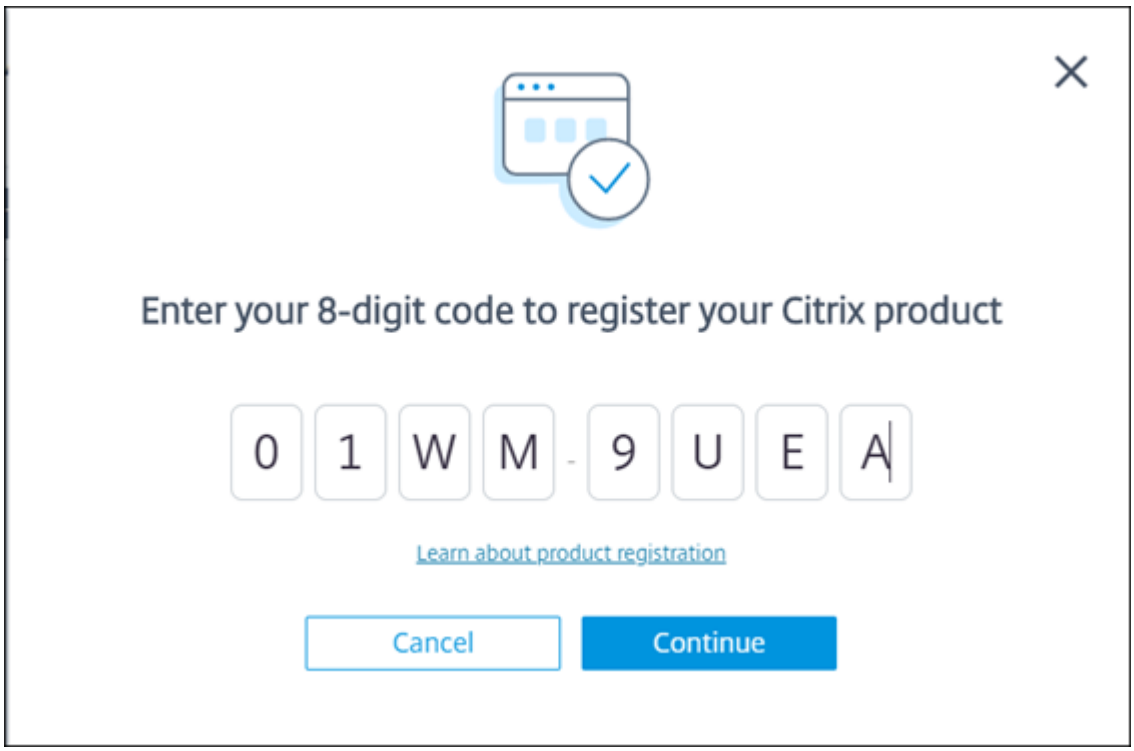
4. Revise os pré-requisitos e certifique-se de que sejam atendidos. Revise os detalhes do site.
5. Clique em **Connect Site** para iniciar o processo de configuração.



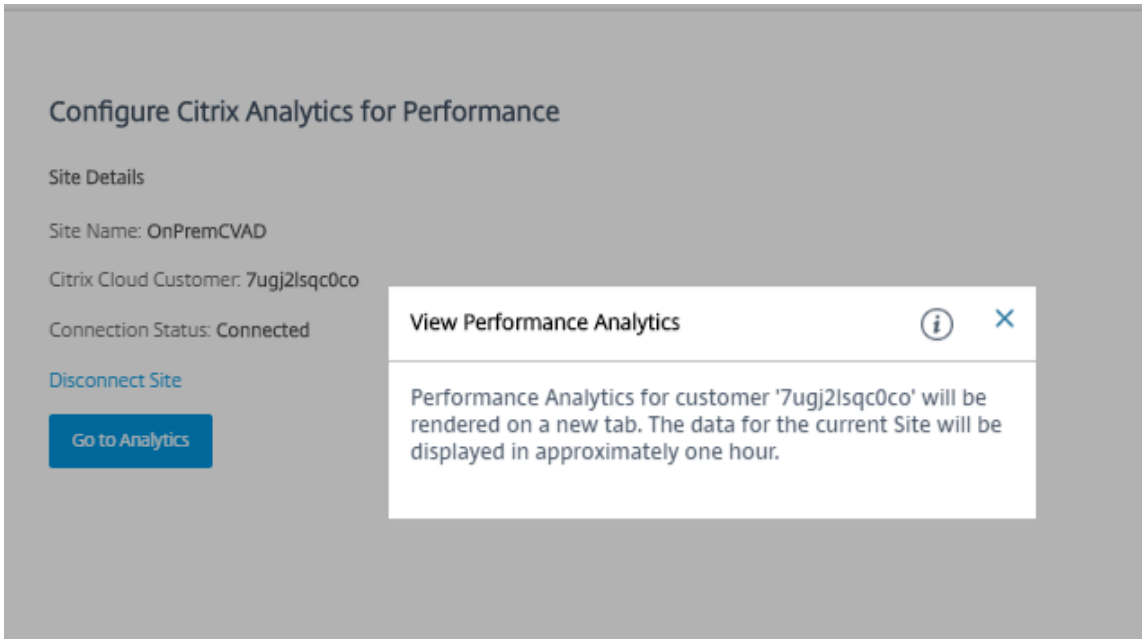
6. Um código de registro exclusivo de 8 dígitos é gerado para ser usado para registrar o site no Citrix Cloud.



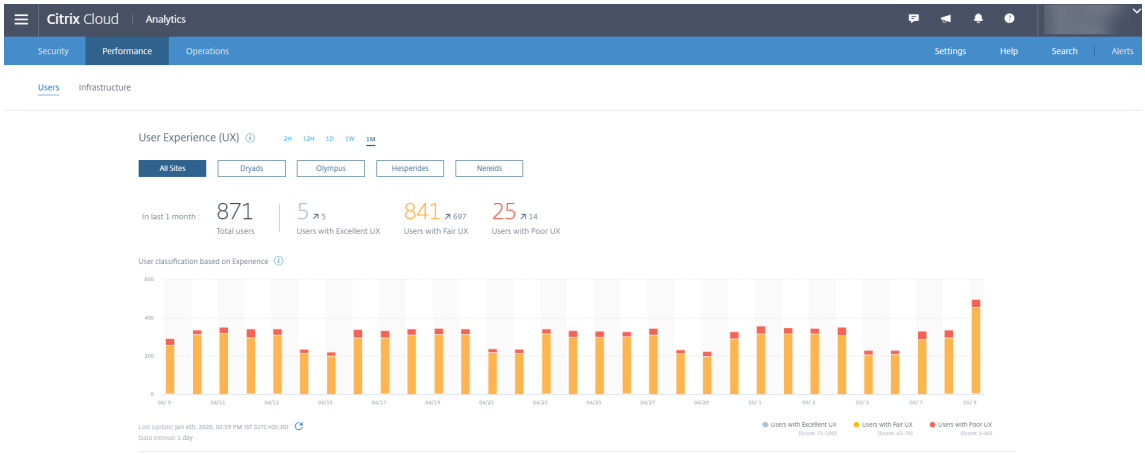
7. Clique em **Copy Code** para copiar o código e, em seguida, clique em **Register on Citrix Cloud**.
8. Você é redirecionado para a URL de registro no Citrix Cloud. Faça login com suas credenciais do Citrix Cloud e selecione o seu cliente.
9. Cole o código de registro copiado na página de registro de produtos no Citrix Cloud. Clique em **Continue** para se registrar. Revise os detalhes do registro e clique em **Register**.



10. Seu site local é registrado no Citrix Cloud. Agora, no **Director**, clique em **Go to Analytics** na guia **Analytics**.



11. O Performance Analytics é aberto em uma nova guia do navegador.



Se a sua sessão do Citrix Cloud expirou, você é redirecionado para a página de logon da conta My Citrix ou Citrix.com.

12. Para registrar vários sites no Performance Analytics, repita as etapas de configuração anteriores para cada site do Director. As métricas para todos os sites configurados são exibidas no painel de análise de desempenho.

    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 serão atualizadas no próximo recarregamento após o processo de configuração.

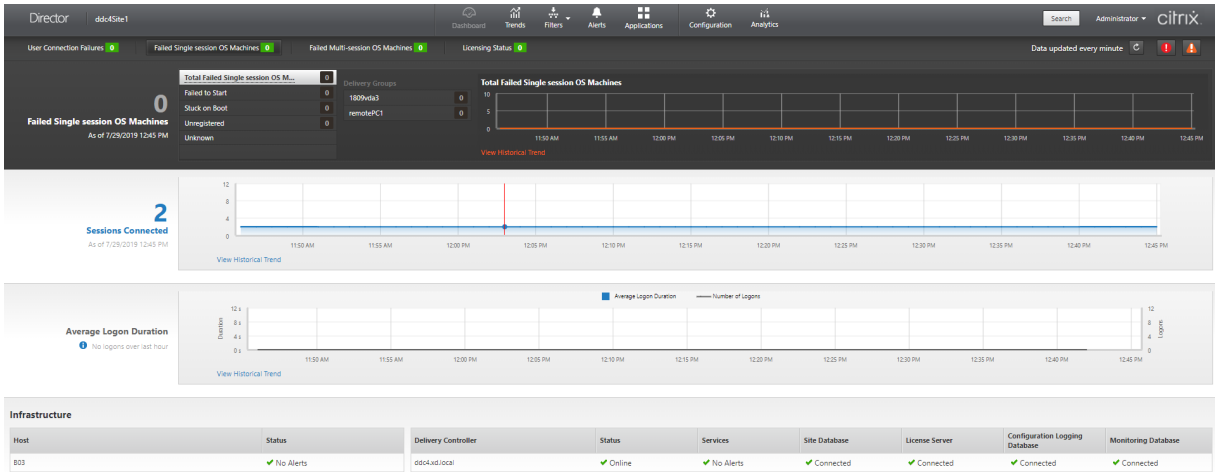
13. Para desconectar seu site do Citrix Cloud, clique em **Disconnect Site**. Essa opção exclui a configuração existente.

    > **Observações:**
    >
    > Na primeira vez que você configurar 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 de análise de desempenho. Depois disso, os eventos são atualizados a 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 no painel de análise de desempenho.
    >
    > Após o seu direito ao Citrix Analytics Service expirar, demora até um dia para que as métricas parem de ser enviadas do site para o Performance Analytics.

Análise do site

June 28, 2023

Com permissão de administrador total, quando você abre o Director, o painel fornece um local centralizado para monitorar a integridade e o uso de um site.



Se não houver falhas no momento e não tiver ocorrido nenhuma falha nos últimos 60 minutos, os painéis permanecem recolhidos. Quando há falhas, o painel de falhas específico aparece automaticamente.

> **Nota:**
>
> Dependendo da licença da sua organização e dos privilégios de Administrador, algumas opções ou recursos não estarão disponíveis.

Panels on the Director Dashboard

Falhas de conexão do usuário, em User Connection Failures

Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para exibir as métricas desse tipo de falha. Na tabela adjacente, esse número é dividido por grupos de entrega. As falhas de conexão incluem falhas causadas por atingir os limites dos aplicativos. Para obter mais informações sobre os limites de aplicativos, consulte Aplicativos.

Máquinas com SO de sessão única com falha, em Failed Single-session OS Machines, ou máquinas com SO multissessão com falha, em Failed Multi-session OS Machines

Total de falhas nos últimos 60 minutos divididos por grupos de entrega. Falhas divididas por tipos, incluindo falhas na inicialização em Failed to Start, bloqueios na inicialização, em Stuck on Boot, e

cancelamentos de registro, em Unregistered. Para máquinas com SO multissessão, as falhas também incluem máquinas que atingem a carga máxima.

Licenciamento, em Licensing Status

Os alertas do License Server exibem alertas enviados pelo License Server e as ações necessárias para resolver os alertas. Requer o License Server versão 11.12.1 ou posterior. Os alertas do Delivery Controller mostram os detalhes do estado de licenciamento conforme visto pelo Controller e são enviados pelo Controller. Requer o Controller para XenApp 7.6 ou XenDesktop 7.6 ou posterior. Você pode definir o limite para os alertas no Studio. O status do licenciamento exibido em **Delivery Controllers** > **Details** > **Product Editions** > **PLT** indica **Premium** e não **Platinum**.

Estado do período de tolerância, em Grace State

O Director exibe um dos seguintes estados de período de tolerância. Essas informações são obtidas do Delivery Controller.

1. **Not Active:** não se encontra em nenhum tipo de período de tolerância. Limites de licenciamento normais se aplicam.
2. **Out of Box Grace:** 10 conexões nos primeiros 30 dias após uma nova instalação que aponta para um servidor de licenças sem licenças.
3. **Supplemental Grace:** quando todas as licenças são consumidas, um período de tolerância de 15 dias é oferecido para garantir a continuidade dos negócios até que novas licenças sejam adicionadas ou o consumo seja reduzido. São permitidas conexões ilimitadas durante o período de tolerância suplementar. Os usuários não são afetados. Os avisos mostrados no Director não podem ser descartados até que o período de tolerância suplementar expire ou seja redefinido.
4. **Emergency Grace:** 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. O período de tolerância de emergência é válido por 30 dias. Os usuários não são afetados. Os erros mostrados no Director não podem ser descartados até que o servidor de licenças esteja acessível.
5. **Grace Expired:** o período de tolerância de emergência ou o período de carência suplementar expirou.

Para obter mais informações, consulte License overdraft e Supplemental grace period.

Sessões conectadas, em Sessions Connected

Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.

Duração média de logon, em Average Logon Duration

Dados de logon nos últimos 60 minutos. O número grande à esquerda é a duração média de logons durante o intervalo de hora. Os dados de logon de VDAs anteriores ao XenDesktop 7.0 não estão incluídos nessa média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Infraestrutura

Lista a infraestrutura do seu site: hosts e Controllers. Na infraestrutura do Citrix Hypervisor ou VMware, você pode visualizar os alertas de desempenho. Por exemplo, você pode configurar o XenCenter para gerar alertas de desempenho quando o uso de CPU, E/S de rede ou E/S de disco ultrapassar 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 configurar esse valor. Para obter detalhes, consulte a seção XenCenter Performance Alerts na documentação do produto Citrix Hypervisor.

> **Nota:**
>
> Se nenhum ícone aparecer para uma métrica específica, isso indica que a métrica não é suportada pelo tipo de host que você está usando. Por exemplo, nenhuma informação de integridade está disponível para hosts do System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

Continue a corrigir os problemas usando estas opções (que estão documentadas nas seções a seguir):

- Controlar a energia da máquina do usuário
- Prevenir conexões a máquinas

Monitorar sessões

Se uma sessão for desconectada, ela permanece ativa e seus aplicativos continuam em execução, mas o dispositivo do usuário não se comunica mais com o servidor.

Ação	Descrição
Ver a máquina ou sessão conectada de um usuário no momento	Nas exibições Activity Manager e User Details, veja a máquina ou sessão conectada do usuário no momento e uma lista de todas as máquinas e sessões às quais o usuário tem acesso. Para acessar essa lista, clique no ícone do seletor de sessão na barra de título do usuário. Para obter mais informações, consulte Restaurar sessões.
Ver o número total de sessões conectadas em todos os grupos de entrega	Em Dashboard, no painel **Sessions Connected**, veja o número total de sessões conectadas em todos os grupos de entrega nos últimos 60 minutos. Clique no número total grande, que abre a exibição Filters, onde você pode exibir dados gráficos da sessão baseados em grupos de entrega selecionados e intervalos e uso entre os grupos de entrega.
Encerrar sessões ociosas	A exibição Sessions Filters mostra dados relacionados a todas as sessões ativas. Filtre as sessões por usuário associado, grupo de entrega, estado da sessão e tempo ocioso maior que um período de tempo limite. Na lista filtrada, selecione as sessões para logoff ou desconexão. Para obter mais informações, consulte Solucionar problemas de aplicativos.
Ver dados de um período de tempo mais longo	Na exibição Trends, selecione a guia **Sessions** para ver dados de uso detalhados e mais específicos das sessões conectadas e desconectadas durante um período de tempo mais longo (ou seja, totais das sessões anteriores aos últimos 60 minutos). Para ver essas informações, clique em **View historical trends**.

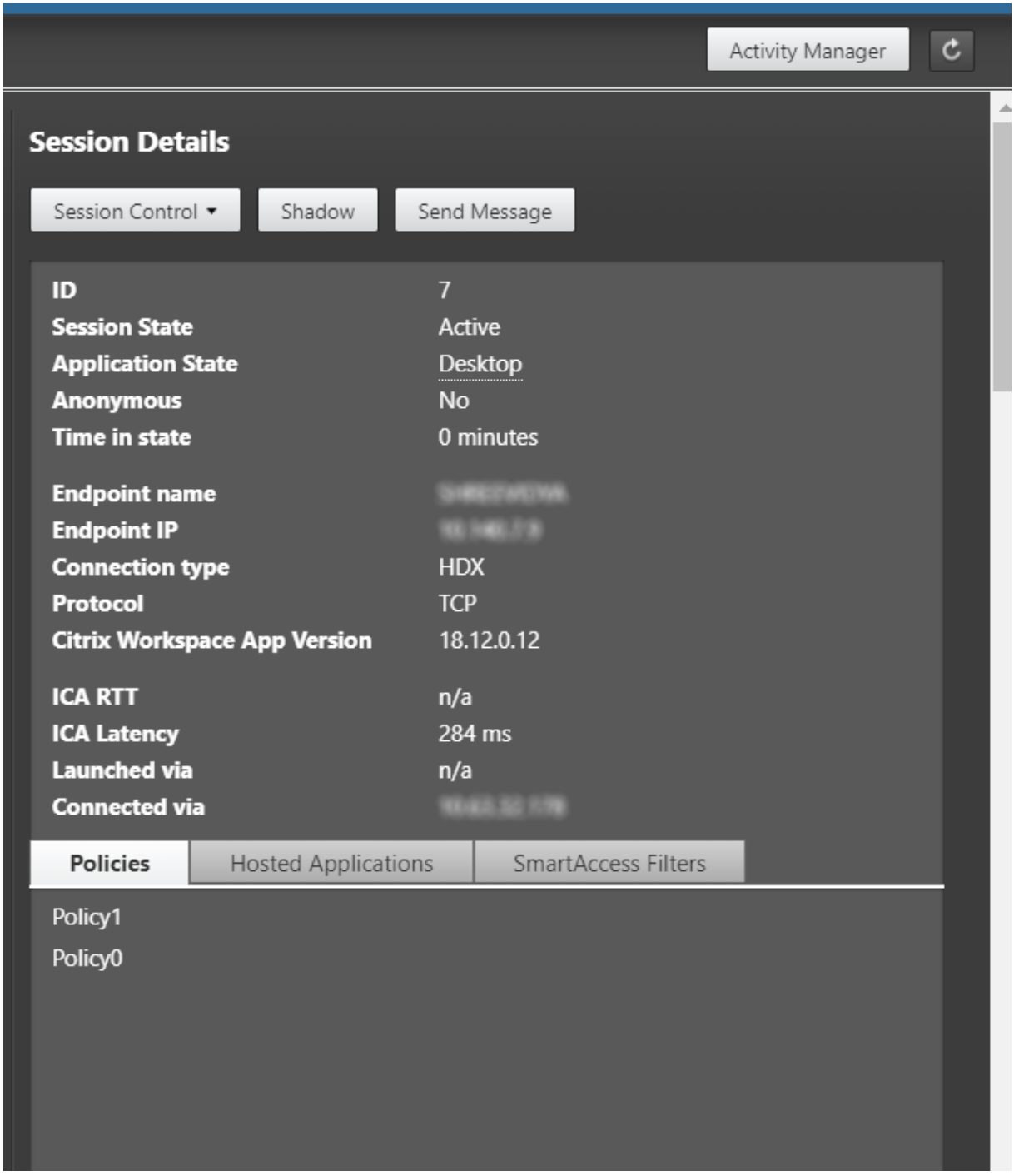
> **Nota:**
>
> Se o dispositivo do usuário estiver executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7 ou um Linux VDA, o Director não consegue exibir as informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem informando que as informações não estão disponíveis.

Limitação das regras de atribuição de área de trabalho:
o Web Studio permite a atribuição de várias regras de atribuição de área de trabalho (DAR) de diferentes usuários ou grupos de usuários para um único VDA no grupo de entrega. O StoreFront exibe a área de trabalho atribuída com o **nome de exibição** correspondente de acordo com o DAR do usuário conectado. No entanto, o Director não oferece suporte a regras DAR e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário conectado. Como resultado, você não pode mapear uma área de trabalho específica a uma máquina no Director. Você pode mapear a área de trabalho atribuída exibida no StoreFront para o nome do grupo de entrega exibido no Director usando o seguinte comando do PowerShell:

```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

Protocolo de transporte de sessão

Veja o protocolo de transporte em uso para o tipo de conexão HDX da sessão atual no painel **Session Details**. Essas informações estão disponíveis para sessões iniciadas em VDAs versão 7.13 ou posteriores.



- Para o tipo de conexão **HDX**:
  - O protocolo é exibido como **UDP**, se EDT for usado para a conexão HDX.
  - O protocolo é exibido como **TCP**, se TCP for usado para a conexão HDX.
- Para o tipo de conexão **RDP**, o protocolo é exibido como **n/a**.

Quando o transporte adaptativo é configurado, o protocolo de transporte de sessão se alterna dinami-

camente entre EDT (por UDP) e TCP com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ocorre o fallback para o protocolo TCP.

Para obter mais informações sobre a configuração de transporte adaptativo, consulte Transporte adaptativo.

Exportar relatórios

Você pode exportar dados de tendências para gerar relatórios regulares de gerenciamento de capacidade e uso. A exportação oferece suporte aos formatos de relatório PDF, Excel e CSV. Relatórios nos formatos PDF e Excel contêm tendências representadas como gráficos e tabelas. Os relatórios em formato CSV contêm dados tabulares que podem ser processados para gerar exibições ou para arquivamento.

Para exportar um relatório:

1. Vá para a guia **Trends**.
2. Defina os critérios de filtro e o período de tempo e clique em **Apply**. A tabela e o gráfico de tendências são preenchidos com os dados.
3. Clique em **Export** e insira o nome e o formato do relatório.

O Director gera o relatório com base nos critérios de filtro selecionados. Se você alterar os critérios de filtro, clique em **Apply** antes de clicar em **Export**.

> **Nota:**
>
> A exportação de uma grande quantidade de dados causa um aumento significativo no consumo de memória e CPU no servidor Director, no Delivery Controller e em SQL Servers. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados são definidos a limites padrão para alcançar o desempenho de exportação ideal.

Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos dos critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados se ultrapassam os limites padrão de número de linhas ou registros na tabela. O número padrão de registros suportados é definido com base no formato do relatório.

Você pode alterar o limite padrão definindo as configurações de aplicativo do Director no IIS (Serviços de Informações da Internet).

Formato do relatório	Número padrão de registros suportados	Campos nas configurações de aplicativo do Director	Número máximo de registros suportados
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100.000	UI.ExportExcelDrilldownLimit	1000.000
CSV	100.000 (10.000.000 na guia **Sessions**)	UI.ExportCsvDrilldownLimit	10000.000

Para alterar o limite do número de registros que você pode exportar:

1. Abra o console do Gerenciador do IIS.
2. Acesse o site do Director sob o site padrão.
3. Clique duas vezes em **Application Settings**.
4. Edite ou adicione uma configuração para os campos UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLi
   ou UI.ExportCsvDrilldownLimit, conforme necessário.

Adicionar esses valores de campo às configurações em Application Settings substitui os valores padrão.

> **Aviso:**
>
> Definir valores de campo maiores que o número máximo de registros suportados pode afetar o desempenho da exportação, além de não ser suportado.

Tratamento de erros

Esta seção fornece informações sobre como tratar os erros que você possa encontrar durante uma operação de exportação.

- **Director has timed out**

Esse erro pode ocorrer devido a problemas de rede ou alto uso de recursos no servidor do Director ou com o Monitor Service.

A duração do tempo limite padrão é de 100 segundos. Para aumentar a duração do tempo limite do Director Service, defina o valor do campo **Connector.DataServiceContext.Timeout** nas configurações de aplicativo do Director no IIS (Serviços de Informações da Internet):

1. Abra o console do Gerenciador do IIS.
2. Acesse o site do Director sob o site padrão.
3. Clique duas vezes em **Application Settings**.

4. Edite o valor **Connector.DataServiceContext.Timeout**.

- **Monitor has timed out**

Esse erro pode ocorrer devido a problemas de rede ou alto uso de recursos com o Monitor Service ou no SQL Server.

Para aumentar a duração do tempo limite do Monitor Service, execute os seguintes comandos do PowerShell no Delivery Controller:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Max concurrent Export or Preview operations ongoing**

O Director suporta uma instância de Export ou Preview. Se você receber um erro referente a **operações máximas simultâneas de exportação e visualização**, tente refazer a operação Export seguinte mais tarde.

É possível aumentar o número de operações Export ou Preview simultâneas, no entanto, isso pode afetar o desempenho do Director, além de não ser suportado:

1. Abra o console do Gerenciador do IIS.
2. Acesse o site do Director sob o site padrão.
3. Clique duas vezes em **Application Settings**.
4. Edite o valor **UI.ConcurrentExportLimit**.

- **Insufficient disk space in Director**

Cada operação de exportação requer um máximo de 2 GB de espaço de disco rígido na pasta Temp do Windows. Tente exportar novamente depois de limpar espaço ou adicionar mais espaço ao disco rígido no servidor do Director.

Monitorar hotfixes

Para ver os hotfixes instalados no VDA de uma máquina específica (física ou VM), escolha a exibição **Machine Details**.

Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas selecionadas no Director, use as opções de controle de energia. Essas opções estão disponíveis para máquinas com SO de sessão única, mas podem não estar disponíveis para máquinas com SO multissessão.

> **Nota:**
>
> Essa funcionalidade não está disponível para máquinas físicas ou máquinas que usam o Remote PC Access.

Comando	Função
Restart	Executa o desligamento ordenado (suave) da máquina virtual, e todos os processos em execução são interrompidos individualmente antes de reiniciar a máquina virtual. Por exemplo, selecione máquinas que aparecem no Director com o erro "failed to start"e use esse comando para reiniciá-las.
Force Restart	Reinicia a máquina virtual sem executar nenhum procedimento de desligamento primeiro. Esse comando funciona da mesma forma que desconectar o cabo de um servidor físico, reconectá-lo em seguida e ligar o servidor novamente.
Shut Down	Executa o desligamento ordenado (suave) da máquina virtual. Todos os processos em execução são interrompidos individualmente.
Force Shutdown	Desliga a máquina virtual sem executar nenhum procedimento de desligamento primeiro. Esse comando funciona da mesma forma que desconectar o cabo de um servidor físico. Porém, nem sempre os processos em execução são encerrados e você corre o risco de perder dados se encerrar uma máquina virtual dessa maneira.
Suspend	Suspende uma máquina virtual em execução em seu estado atual e armazena o estado em um arquivo no repositório de armazenamento padrão. Essa opção permite que você desligue o servidor host da máquina virtual e, posteriormente, após reinicializá-lo, retome a máquina virtual, retornando-a ao seu estado de execução original.

Comando	Função
Resume	Retoma uma máquina virtual suspensa e restaura seu estado de execução original.
Start	Inicia uma máquina virtual quando ela está desligada (também chamada de inicialização a frio).

Se as ações de controle de energia falharem, passe o mouse sobre o alerta e uma mensagem pop-up aparece com detalhes sobre a falha.

Prevenir conexões a máquinas

Use o modo de manutenção para evitar novas conexões temporariamente enquanto o administrador apropriado executa tarefas de manutenção na imagem.

Quando você ativa o modo de manutenção em máquinas, nenhuma nova conexão é permitida até você desativá-lo. Se os usuários estiverem conectados no momento, o modo de manutenção entrará em vigor assim que todos os usuários estiverem desconectados. Para usuários que não fizerem logoff, envie uma mensagem informando que as máquinas serão desligadas em um determinado momento e use os controles de energia para forçar as máquinas a desligarem.

1. Selecione a máquina, como, por exemplo, na exibição User Details, ou um grupo de máquinas na exibição Filters.
2. Selecione **Maintenance Mode** e ative a opção.

Se um usuário tentar se conectar a uma área de trabalho atribuída enquanto estiver no modo de manutenção, será exibida uma mensagem indicando que a área de trabalho está indisponível. Nenhuma nova conexão pode ser feita até que você desative o modo de manutenção.

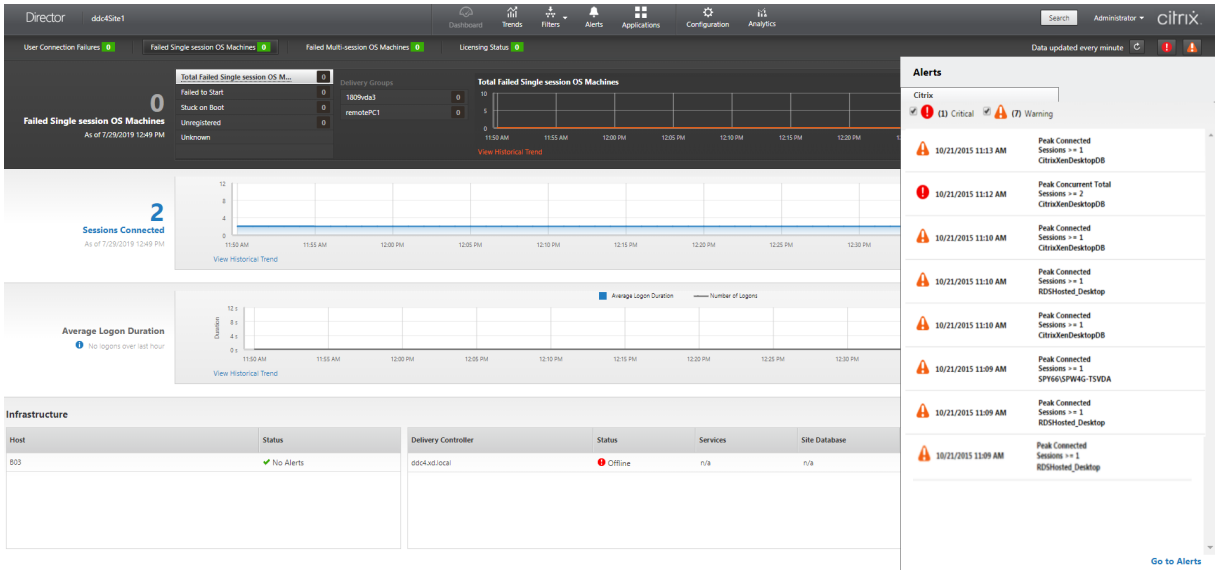
Análise de aplicativos

A guia **Applications** exibe análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos com eficiência. Você pode obter informações valiosas sobre a integridade e uso de todos os aplicativos publicados no site. Ela mostra métricas, tais como, os resultados de investigações, o número de instâncias por aplicativo e falhas e erros associados aos aplicativos publicados. Para obter mais informações, consulte a seção Análise de aplicativos em **Solucionar problemas de aplicativos**.

Alertas e notificações

June 28, 2023

Os alertas são exibidos no Director, no painel e em outras visualizações de alto nível, com símbolos de alerta crítico e de aviso. Os alertas estão disponíveis para sites licenciados **Premium**. Os alertas são atualizados automaticamente a cada minuto, mas você também pode atualizar os alertas sob demanda.

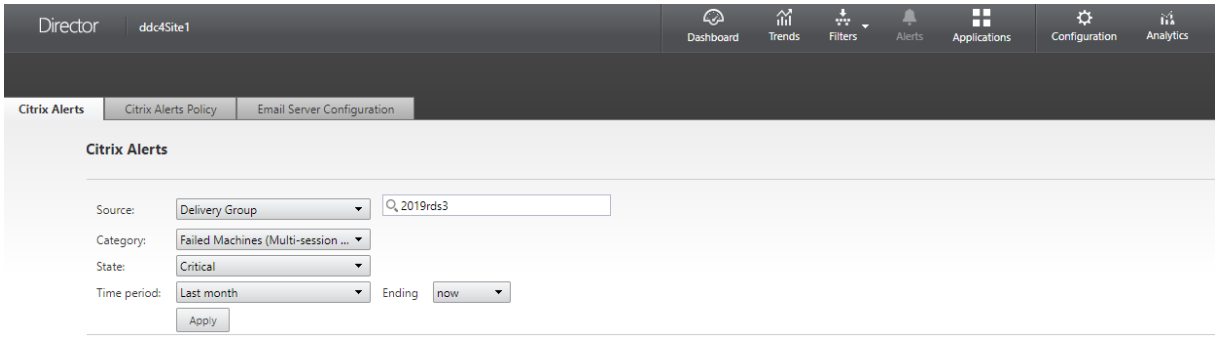


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre alertas selecionando um alerta na barra lateral, clicando no link **Go to Alerts**, na parte inferior da barra lateral, ou selecionando **Alerts** na parte superior da página do Director.

Na exibição Alerts, você pode filtrar e exportar os alertas. Por exemplo, para ver as máquinas com SO multissessão em um grupo de entrega específico que apresentaram falha no último mês ou todos os alertas a um usuário específico. Para obter mais informações, consulte Exportar relatórios.



Alertas Citrix

Os alertas Citrix são alertas monitorados no Director que se originam de componentes Citrix. Você pode configurar alertas Citrix no Director em **Alerts** > **Citrix Alerts Policy**. Como parte da configuração, você pode definir notificações para serem enviadas por e-mail para indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar alertas Citrix, consulte Criar políticas de alertas.

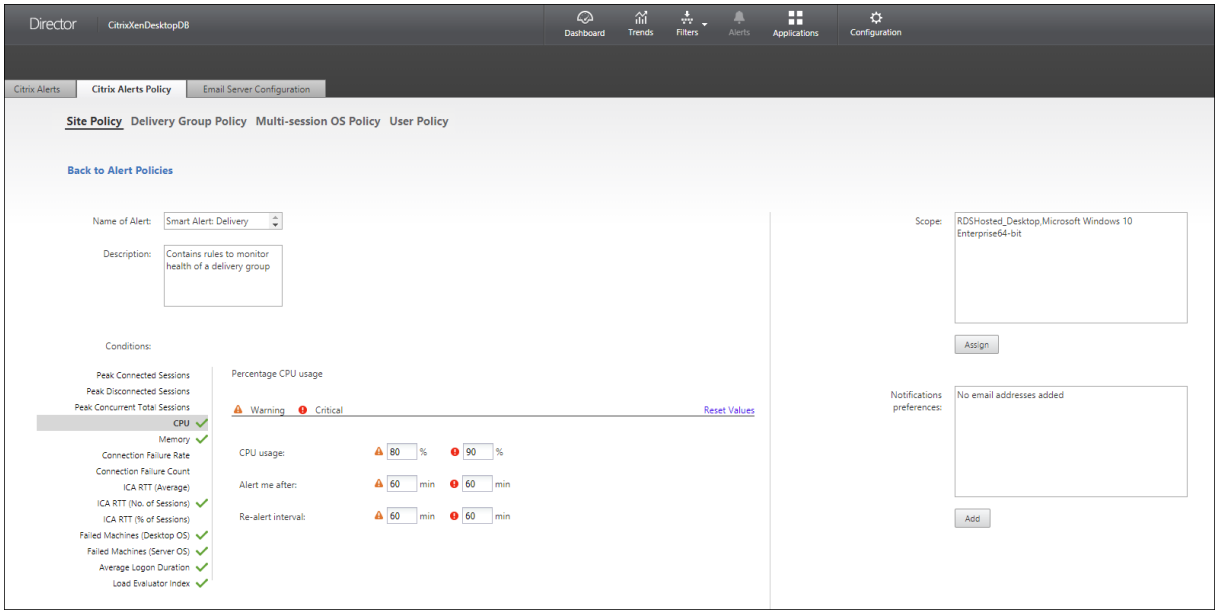
> **Nota:**
>
> Certifique-se de que o firewall, o proxy ou o Microsoft Exchange Server não bloqueie os alertas por e-mail.

Políticas de alertas inteligentes

Um conjunto de políticas de alertas internos com valores limite predefinidos está disponível para o escopo de VDA com SO multissessão e grupos de entrega. Esse recurso requer Delivery Controllers versão 7.18 ou posterior. Você pode modificar os parâmetros de limite das políticas de alertas internos em **Alerts** > **Citrix Alerts Policy**.
Essas políticas são criadas quando há pelo menos um alvo de alerta: um grupo de entrega ou um VDA com SO multissessão definido em seu site. Além disso, esses alertas internos são adicionados automaticamente a um novo grupo de entrega ou a um VDA com SO multissessão.

Caso você atualize o Director e seu site, as políticas de alerta da instância anterior do Director serão transferidas. As políticas de alertas internos são criadas somente se não houver regras de alertas correspondentes no banco de dados de monitoramento.

Para obter os valores limite das políticas de alertas internos, consulte a seção Condições das políticas de alertas.

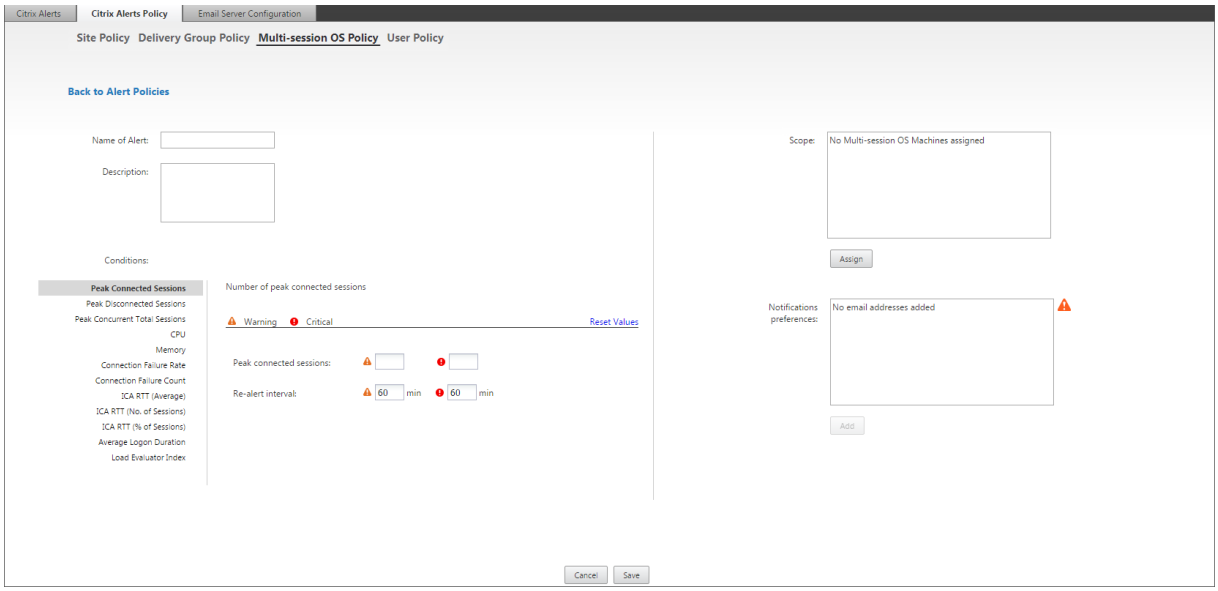


Alertas SCOM

Os alertas SCOM exibem informações de alerta do Microsoft System Center 2012 Operations Manager (SCOM) para fornecer uma indicação mais abrangente da integridade e do desempenho do data center no Director. Para obter mais informações, consulte a seção Configurar a integração de alertas SCOM.

O número de alertas exibidos ao lado dos ícones de alertas antes de expandir a barra lateral é a soma combinada de alertas Citrix e SCOM.

Criar políticas de alertas



Para criar uma nova política de alertas, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alerts** > **Citrix Alerts Policy** e selecione, por exemplo, a política de SO multissessão.
2. Clique em **Create**.
3. Dê um nome e uma descrição para política e defina as condições que precisam ser atendidas para que o alerta seja disparado. Por exemplo, especifique os valores de pico de avisos e alertas críticos em Peak Connected Sessions, Peak Disconnected Sessions e Peak Concurrent Total Sessions. Os valores em Warning não devem ser maiores que os valores em Critical. Para obter mais informações, consulte Condições das políticas de alertas.
4. Defina o intervalo de repetição de alerta em Re-alert interval. Se as condições para o alerta continuarem a ser atendidas, o alerta será disparado novamente nesse intervalo de tempo e, se configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta descartado não gera uma notificação por e-mail no intervalo de repetição do alerta.
5. Defina o escopo em Scope. Por exemplo, defina para um grupo de entrega específico.
6. Em Notification preferences, especifique quem deve ser notificado por e-mail quando o alerta for disparado. Você precisa especificar um servidor de e-mail na guia **Email Server Configuration** para definir as preferências de notificação por e-mail nas políticas de alertas.
7. Clique em **Salvar**.

A criação de uma política com 20 ou mais grupos de entrega definidos no escopo pode levar aproximadamente 30 segundos para concluir a configuração. Um controle giratório é exibido durante esse período.

A criação de mais de 50 políticas para até 20 grupos de entrega exclusivos (1000 alvos do grupo de entrega no total) pode resultar em um aumento no tempo de resposta (mais de 5 segundos).

Mover uma máquina contendo sessões ativas de um grupo de entrega para outro pode disparar alertas incorretamente do grupo de entrega que são definidos usando parâmetros da máquina.

Condições das políticas de alertas

Veja abaixo as categorias de alertas, as ações recomendadas para mitigar o alerta e as condições de políticas internas, se definidas. As políticas de alertas internos são definidas para alertar repetidamente a intervalos de 60 minutos.

Pico de sessões conectadas, em Peak Connected Sessions

- No Director, verifique a exibição Session Trends ver o pico de sessões conectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.

Pico de sessões desconectadas, em Peak Disconnected Sessions

- No Director, verifique a exibição Session Trends ver o pico de sessões desconectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

Pico total de sessões simultâneas, em Peak Concurrent Total Sessions

- No Director, verifique a exibição Session Trends ver o pico de sessões simultâneas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

CPU

A porcentagem do uso da CPU indica o consumo geral da CPU no VDA, incluindo os processos. Você pode obter mais informações sobre a utilização da CPU por processos individuais na página **Machine details** do VDA correspondente.

- Vá para **Machine Details > View Historical Utilization > Top 10 Processes** e identifique os processos que consomem a CPU. Certifique-se de que a política de monitoramento de processos esteja ativada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.

- Encerre o processo, se necessário.
- Com o término do processo, os dados não salvos são perdidos.
- Se tudo estiver funcionando conforme o esperado, adicione recursos extras de CPU no futuro.

> **Nota:**
>
> A configuração de política **Enable resource monitoring** é permitida por padrão para o monitoramento de contadores de desempenho de memória e CPU em máquinas com VDAs. Se essa configuração de política estiver desativada, os alertas com condições de CPU e memória não são disparados. Para obter mais informações, consulte Configurações da política de monitoramento.

Condições de políticas inteligentes:

- **Escopo:** scope de Delivery Group, Multi-session OS
- **Valores limite:** Warning - 80%, Critical - 90%

Memória

A porcentagem de uso de memória indica o consumo geral de memória no VDA, incluindo os processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Machine details** do VDA correspondente.

- Vá para **Machine Details > View Historical Utilization > Top 10 Processes** e identifique os processos que consomem a memória. Certifique-se de que a política de monitoramento de processos esteja ativada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Com o término do processo, os dados não salvos são perdidos.
- Se tudo estiver funcionando conforme o esperado, adicione memória extra no futuro.

> **Nota:**
>
> A configuração de política **Enable resource monitoring** é permitida por padrão para o monitoramento de contadores de desempenho de memória e CPU em máquinas com VDAs. Se essa configuração de política estiver desativada, os alertas com condições de CPU e memória não são disparados. Para obter mais informações, consulte Configurações da política de monitoramento.

Condições de políticas inteligentes:

- **Escopo:** scope de Delivery Group, Multi-session OS
- **Valores limite:** Warning - 80%, Critical - 90%

Taxa de falha na conexão, em Connection Failure Rate

Porcentagem de falhas de conexão na última hora.

- Calculado com base no total de falhas das tentativas totais de conexões.
- No Director, verifique a exibição Connection Failures Trends para ver os eventos registrados no log de configuração.
- Determine se os aplicativos ou as áreas de trabalho são acessíveis.

Contagem de falhas de conexão, em Connection Failure Count

Número de falhas de conexão na última hora.

- No Director, verifique a exibição Connection Failures Trends para ver os eventos registrados no log de configuração.
- Determine se os aplicativos ou as áreas de trabalho são acessíveis.

Média, em ICA RTT (Average)

Tempo médio de resposta do ICA (Independent Computing Architecture).

- Verifique o Citrix ADM para obter uma análise do ICA RTT para determinar a causa raiz. Para obter mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, verifique a exibição User Details no Director para saber o ICA RTT e Latência e determinar se é um problema de rede ou um problema com aplicativos ou áreas de trabalho.

Valor, em ICA RTT (No. of Sessions)

Número de sessões que excedem o limite de tempo de resposta do ICA.

- Verifique o Citrix ADM para saber o número de sessões com alto ICA RTT. Para obter mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, fale com uma equipe de rede para determinar a causa raiz.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 300 ms por 5 ou mais sessões, Critical - 400 ms por 10 ou mais sessões

Valor, em ICA RTT (% of Sessions)

Porcentagem de sessões que excedem o tempo médio de resposta do ICA.

- Verifique o Citrix ADM para saber o número de sessões com alto ICA RTT. Para obter mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, fale com uma equipe de rede para determinar a causa raiz.

Valor, em ICA RTT (User)

Tempo de resposta do ICA que é aplicado às sessões iniciadas pelo usuário especificado. O alerta é acionado se o ICA RTT for maior que o limite em pelo menos uma sessão.

Máquinas com falha em sistemas de sessão única, em Failed Machines (Single-session OS)

Número de máquinas com SO de sessão única com falhas. As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Director em Dashboard e Filters.

- Execute o diagnóstico do Citrix Scout para determinar a causa raiz.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 1, Critical - 2

Máquinas com falha em sistemas multissessão, em Failed Machines (Multi-session OS)

Número de máquinas com SO multissessão com falhas. As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Director em Dashboard e Filters.

- Execute o diagnóstico do Citrix Scout para determinar a causa raiz.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 1, Critical - 2

Máquinas com falha (em %)

Porcentagem de máquinas com SO de sessão única e multissessão com falha em um grupo de entrega calculada com base no número de máquinas com falha. Essa condição de alerta permite que

você configure limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega, calculada a cada 30 segundos.
As falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Director em Dashboard e Filters. Execute o diagnóstico do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Resolução de problemas de usuário.

Duração média de logon, em Average Logon Duration

Duração média dos logons ocorridos na última hora.

- Verifique o Dashboard do Director para obter métricas atualizadas em relação à duração do logon. Um grande número de usuários fazendo login em um curto período de tempo pode aumentar a duração do logon.
- Verifique a linha de base e a análise detalhada dos logons para determinar a causa. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 45 segundos, Critical - 60 segundos

Duração do logon (usuário), em Logon Duration (User)

Duração dos logons de um usuário especificado que ocorreu na última hora.

Índice do avaliador de carga, em Load Evaluator Index

Valor do índice do avaliador de carga nos últimos 5 minutos.

- No Director, verifique os computadores em Multi-session OS Machines que possam ter um pico de carga (carga máxima). Analise as falhas no Dashboard e o relatório de tendências do índice do avaliador de carga.

  Condições de políticas inteligentes:

  - **Escopo:** scope de Delivery Group, Multi-session OS
  - **Valores limite:** Warning - 80%, Critical - 90%

Monitoramento de alertas do Hypervisor

O Director exibe alertas para monitorar a integridade do hipervisor. Alertas do Citrix Hypervisor e do VMware vSphere ajudam a monitorar parâmetros e estados do Hypervisor. O status da conexão

com o Hypervisor também é monitorado para fornecer um alerta se o cluster ou pool de hosts for reinicializado ou não estiver disponível.

Para receber alertas de hipervisor, certifique-se de que uma conexão de hospedagem seja criada no Web Studio. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas quanto a alertas do Hypervisor. A tabela a seguir descreve os vários parâmetros e estados dos alertas do Hypervisor.

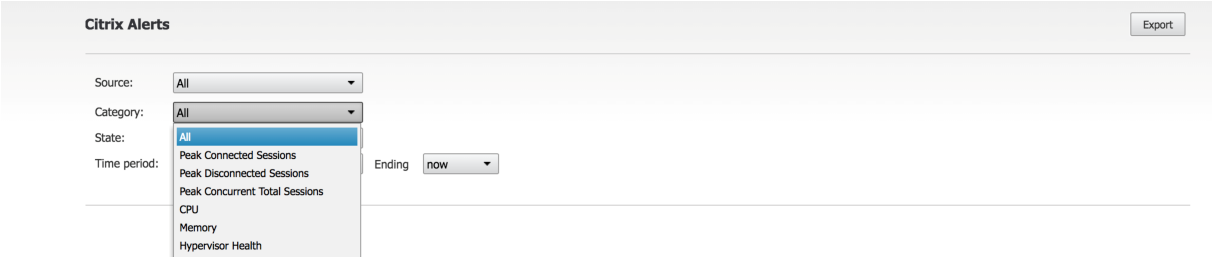
Alerta	Hypervisors compatíveis	Disparado por	Condição	Configuração
Uso de CPU	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da CPU é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Uso de memória	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de memória é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Uso de rede	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da rede é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Disk usage	VMware vSphere	Hypervisor	O limite de alerta de uso do disco é atingido ou excedido	Limites de alerta devem ser configurados no Hypervisor.
Conexão do host ou estado de energia	VMware vSphere	Hypervisor	O host do Hypervisor foi reinicializado ou não está disponível	Os alertas estão integrados ao VMware vSphere. Não são necessárias configurações adicionais.

Alerta	Hypervisors compatíveis	Disparado por	Condição	Configuração
Conexão com o Hypervisor não disponível	Citrix Hypervisor, VMware vSphere	Delivery Controller	A conexão com o Hypervisor (pool ou cluster) é perdida ou desligada ou reinicializada. Esse alerta é gerado a cada hora, enquanto a conexão não estiver disponível.	Os alertas estão integrados ao Delivery Controller. Não são necessárias configurações adicionais.

> **Nota:**
>
> Para obter mais informações sobre como configurar alertas, consulte Citrix XenCenter Alerts ou a documentação de VMware vCenter Alerts.

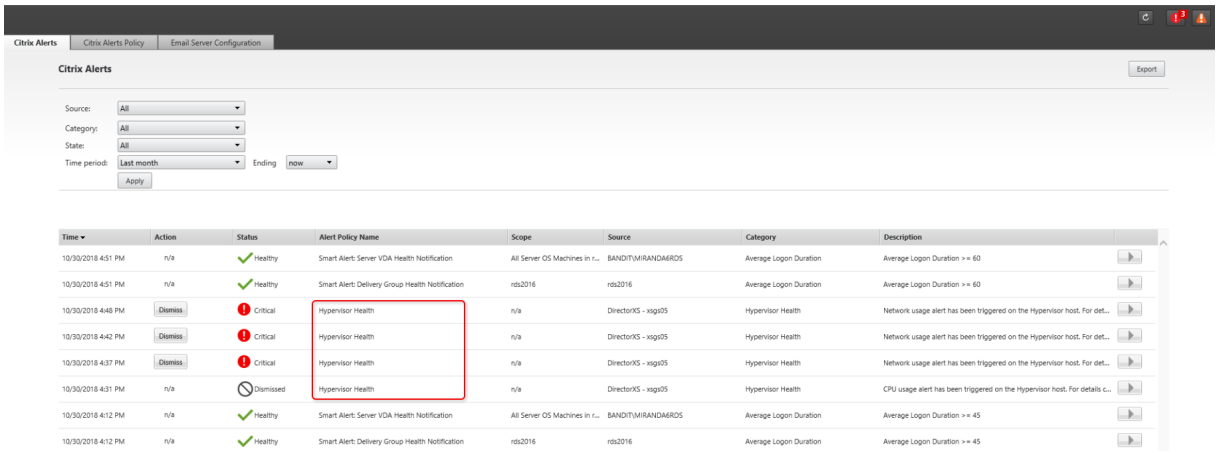
A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > site Policy > Hypervisor Health**. As condições de limite para as políticas de alerta do Hypervisor podem ser configuradas, editadas, desativadas ou excluídas somente no hipervisor, não no Director. No entanto, modificar as preferências de e-mail e descartar um alerta pode ser feito no Director.

> **Importante:**
>
> - Os alertas disparados pelo hipervisor são obtidos e exibidos no Director. No entanto, as mudanças no ciclo de vida/estado dos alertas do Hypervisor não são refletidas no Director.
> - Alertas de boa integridade, ou que são descartados ou desativados no console do Hypervisor continuam a aparecer no Director e precisam ser descartados explicitamente.
> - Os alertas que são descartados no Director não são descartados automaticamente no console do Hypervisor.



Uma nova categoria de alerta chamada **Hypervisor Health** foi adicionada para permitir a filtragem somente dos alertas do Hypervisor. Esses alertas são exibidos quando os limites são atingidos ou excedidos. Alertas do Hypervisor podem ser:

- Critical —limite crítico da política de alarme do Hypervisor atingido ou excedido
- Warning —limite de aviso da política de alarme do Hypervisor atingido ou excedido
- Dismissed —o alerta não aparece mais como um alerta ativo



Esse 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, somente a contagem de alertas do Hypervisor será exibida. Para exibir os alertas, você deve atualizar o Director.

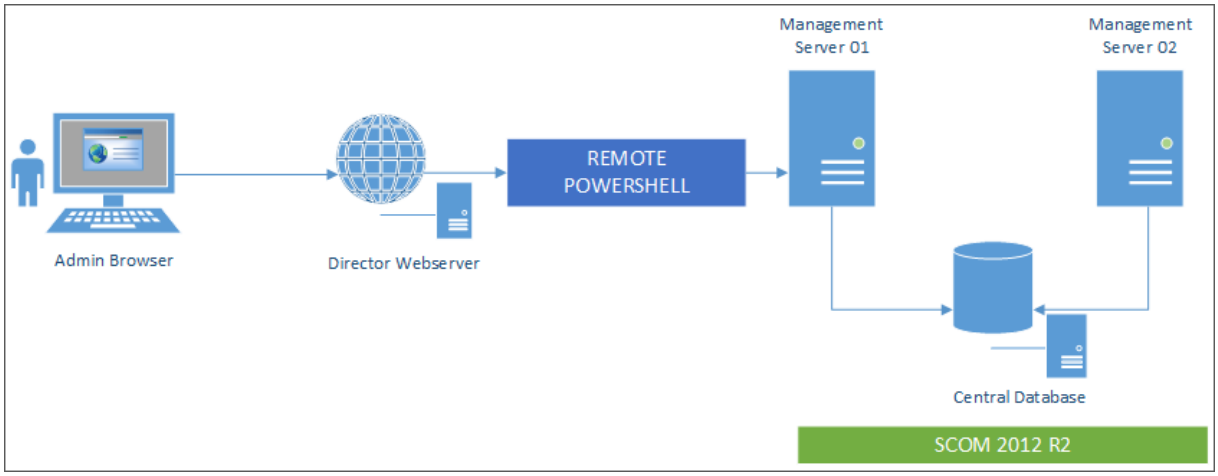
Configurar a integração de alertas SCOM

A integração do SCOM com o Director permite exibir informações de alertas SCOM no Dashboard e em outras exibições de nível alto no Director.

Os alertas SCOM são exibidos na tela ao lado de alertas Citrix. Você pode acessar e ver os detalhes dos alertas SCOM na guia SCOM na barra lateral.

Você pode exibir alertas históricos 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 no servidor de gerenciamento do SCOM e mantém uma conexão runspace persistente na sessão do Director do usuário. O servidor do Director e do 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 do SCOM devem ser correspondentes)
- CPU Quad Core com 16 GB de RAM (recomendado)
- Um servidor de gerenciamento primário para o 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 do SCOM para que as informações completas do alerta possam ser recuperadas no Director. Se isso não for possível, uma conta de administrador do SCOM poderá 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 servidor de gerenciamento do SCOM para garantir um bom desempenho.

No servidor do Director:

1. Digite **Enable-PSRemoting** para ativar a comunicação remota do PowerShell.
2. Adicione o servidor de gerenciamento do SCOM à lista TrustedHosts. Abra um prompt do PowerShell e execute os seguintes comandos:

    - Obtenha a lista atual TrustedHosts

      Get-Item WSMAN:\localhost\Client\TrustedHosts

    - Adicione o FQDN do servidor de gerenciamento do SCOM à lista TrustedHosts. <Old Values> representa o conjunto existente de entradas retornadas do cmdlet Get-Item.

      Set-Item WSMAN:localhostClientTrustedHosts -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 do SCOM:

1. Atribua administradores do Director a uma função de administrador do SCOM.

   a) Abra o console de gerenciamento do 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 função existente. Existem quatro categorias de funções de operador no 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 consegue detectar ou gerenciar regras, máquinas ou contas. Uma função de Operador é uma função de administrador completa.

   > **Nota:**
   >
   > As seguintes operações não estarão disponíveis se o administrador do Director for atribuído a uma função de não 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, que é o mesmo servidor que o especificado com a ferramenta DirectorConfig na etapa 3 acima. Os servidores de gerenciamento secundários são servidores de gerenciamento do mesmo nível do servidor primário.
   > - Ao filtrar alertas, o administrador do Director não pode procurar a origem do alerta. Isso requer uma permissão com nível de operador.

   c) Para modificar uma função do usuário, clique com o botão direito do mouse na função e clique em **Propriedades**.

   d) Na caixa de diálogo de propriedades da função do usuário, você pode adicionar ou remover administradores do Director para a função de usuário especificada.

2. Adicione administradores do Director ao grupo Usuários de Gerenciamento Remoto no servidor de gerenciamento do SCOM. Isso permite que os administradores do Director estabeleçam uma conexão remota do PowerShell.
3. Digite **Enable-PSRemoting** para ativar a comunicação remota do PowerShell.
4. Defina os limites das propriedades do WS-Management:

   a) Modificar MaxConcurrentUsers:

Na CLI:

“‘winrm set winrm/config/winrs @{MaxConcurrentUsers = “20”}

```
No PS:

```Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20<!--NeedCopy-->
```

b) Modificar MaxShellsPerUser:

Na CLI:

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--NeedCopy-->
```

No PS:

“‘Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20

```
1.  Modificar MaxMemoryPerShellMB:

    Na CLI:

    ```winrm set winrm/config/winrs @{
 MaxMemoryPerShellMB="1024" }
 <!--NeedCopy-->
```

```
No PS:
```

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024<!--NeedCopy-->
```

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 poderão exigir que você reinstale o seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

Depois que a integração do SCOM for configurada, você poderá ver a mensagem similar a “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 SCOM.
- O serviço SCOM não está disponível ou está muito ocupado para responder.
- Falha na autorização devido a uma alteração nas permissões do usuário configurado.
- Um erro no Director durante o processamento dos dados do SCOM.
- Incompatibilidade de versão do PowerShell entre o Director e o servidor do SCOM.

Filtrar dados para solucionar problemas de falhas

June 28, 2023

Quando você clica em números no painel Dashboard ou seleciona um filtro predefinido no menu Filters, a exibição Filters é aberta para exibir os dados com base na máquina selecionada ou no tipo de falha.

Os filtros predefinidos não podem ser editados, mas você pode salvar um filtro predefinido como um filtro personalizado e 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:

    - **Machines**. Selecione Single-session OS Machines ou Multi-session OS Machines. Essas exibições mostram o número de máquinas configuradas. A guia Multi-session OS Machines também inclui o índice do avaliador de carga, que indica a distribuição dos contadores de desempenho e exibe dicas de ferramentas de contagem de sessões se você passar o mouse sobre o link.
    - **Sessions**. Você também pode ver a contagem de sessões na exibição Sessions. Use as medições de tempo ocioso para identificar sessões que estão ociosas além de um período de tempo limite.
    - **Connections**. Filtre conexões por diferentes períodos de tempo, incluindo últimos 60 minutos, últimas 24 horas ou últimos 7 dias.
    - **Application Instances**. Essa exibição exibe as propriedades de todas as instâncias de aplicativos em VDAs do servidor e SO de sessão única. As medições de tempo ocioso da sessão estão disponíveis para instâncias de aplicativos em VDAs com SO multissessão.

    > **Nota:**
    >
    > Se você iniciou sessões de área de trabalho em VDAs instalados em um computador com Windows 10 1809, o Activity Manager no Director pode, às vezes, exibir o Microsoft Edge e

> o Office como aplicativos em execução ativa, quando, na verdade, eles estão sendo executados apenas em segundo plano.

2. Em **Filter by**, selecione os critérios.
3. Use as guias adicionais para cada exibição, conforme necessário, para preencher o filtro.
4. Selecione colunas extras, conforme necessário, para solucionar problemas mais complexos.
5. Salve e dê um nome ao seu filtro.
6. Para acessar filtros de vários servidores do 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 do Director.
   - Os servidores do Director devem ser configurados para acessar a pasta compartilhada. Para configurar, execute o **Gerenciador do IIS**. Em **Sites > Site Padrão > Director\ > Configurações do aplicativo**, modifique a configuração **Service.UserSettingsPath** para refletir o caminho UNC da pasta compartilhada.
7. Para abrir o filtro posteriormente, no menu **Filters**, selecione o tipo de filtro (Machines, Sessions, Connections ou Application Instances) e, em seguida, selecione o filtro salvo.
8. Clique em **Export** para exportar os dados para arquivos no formato CSV. Dados de até 100.000 registros podem ser exportados. Esse recurso está disponível no Delivery Controller versão 1808 e posterior.
9. Se necessário, para as exibições de **Machines** ou **Connections**, use os controles de energia para todas as máquinas selecionadas na lista filtrada. Para a exibição Sessions, use os controles de sessão ou a opção para enviar mensagens.
10. Nas exibições **Machines** e **Connections**, clique em **Failure Reason** em uma máquina ou conexão com falha para obter uma descrição detalhada da falha e das ações recomendadas para solucionar o problema da falha. Os motivos de falha e as ações recomendadas para falhas de máquina e na conexão estão disponíveis em Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
11. Na exibição **Machines**, clique no link do nome de uma máquina para ir para a página **Machine Details** correspondente. A página exibe os detalhes da máquina, fornece controles de energia, mostra os dados de monitoramento de CPU, memória e disco, além do gráfico de monitoramento da GPU. Clique também em **View Historical Utilization** para ver as tendências de utilização dos recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
12. Na exibição **Application Instances**, classifique ou filtre com base no **Idle Time** maior que um período de tempo limite. Selecione as instâncias do aplicativo ociosas para encerrá-las. O lo-

goff ou a desconexão de uma instância de aplicativo encerra todas as instâncias de aplicativo ativas em uma mesma sessão. Para obter mais informações, consulte Solucionar problemas de aplicativos. A página de filtro Application Instances e as medições de tempo ocioso nas páginas de filtro Sessions ficam disponíveis se o Director, os Delivery Controllers e os VDAs forem da versão 7.13 ou posterior.

> **Nota:**
> O Web Studio permite a atribuição de várias regras de atribuição de área de trabalho (DAR) de diferentes usuários ou grupos de usuários para um único VDA no grupo de entrega. O StoreFront exibe a área de trabalho atribuída com o nome de exibição correspondente de acordo com o DAR do usuário conectado. No entanto, o Director não oferece suporte a regras DAR e exibe a área de trabalho atribuída usando o nome do grupo de entrega, independentemente do usuário conectado. Como resultado, você não pode mapear uma área de trabalho específica a uma máquina no 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 do PowerShell:

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

Monitorar tendências históricas em um site

June 28, 2023

A exibição Trends acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas na máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade
- uso da máquina
- utilização de recursos
- análise de rede para cada site

Para localizar essas informações, clique no menu **Trends**.

O recurso de zoom na análise detalhada permite navegar pelos gráficos de tendências, destacando um período de tempo (clicando em um ponto de dados no gráfico) para ver os pormenores associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que é afetado.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

Escolha um período de tempo do qual deseja obter as informações históricas da tendência. A disponibilidade do período de tempo depende da implantação do Director da seguinte forma:

- Relatórios de tendências do último ano (365 dias) estão disponíveis nos sites com licença Premium.
- Relatórios de tendências do último mês (31 dias) estão disponíveis nos sites com licença Advanced.
- Relatórios de tendências dos últimos 7 dias para os sites sem licença Premium ou Advanced.

> **Nota:**
>
> - Em todas as implantações do Director, as informações de tendências de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período é definido como Last month (**Ending now**) ou mais curto. Para os períodos Last Month, com uma data de término personalizada, ou Last Year, as informações de tendência ficam disponíveis como gráficos, 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. Os clientes em sites com licença Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção.
> - Os parâmetros a seguir no Gerenciador do IIS controlam o intervalo de datas de término personalizadas disponíveis para seleção. No entanto, a disponibilidade de dados para as datas selecionadas depende da configuração de retenção de limpeza para a métrica específica que está sendo medida.

Parâmetro	Valores padrão
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

Tendências disponíveis

Exibir tendências para sessões: na guia **Sessions**, selecione o grupo de entrega e o período de tempo para exibir informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Session Auto Reconnect** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas Session Reliability ou Auto Client Reconnect estão em vigor. Quando há uma interrupção de rede no ponto de extremidade, as seguintes políticas entram em vigor:

- A confiabilidade da sessão, em Session Reliability, entra em vigor (por padrão, por 3 minutos) quando o Citrix Receiver ou o aplicativo Citrix Workspace tenta se conectar com o VDA.
- A reconexão automática de cliente, em Auto Client Reconnect, entra em vigor entre 3 e 5 minutos, quando o cliente tenta se conectar com o VDA.

As duas reconexões são capturadas e exibidas para o usuário. Essas informações podem levar um tempo máximo de 5 minutos para aparecer na interface do usuário do Director após ocorrer a reconexão.

As informações de reconexão automática ajudam a visualizar e solucionar problemas de conexões de rede com interrupções. Elas também analisam as redes com uma experiência fluida. Você pode exibir o número de reconexões para um grupo de entrega específico ou período de tempo selecionado nos filtros. Uma análise detalhada fornece informações adicionais, como dados de confiabilidade da sessão ou reconexão automática de cliente, carimbos de hora, IP do ponto de extremidade e nome do ponto de extremidade da máquina em que o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de hora do evento em ordem decrescente. Esse recurso está disponível para o aplicativo Citrix Workspace para Windows, aplicativo Citrix Workspace para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Esse recurso requer o Delivery Controller versão 7 1906 ou posterior e VDAs 1906 ou posteriores.

Para obter mais informações sobre reconexões de sessão, consulte Sessões.

Para obter mais informações sobre políticas, consulte Configurações da política de reconexão automática de cliente e Configurações da política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Director pelos seguintes motivos:

- O aplicativo Workspace não envia os dados de reconexão automática para o VDA.
- O VDA não envia os dados para o Monitor Service.
- Os Delivery Controllers descartam as cargas úteis do VDA, pois podem não ter as sessões correspondentes.

> **Nota:**
>
> Às vezes, o endereço IP do cliente não é obtido corretamente se determinadas políticas do Citrix Gateway estiverem definidas.

Exibir tendências de falhas de conexão: na guia Failures, selecione a conexão, o tipo de máquina, o tipo de falha, o grupo de entrega e o período de tempo para exibir um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em todo o site.

Exibir tendências de falhas de máquinas: na guia **Single-session OS Machine Failures ou Multi-session OS Machines**, selecione o tipo de falha, grupo de entrega e período de tempo para exibir um gráfico contendo informações mais detalhadas sobre as falhas da máquina em todo o site.

Exibir tendências de desempenho de logon: na guia **Logon Performance**, selecione o grupo de entrega e o período de tempo para exibir um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em todo o site e se o número de logons afeta o desempenho. Essa exibição também mostra a duração média das fases de logon, como a duração de intermediação do agente e a hora de início da máquina virtual.
Esses dados são especificamente para logons de usuários e não incluem usuários que tentam se reconectar em sessões desconectadas.
A tabela abaixo do gráfico mostra a duração do logon por sessão de usuário. Você pode escolher as colunas para exibir e classificar o relatório por qualquer uma das colunas.
Para obter mais informações, consulte Diagnosticar problemas de logon do usuário

Exibir tendências de avaliação de carga: na guia **Load Evaluator Index**, veja um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas com SO multissessão. As opções de filtro do gráfico incluem: grupo de entrega ou máquina com SO multissessão em um grupo de entrega, máquina com SO multissessão (disponível somente se a máquina com SO multissessão em um grupo de entrega tiver sido selecionada) e um intervalo.

Exibir o uso de aplicativos hospedados: a disponibilidade desse recurso depende da licença da sua organização.
Na guia **Capacity Management**, selecione a guia **Hosted Applications Usage**. Selecione o grupo de entrega e o período de tempo para exibir um gráfico que mostra o pico no uso simultâneo e uma tabela que mostra o uso baseado em aplicativos. Na tabela Application Based Usage, você pode escolher um aplicativo específico para ver seus detalhes e uma lista dos usuários que estão usando ou usaram o aplicativo.

Exibir uso de SO de sessão única e multissessão: a exibição Trends mostra o uso do sistema operacional de sessão única por site e por grupo de entrega. Quando você seleciona **Site**, o uso é mostrado por grupo de entrega. Quando você seleciona Delivery Group, o uso é mostrado por usuário.
A exibição Trends também mostra o uso do sistema operacional multissessão por site, por grupo de entrega e por máquina. Quando você seleciona **Site**, o uso é mostrado por grupo de entrega. Quando

você seleciona Delivery Group, o uso é mostrado por máquina e por usuário. Quando você seleciona Machine, o uso é mostrado por usuário.

Exibir o uso da máquina virtual: na guia **Machine Usage**, selecione **Single-session OS Machines ou Multi-session OS Machines** para ver uma exibição em tempo real do uso da sua máquina virtual, permitindo que você avalie rapidamente as necessidades de capacidade do site.
Single-session OS availability –exibe o estado atual das máquinas com SO de sessão única (VDIs) por disponibilidade de todo o site ou de um grupo de entrega específico.
Multi-session OS availability - exibe o estado atual das máquinas com SO multissessão por disponibilidade de todo o site ou de um grupo de entrega específico.

> **Nota:**
> O número de máquinas que aparece em Available Counter inclui máquinas no modo de manutenção.

Exibir utilização de recursos: na guia **Resource Utilization**, selecione **Single-session OS Machines ou Multi-session OS Machines** para ver informações sobre os dados de tendências históricas de uso de CPU e memória, além de IOPS e latência de disco de cada máquina VDI para poder planejar melhor a sua capacidade.
Esse recurso requer Delivery Controllers e VDAs **versão 7.11** ou posterior.
Os gráficos mostram dados médios de CPU, memória e IOPS, latência do disco e pico de sessões simultâneas. Você pode fazer o detalhamento dos dados por máquina e visualizar dados e gráficos dos 10 principais processos que consomem a CPU.

Filtre por grupo de entrega e período de tempo. Os gráficos de CPU, uso de memória e pico de sessões simultâneas estão disponíveis para as últimas 2 horas, últimas 24 horas, últimos 7 dias, último mês e último ano. Os gráficos de médias de latência de disco e IOPS estão disponíveis para as últimas 24 horas, o último mês e o último ano.

> **Nota:**
>
> - A configuração da política Monitoring, **Enable Process Monitoring**, deve ser definida como **Allowed** para coletar e exibir dados na tabela Top 10 Processes na página Historic Machine Utilization. A política é definida como **Prohibited** por padrão. Por padrão, todos os dados de utilização de recursos são coletados. Isso pode ser desativado usando a configuração de política **Enable Resource Monitoring**. A tabela abaixo dos gráficos mostra os dados de utilização dos recursos por máquina. Para obter mais informações, consulte Configurações da política de monitoramento.
> - O IOPS médio mostra as médias diárias. O pico de IOPS é calculado como a maior das médias de IOPS para o intervalo de tempo selecionado. (O IOPS médio é a média de IOPS por hora coletada durante a hora no VDA.)
> - O detalhamento da máquina lista processos com uso médio de CPU ou memória de mais

> de 1%. Isso pode significar que, às vezes, menos de 10 processos são listados.

Exibir dados de análise de rede: a disponibilidade desse recurso depende da licença da sua organização e das permissões de administrador. Esse recurso requer Delivery Controllers **versão 7.11** ou posterior.

Na guia **Network**, monitore a análise da sua rede, que fornece uma visão contextual de usuário, aplicativo e área de trabalho 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.

Exibir falhas de aplicativos: a guia **Application Failures** exibe falhas associadas aos aplicativos publicados nos VDAs.

Esse recurso requer Delivery Controllers e VDAs **versão 7.15** ou posterior. VDAs com SO de sessão única executando Windows Vista, e posterior, e VDAs com SO multissessão executando Windows Server 2008, e posterior, são suportados.
Para obter mais informações, consulte Monitoramento de falhas de aplicativos históricas.

Por padrão, somente falhas de aplicativos de VDAs com SO multissessão são exibidas. Você pode definir o monitoramento de falhas de aplicativos usando as políticas Monitoring. Para obter mais informações, consulte Configurações da política de monitoramento.

Exibir resultados do probe de aplicativo: a guia Application Probe Results exibe os resultados do probe dos aplicativos que foram configurados para investigação na página Configuration. Nela, é registrado o estágio da inicialização durante o qual ocorreu a falha do início do aplicativo.

Esse recurso requer Delivery Controllers e VDAs **versão 7.18** ou posterior. Para obter mais informações, consulte Investigação de aplicativo.

Criar relatórios personalizados: a guia Custom Reports fornece uma interface de usuário para gerar relatórios personalizados contendo dados históricos e em tempo real do banco de dados de monitoramento em formato tabular.

Esse recurso requer Delivery Controllers **versão 7.12** ou posterior.

Na lista de consultas ao relatório personalizado salvas anteriormente, você pode clicar em **Run and download**, para exportar o relatório em formato CSV, clicar em **Copy OData**, para copiar e compartilhar a consulta OData correspondente, ou clicar em **Edit**, para editar a consulta.
Você pode criar uma consulta ao relatório personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativos. Especifique as condições de filtro com base em máquina, grupo de entrega ou período de tempo. Especifique as colunas adicionais necessárias no seu relatório personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta ao relatório personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta ao relatório personalizado com base em uma consulta OData copiada.

Para isso, selecione a opção OData Query e cole a consulta OData copiada. Você pode salvar a consulta resultante para executar posteriormente.

> **Nota:**
> Os nomes das colunas no relatório de visualização e exportação gerados usando consultas OData não são localizados e aparecem em inglês.

Os ícones dos sinalizadores no gráfico indicam eventos ou ações significativos para o intervalo de tempo específico. Passe o mouse sobre o sinalizador e clique para listar eventos ou ações.

> **Nota:**
>
> - Os dados de logon da conexão HDX não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
> - Os grupos de entrega excluídos no Citrix Studio estão disponíveis para seleção nos filtros Trends do Director até que os dados relacionados a eles sejam eliminados. Selecionar um grupo de entrega excluído exibe gráficos com os dados disponíveis até a retenção. No entanto, as tabelas não mostram nenhum dado.
> - Mover uma máquina contendo sessões ativas de um grupo de entrega para outro faz com que as tabelas **Resource Utilization e Load Evaluator Index** do novo grupo de entrega exibam métricas consolidadas dos grupos de entrega antigo e novo.

Solucionar problemas de implantações

June 28, 2023

Como administrador do suporte técnico, você pode pesquisar o usuário que relatou um problema e exibir detalhes de sessões ou aplicativos associados a esse usuário. Da mesma forma, procure máquinas ou pontos de extremidade onde os problemas são relatados. Resolva problemas rapidamente monitorando as métricas relevantes e realizando as ações adequadas.

As ações disponíveis incluem:

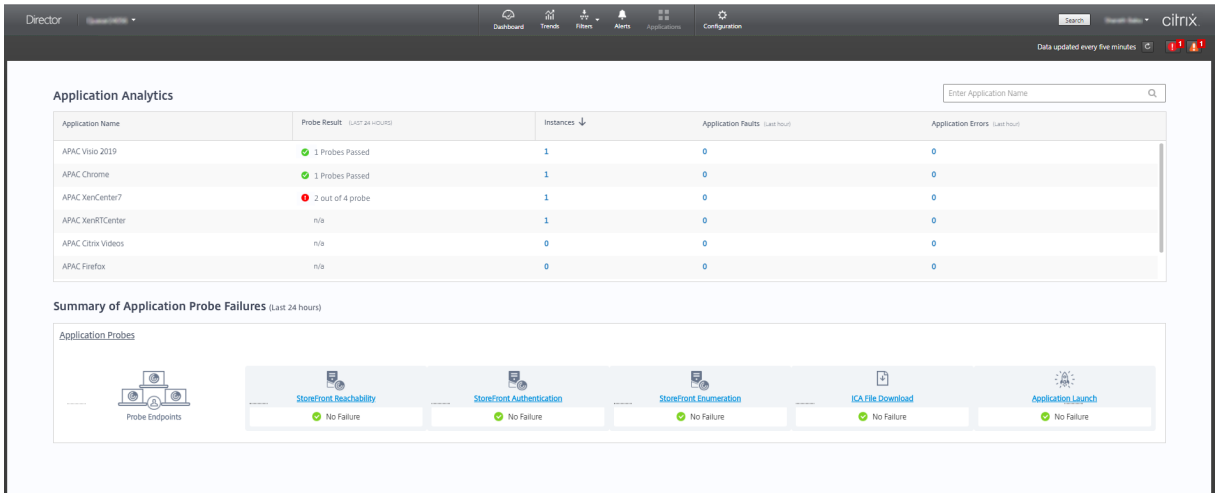
- Encerrar um aplicativo ou processo que não responde
- Sombrear operações na máquina do usuário
- Fazer logoff de uma sessão que não responde
- Reiniciar a máquina
- Colocar uma máquina no modo de manutenção
- Redefinir um perfil de usuário

Solucionar problemas de aplicativos

June 28, 2023

Análise de aplicativos

A exibição **Applications** mostra análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos com eficiência. Você pode obter informações valiosas sobre a integridade e uso de todos os aplicativos publicados no site. A exibição padrão ajuda a identificar os aplicativos em execução mais frequentemente.
Esse recurso requer Delivery Controllers versão 7.16 ou posterior e VDAs versão 7.15 ou posterior.



A coluna **Probe Result** exibe o resultado da execução da investigação do aplicativo nas últimas 24 horas. Clique no link do resultado da investigação na página **Trends** > **Application Probe Results**. Para obter mais detalhes sobre como configurar probes de aplicativos, consulte Investigação de aplicativo.

A coluna **Instances** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativos em execução no momento (instâncias conectadas e desconectadas). Para solucionar problemas, clique no campo **Instances** para ver a página de filtros **Application Instances** correspondente. Nela você pode selecionar instâncias de aplicativos para fazer logoff ou desconectar.

> **Nota:**
>
> Para administradores de escopo personalizados, o Director não exibe instâncias de aplicativos criadas em grupos de aplicativos. Para exibir todas as instâncias do aplicativo, você deve ser um administrador completo. Para obter mais informações, consulte o artigo do Knowledge Center CTX256001.

Monitore a integridade dos aplicativos publicados em seu site com as colunas **Application Faults** e **Application Errors**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao iniciar o aplicativo correspondente na última hora. Clique no campo **Application Faults** ou **Application Errors** para ver os detalhes da falha na página **Trends** > **Application Failures** correspondente ao aplicativo selecionado.

As configurações da política de falha do aplicativo regem a disponibilidade e a exibição de falhas e erros. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da **política Monitoring**.

Monitoramento de aplicativos em tempo real

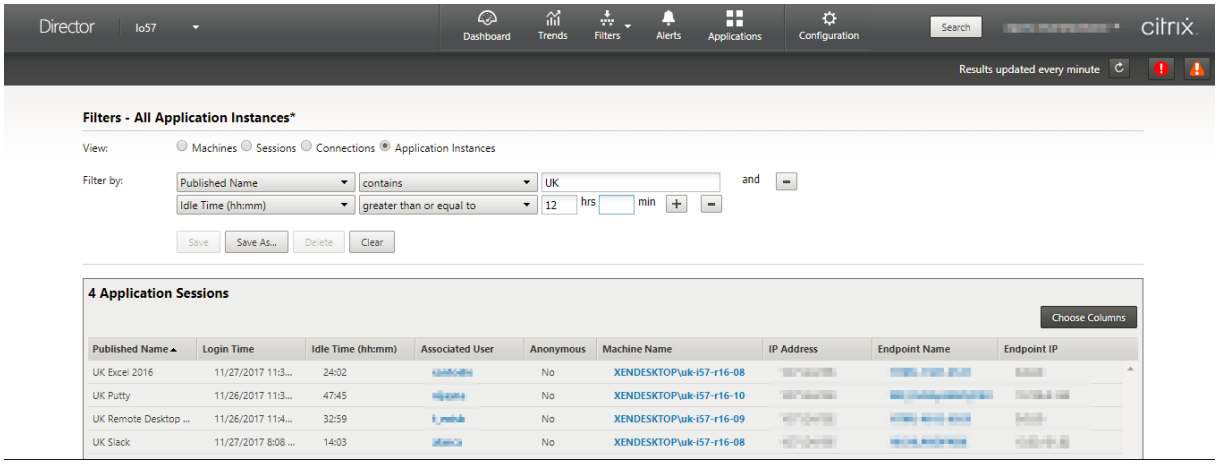
Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas com base em aplicativos são do setor de saúde, onde os funcionários compartilham licenças de aplicativos. Nesses casos, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente do Citrix Virtual Apps and Desktops, para reconfigurar servidores com baixo desempenho ou para manter e atualizar aplicativos.

A página de filtro **Application Instances** lista todas as instâncias de aplicativos em VDAs de SO de sessão única ou servidor. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativos em VDAs com SO multissessão que ficaram ociosas por pelo menos 10 minutos

> **Nota:**
> As métricas de instâncias de aplicativos estão disponíveis nos sites de todas as edições de licença.

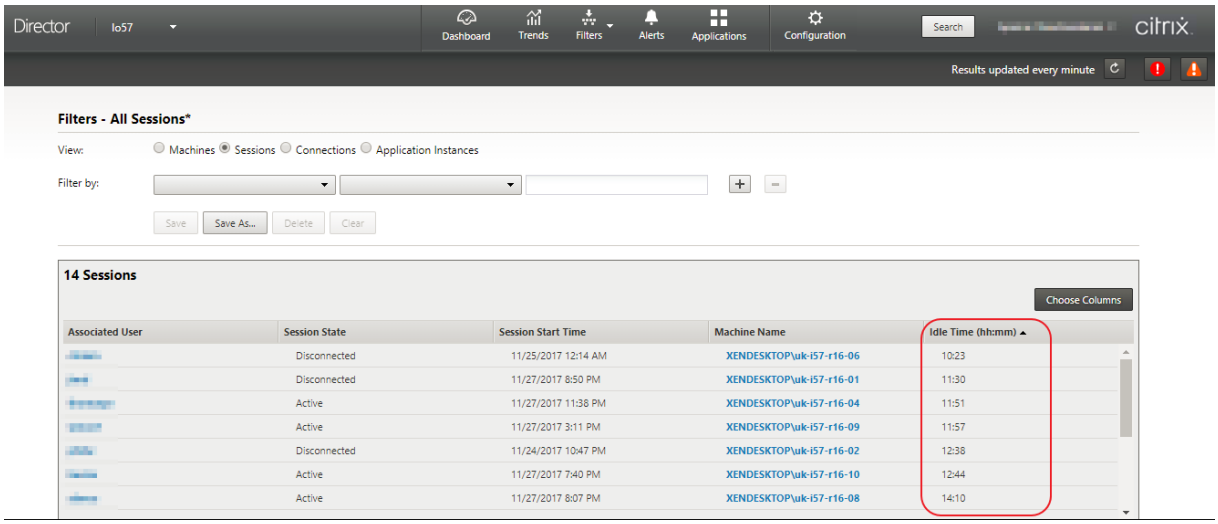
Use essas informações para identificar as instâncias do aplicativo que estão ociosas além de um período de tempo específico e faça logoff ou desconecte-as conforme apropriado. Para isso, selecione **Filters > Application Instances** e selecione um filtro pré-salvo ou escolha **All Application Instances** e crie o seu próprio filtro.



Um exemplo de filtro seria o que se segue. Como critério, em **Filter by**, escolha **Published Name** (do aplicativo) e **Idle Time**. Depois defina **Idle Time** como **greater than or equal to**, especifique um limite de tempo e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias do aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Session Control**, escolha **Logoff** ou **Disconnect** para encerrar as instâncias.

> **Nota:**
> Fazer logoff ou desconectar uma instância do aplicativo encerra ou desconecta a sessão atual, dessa forma, terminando todas as instâncias do aplicativo que pertencem à mesma sessão.

Você pode identificar sessões ociosas na página de filtro **Sessions** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Idle Time** ou defina um filtro para identificar sessões que estão ociosas além de um limite de tempo específico. O tempo ocioso é listado para sessões em VDAs com SO multissessão que ficaram ociosas por pelo menos 10 minutos.



Idle time aparece como **N/A** quando a instância do aplicativo ou sessão

- não ficou ociosa por mais de 10 minutos,

- é iniciado em um VDA com SO de sessão única ou
- é iniciada em um VDA executando a versão 7.12 ou anterior.

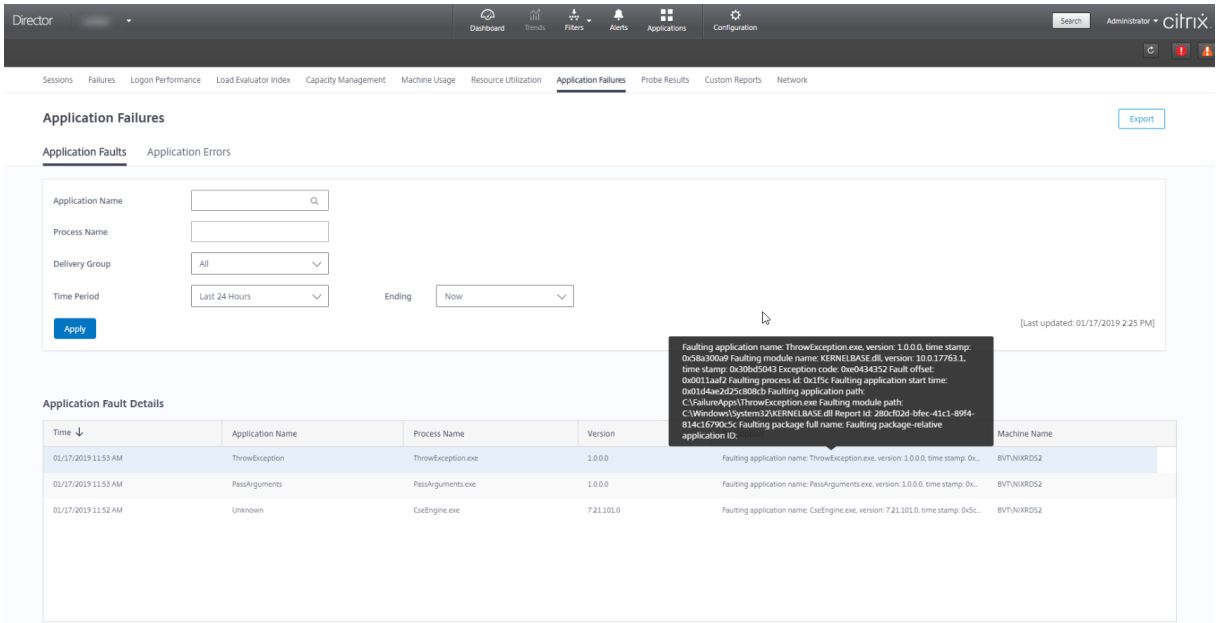
Monitoramento de falhas de aplicativos históricas

A guia **Trends** -> **Application Failures** exibe falhas associadas aos aplicativos publicados nos VDAs.

As tendências de falha de aplicativos estão disponíveis para as últimas 2 horas, 24 horas, 7 dias e um mês, para sites com licenças Premium e Advanced. Para outros tipos de licença, elas estão disponíveis para as últimas 2 horas, 24 horas e 7 dias. As falhas de aplicativo registradas no log do Event Viewer com "Application Errors"na origem são monitoradas. Clique em **Export** para gerar relatórios em formatos CSV, Excel ou PDF.

As configurações de retenção de limpeza para monitoramento de falhas de aplicativos, GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays, são definidas como um dia por padrão para sites licenciados Premium e não Premium. Você pode alterar essa configuração usando o comando do PowerShell:

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value
\> <!--NeedCopy-->
```



As falhas são exibidas como **Application Faults** ou **Application Errors** com base em sua gravidade. A guia Application Faults exibe falhas associadas à perda de funcionalidade ou dados. Application Errors indica problemas que não são imediatamente relevantes, mas que significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Published Application Name**, **Process Name** ou **Delivery Group**, e **Time Period.** A tabela exibe o código de falha ou erro e uma breve descrição da falha. A

descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:**
> O nome do aplicativo publicado é exibido como "Unknown"quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de área de trabalho ou quando falha devido a uma exceção não tratada causada por um executável dependente.

Por padrão, somente falhas de aplicativos hospedados em VDAs com SO multissessão são monitoradas. Você pode modificar as configurações de monitoramento por meio das políticas de grupo Monitoring: Enable monitoring of application failures, Enable monitoring of application failures on Single-session OS VDAs e List of applications excluded from failure monitoring. Para obter mais informações, consulte Políticas para monitoramento de falhas de aplicativos nas configurações da política Monitoring.

A página **Trends > Application Probe Results** exibe os resultados da investigação de aplicativos executada no site nas últimas 24 horas e 7 dias. Para obter mais detalhes sobre como configurar probes de aplicativos, consulte Investigação de aplicativo.

Investigação de aplicativo

June 28, 2023

A investigação de aplicativos automatiza o processo de verificação da integridade do Citrix Virtual Apps que é publicado em um site por meio do teste de inicialização de aplicativos selecionados em série usando o StoreFront. Os resultados da investigação do aplicativo estão disponíveis no Director.

Requisitos:

- Delivery Controller executando a versão 7.18 ou posterior.
- Máquinas de ponto de extremidade executando Probe Agents são máquinas Windows com Citrix Receiver para Windows versão 4.8 ou posterior, ou aplicativo Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versão 1808 ou posterior. Aplicativo Workspace para UWP (Plataforma Universal do Windows) não é suportado.
- O Citrix Probe Agent suporta a autenticação padrão baseada em formulários, conforme suportada pelo StoreFront e pelo Citrix WorkSpace. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como logon único (SSO) ou autenticação multifator (MFA). Da mesma forma, o Citrix Probe Agent funciona somente quando não há servidor proxy ou balanceador de carga, como o Citrix Gateway ou o Citrix ADC, implantado.

- Verifique se o Microsoft .NET Framework versão 4.7.2 ou posterior está instalado na máquina de ponto de extremidade em que você deseja instalar o Probe Agent.

Permissões/contas de usuário necessárias para executar a investigação do aplicativo:

- Um usuário exclusivo do StoreFront para investigar cada máquina de ponto de extremidade. O usuário do StoreFront não precisa ser um administrador; os probes podem ser executados em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de ponto de extremidade.
- Uma conta de usuário de administrador completa ou uma função personalizada com as seguintes permissões. A reutilização de contas de usuário existentes para investigação de aplicativos pode encerrar as sessões ativas dos usuários.
  - Permissões do grupo de entrega:
    - Somente leitura
  - Permissões do Director:
    - Criar\editar\remover configuração do servidor de e-mail de alerta –se o servidor de e-mail ainda não estiver configurado
    - Criar\editar\remover configurações de investigação
    - Exibir a página de configurações
    - Exibir a página de tendências

Configurar a investigação de aplicativos

Você pode agendar as investigações do seu aplicativo para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes da investigação podem ajudar a solucionar problemas relacionados a aplicativos, máquina de hospedagem ou conexão antes que os usuários enfrentem esses problemas.

O Citrix Probe Agent versão 2103 suporta a agregação de sites. Aplicativos e áreas de trabalho podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o probe agent, selecione a opção **Workspace (StoreFront) Site Aggregation Enabled** para ativar a enumeração de aplicativos e áreas de trabalho a partir de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com um URL do StoreFront.
- Sites locais e na nuvem com um URL do StoreFront ou do Workspace.
- Vários sites na nuvem com um URL do Workspace.

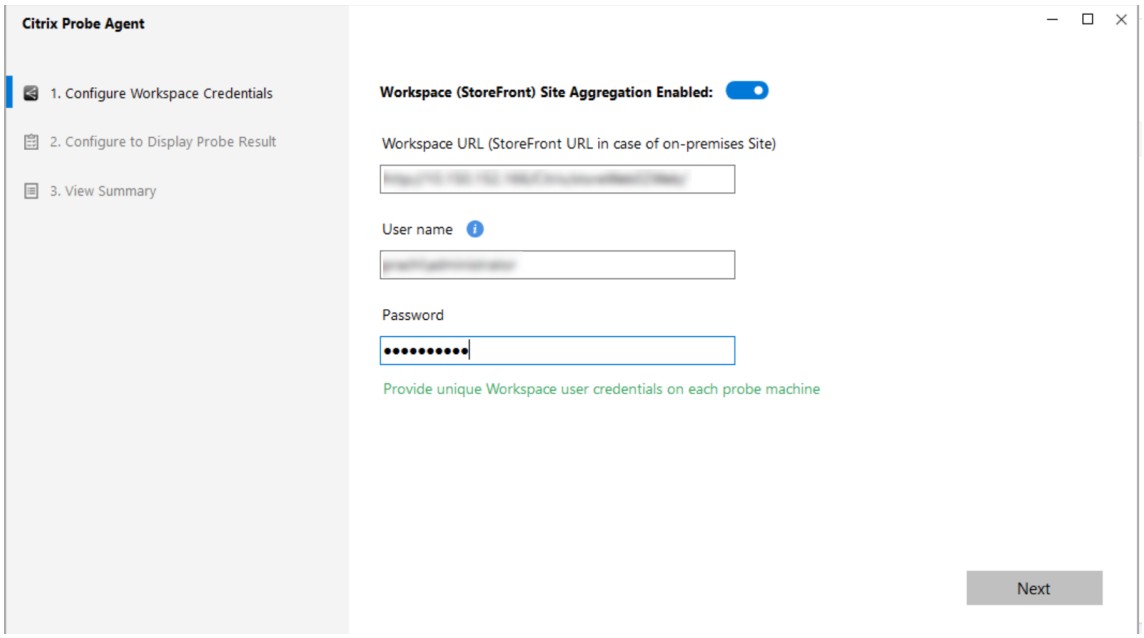
> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar probes que tenham

> acesso a apenas um site.

Etapa 1: Instalar e configurar o Citrix Probe Agent

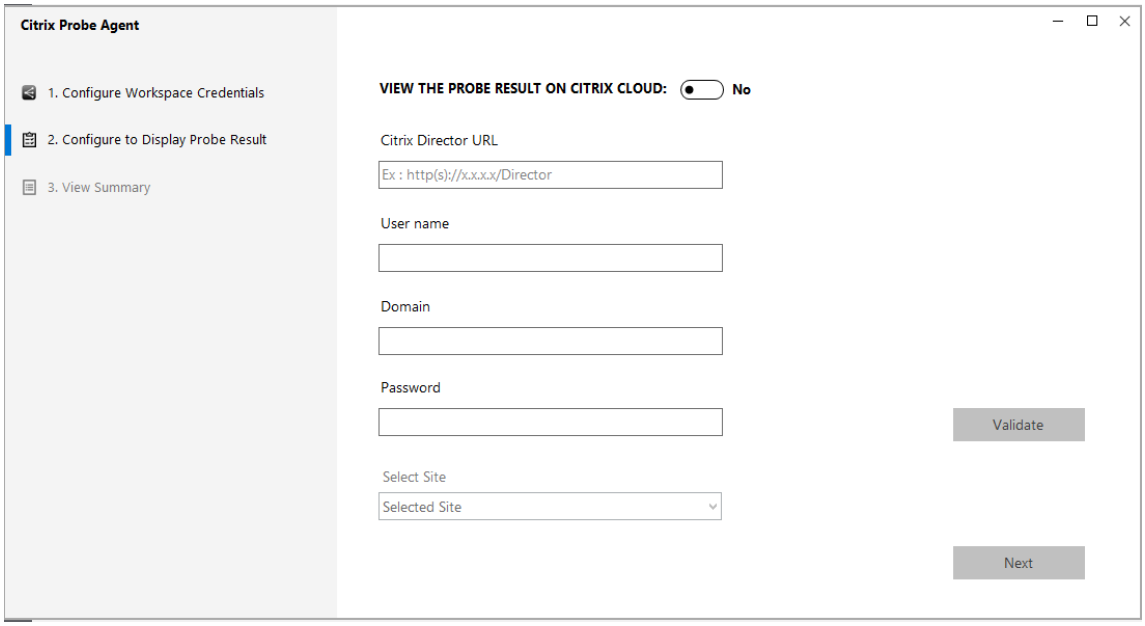
O Citrix Probe Agent é um executável do Windows que simula o início real do aplicativo pelo usuário por meio do StoreFront. Ele testa a inicialização de aplicativos conforme configurada no Director e informa os resultados ao Director.

1. Identifique as máquinas de ponto de extremidade de onde você deseja executar a investigação do aplicativo.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de ponto de extremidade. Baixe o executável Citrix Probe Agent disponível em https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie o agente e configure suas credenciais do StoreFront Receiver para Web. Configure um usuário exclusivo do StoreFront em cada máquina de ponto de extremidade. As credenciais são criptografadas e armazenadas com segurança.



> **Nota:**
>
> Para acessar o site a ser investigado de fora da rede, digite o URL de login do Citrix Gateway no campo de URL do StoreFront. O Citrix Gateway roteia automaticamente a solicitação para o URL do StoreFront do site correspondente. Esse recurso está disponível para o Citrix Gateway versão 12.1 e posterior (tema RfWebUI) e Delivery Controllers 1811 e posteriores.

4. Na guia **Configure To Display Probe Result**, insira suas credenciais do Director e clique em **Validate**.



5. Selecione seu site e clique em **Next**.

Etapa 2: Configurar a investigação de aplicativo no Director

1. Vá para **Configuration** > **Probe Configuration** > **Application Probe** e clique em **Create Probe**.
2. Na página **Create Probe**, insira o nome da investigação.
3. Selecione a programação:

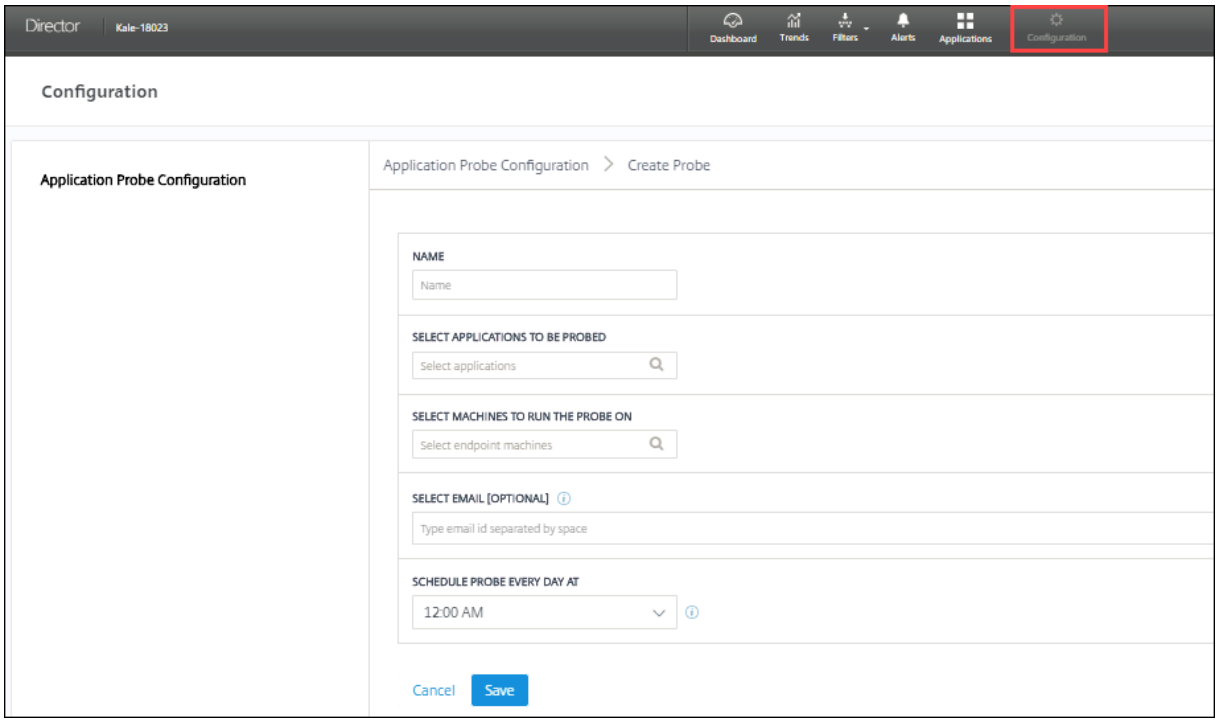
    a) Escolha os dias da semana em que você deseja que a investigação seja executada.
    b) Insira a hora de início na qual você deseja que a investigação seja executada.
    c) Além disso, você pode escolher a opção **Repeat in a day**. Insira a hora de término e o intervalo que deseja que a investigação seja repetida no dia. Por exemplo, a configuração abaixo ajuda a executar investigações de aplicativos das 12h08 até as 16h34, repetindo-as a cada 30 minutos todas as segundas, quartas, quintas e domingos.

4. Selecione o número recomendado de aplicativos a serem investigados, de acordo com o intervalo.
5. Selecione as máquinas de ponto de extremidade nas quais a investigação deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da investigação da falha são enviados.

Nessa configuração, as sessões do aplicativo são iniciadas às 12h08, 12h38, 13h08 e assim por diante até as 16h08 todas as segundas, quartas, quintas e domingos.

Nota:

- Configure seu servidor de e-mail em **Alerts** > **Email Server Configuration**.
- Após a configuração, o agente executa as investigações configuradas começando na próxima hora.
- As investigações, ou sondagens, que foram configuradas antes da introdução da opção **Repeat in a day** continuam sendo executadas no horário programado. Elas têm a opção **Repeat in a day** desativada por padrão.



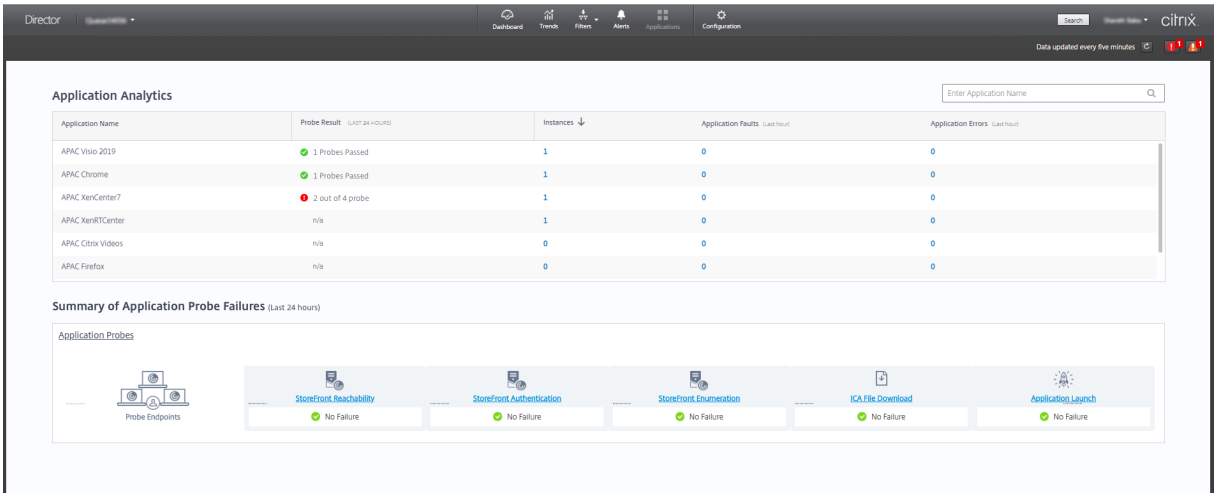
Etapa 3: Execução da investigação

O agente executa a investigação do aplicativo de acordo com a configuração do probe que ele busca no Director periodicamente. Ele inicia aplicativos selecionados em série usando o StoreFront. O agente relata os resultados de volta ao Director através do banco de dados de monitoramento. As falhas são relatadas em cinco estágios específicos:

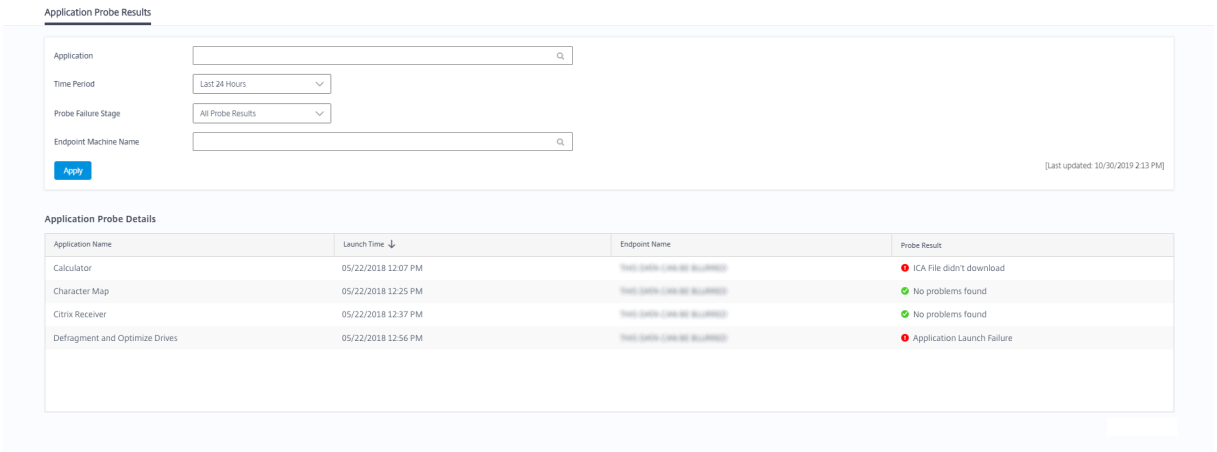
- **StoreFront Reachability** –a URL do StoreFront configurada não pode ser acessada.
- **StoreFront Authentication** –as credenciais do StoreFront configuradas são inválidas.
- **StoreFront Enumeration** –a lista de aplicativos do StoreFront Enumerate não contém o aplicativo a ser investigado.
- **ICA download** –o arquivo ICA não está disponível.
- **Application launch** –o aplicativo não pode ser iniciado.

Etapa 4: Exibir resultados da investigação

Você pode ver os resultados da investigação mais recente na página **Applications**.



Para ver mais detalhes para a solução de problemas, clique no link do resultado da investigação na página **Trends** > **Application Probe Results**.



Os dados dos resultados da investigação consolidados estão disponíveis para as últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a investigação falhou. Você pode filtrar a tabela para um aplicativo específico, estágio de falha da investigação ou máquina de ponto de extremidade.

Investigação da área de trabalho

June 28, 2023

A investigação de áreas de trabalho automatiza o processo de verificação da integridade do Citrix Virtual Desktops que é publicado em um site por meio do teste de inicialização de áreas de trabalho selecionadas em série usando o StoreFront. Os resultados da investigação da área de trabalho estão disponíveis no Director.

Na página Configuration do Director, configure as áreas de trabalho a serem investigadas, as máquinas de ponto de extremidade para executar a investigação e o tempo da investigação. O agente testa o início de áreas de trabalho selecionadas usando o StoreFront e informa os resultados de volta ao Director. Os resultados da investigação são exibidos na interface do usuário do Director —os dados das últimas 24 horas na página Applications e os dados da investigação de histórico na página **Trends > Probe Results > Desktop Probe Results**. Aqui, você pode ver o estágio em que a falha de investigação ocorreu –StoreFront Reachability, StoreFront Authentication, StoreFront Enumeration, ICA Download ou Desktop Launch. O relatório de falhas é enviado para os endereços de e-mail configurados. Você pode agendar as investigações da sua área de trabalho para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes podem ajudar a solucionar problemas proativamente relacionados a áreas de trabalho provisionadas, máquinas de hospedagem ou conexões antes que os usuários enfrentem esses problemas. A investigação de área de trabalho está disponível para sites licenciados Premium. Esse recurso requer Delivery Controllers versão 7 1906 ou posterior e o Probe Agent 1903 ou posterior.

Requisitos:

- Delivery Controller executando a versão 1906 ou posterior.
- Máquinas de ponto de extremidade executando probe agents são máquinas Windows com Citrix Receiver para Windows versão 4.8 ou posterior, ou aplicativo Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versão 1906 ou posterior. Aplicativo Workspace para UWP (Plataforma Universal do Windows) não é suportado.
- O Citrix Probe Agent suporta a autenticação padrão baseada em formulários, conforme suportada pelo StoreFront e pelo Citrix WorkSpace. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como logon único (SSO) ou autenticação multifator (MFA). O Citrix Probe Agent funciona somente quando não há servidor proxy ou balanceador de carga, como o Citrix Gateway ou o Citrix ADC, implantado.
- Verifique se o Microsoft .NET Framework versão 4.7.2 ou posterior está instalado na máquina de ponto de extremidade em que você deseja instalar o Probe Agent.

Permissões ou contas de usuário necessárias para executar a investigação da área de trabalho:

- Um usuário exclusivo do StoreFront para investigar cada máquina de ponto de extremidade. O usuário do StoreFront não precisa ser um administrador; os probes podem ser executados em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de ponto de extremidade.

- Uma conta de usuário de administrador completa ou uma função personalizada com as seguintes permissões. A reutilização de contas de usuário normais para investigação de áreas de trabalho pode encerrar as sessões ativas dos usuários.
  - Permissões do 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 investigação
    - Exibir a página de configurações
    - Exibir a página de tendências

Configurar a investigação de área de trabalho

Você pode agendar as investigações da sua área de trabalho para serem executadas fora do horário de pico em diferentes regiões geográficas. Os resultados abrangentes da investigação podem ajudar a solucionar problemas relacionados a áreas de trabalho, máquina de hospedagem ou conexão antes que os usuários enfrentem esses problemas.

O Citrix Probe Agent versão 2103 suporta a agregação de sites. Aplicativos e áreas de trabalho podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o probe agent, selecione a opção **Workspace (StoreFront) Site Aggregation Enabled** para ativar a enumeração de aplicativos e áreas de trabalho a partir de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com um URL do StoreFront.
- Sites locais e na nuvem com um URL do StoreFront ou do Workspace.
- Vários sites na nuvem com um URL do Workspace.

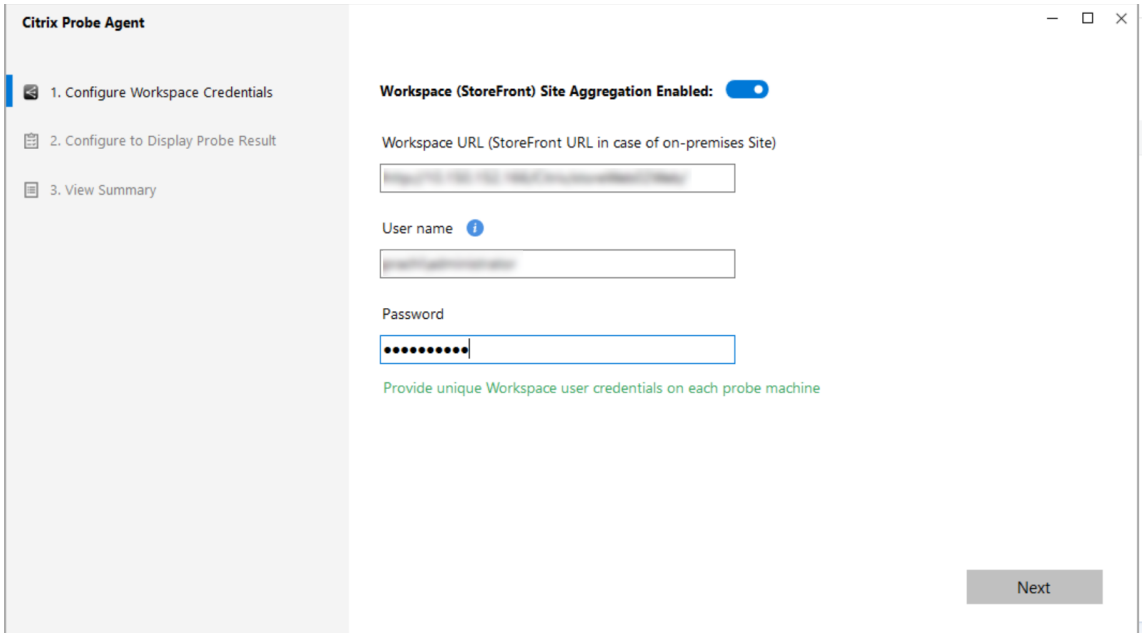
> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar probes que tenham acesso a apenas um site.

Etapa 1: Instalar e configurar o Citrix Probe Agent

O Citrix Probe Agent é um executável do Windows que simula o início real da área de trabalho pelo usuário por meio do StoreFront. Ele testa a inicialização de áreas de trabalho conforme configurada no Director e informa os resultados ao Director.

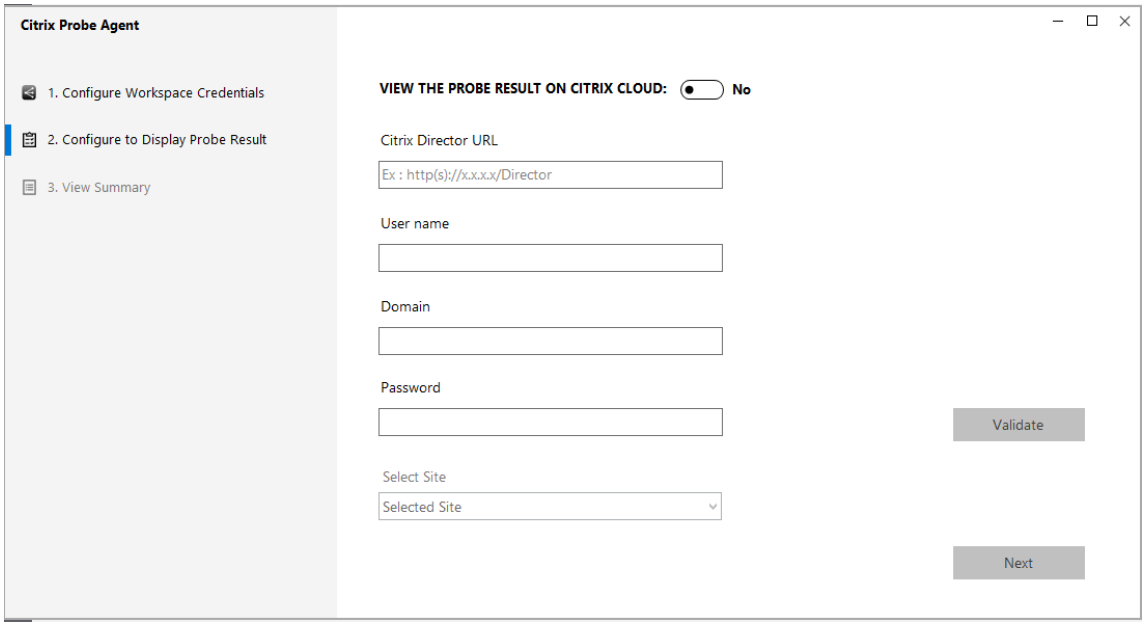
1. Identifique as máquinas de ponto de extremidade de onde você deseja executar a investigação da área de trabalho.

2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de ponto de extremidade. Baixe o executável Citrix Probe Agent disponível em https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie o agente e configure suas credenciais do StoreFront Receiver para Web. Configure um usuário exclusivo do StoreFront em cada máquina de ponto de extremidade. As credenciais são criptografadas e armazenadas com segurança.



> **Nota:**
>
> - Para acessar o site a ser investigado de fora da rede, digite o URL da página de login do Citrix Gateway no campo URL do StoreFront. O Citrix Gateway roteia automaticamente a solicitação para o URL do StoreFront do site correspondente. Esse 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 exclusivo configurado do StoreFront.

4. Na guia **Configure To Display Probe Result**, insira suas credenciais do Director e clique em **Validate**.



5. Selecione seu site e clique em **Next**.

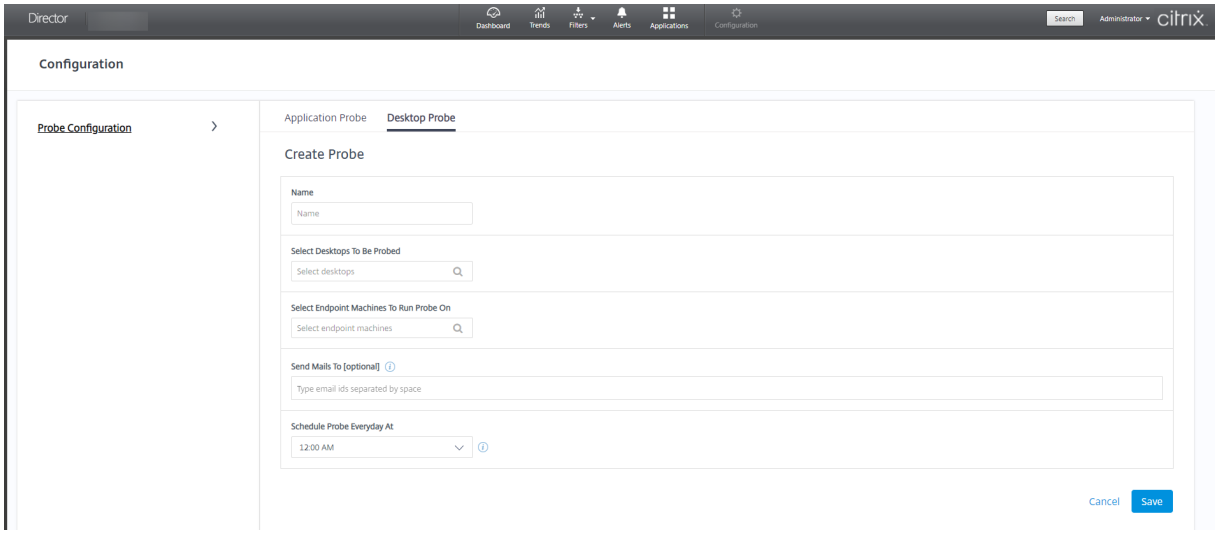
Etapa 2: Configurar a investigação de área de trabalho no Director

1. Vá para **Configuration** > **Probe Configuration** > **Desktop Probe** e clique em **Create Probe**.
2. Na página **Create Probe**, insira o nome da investigação.
3. Selecione a programação:

    a) Escolha os dias da semana em que você deseja que a investigação seja executada.
    b) Insira a hora de início na qual você deseja que a investigação seja executada.
    c) Além disso, você pode escolher a opção **Repeat in a day**. Insira a hora de término e o intervalo que deseja que a investigação seja repetida no dia. Por exemplo, a configuração abaixo ajuda a executar investigações de áreas de trabalho das 12h10 às 23h35, repetindo-as a cada hora todas as terças, quintas e sextas-feiras.

4. Selecione o número recomendado de áres de trabalho a serem investigadas, de acordo com o intervalo.
5. Selecione as máquinas de ponto de extremidade nas quais a investigação deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da investigação da falha são enviados.

Nessa configuração, as sessões de áreas de trabalho são iniciadas às 12h10, 13h10, 14h10 e assim por diante até as 23h10 todas as terças, quintas e sextas-feiras.



Nota:

- Configure seu servidor de e-mail em **Alerts** > **Email Server Configuration**.
- Após concluir a configuração da investigação da área de trabalho, o agente executa as investigações configuradas começando na próxima hora.
- As investigações, ou sondagens, que foram configuradas antes da introdução da opção **Repeat in a day** continuam sendo executadas no horário programado. Elas têm a opção **Repeat in a day** desativada por padrão.

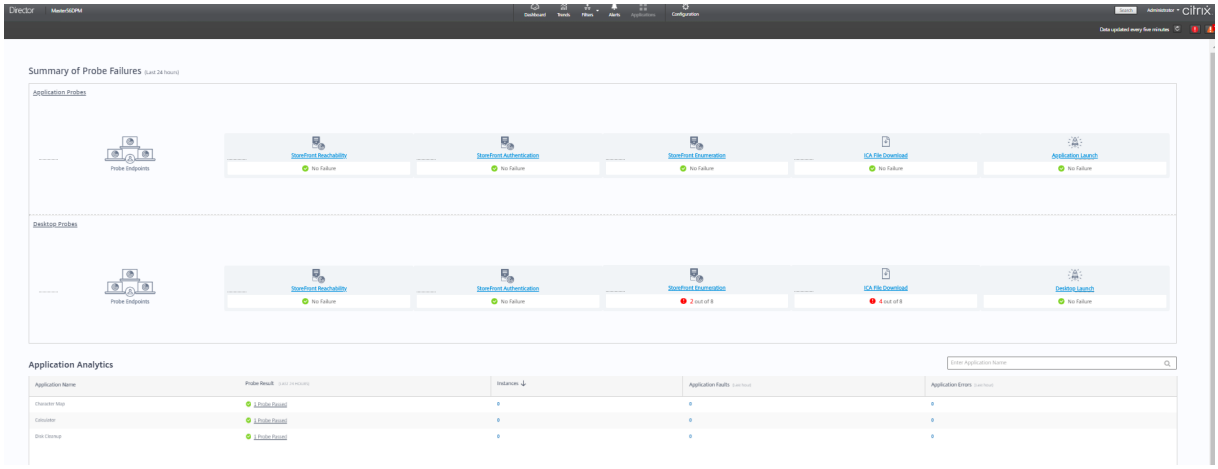
Etapa 3: Execução da investigação

O agente executa a investigação da área de trabalho de acordo com a configuração do probe que ele busca no Director periodicamente. Ele inicia áreas de trabalho selecionadas em série usando o StoreFront. O agente relata os resultados de volta ao Director através do banco de dados de monitoramento. As falhas são relatadas em cinco estágios específicos:

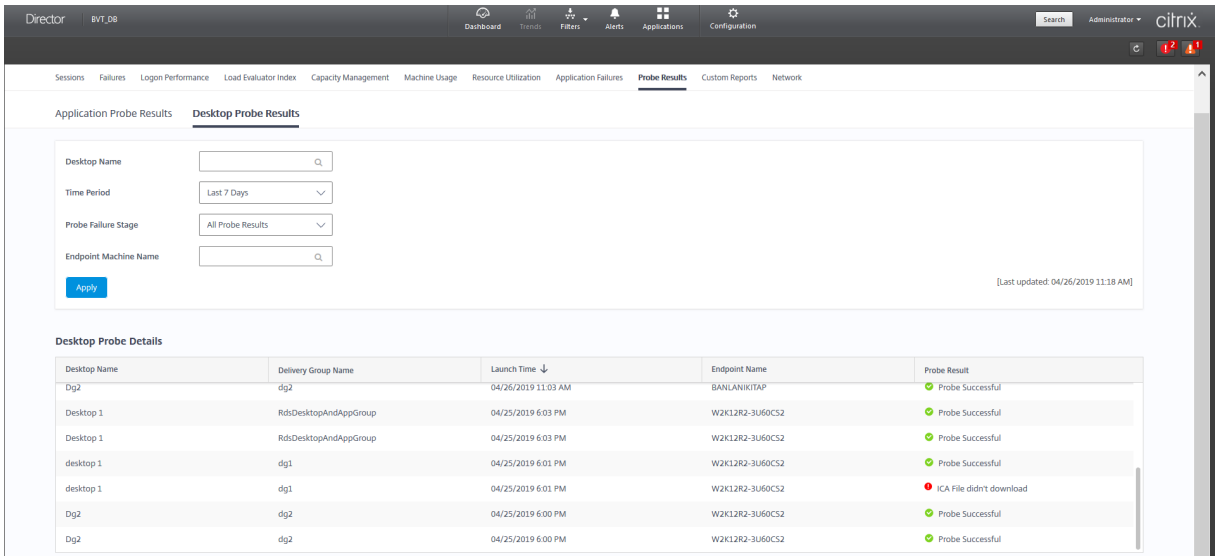
- **StoreFront Reachability** –a URL do StoreFront configurada não pode ser acessada.
- **StoreFront Authentication** –as credenciais do StoreFront configuradas são inválidas.
- **StoreFront Enumeration** –a lista de áreas de trabalho do StoreFront Enumerate não contém a área de trabalho a ser investigada.
- **ICA download** –o arquivo ICA não está disponível.
- **Desktop launch** –a área de trabalho não pode ser iniciada.

Etapa 4: Exibir resultados da investigação

Você pode ver os resultados da investigação mais recente na página **Desktops**.



Para ver mais detalhes para a solução de problemas, clique no link do resultado da investigação na página **Trends** >**Probe Results** > **Desktop Probe Results**.



Os dados dos resultados da investigação consolidados estão disponíveis para as últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a investigação falhou. Você pode filtrar a tabela para uma área de trabalho específica, estágio de falha da investigação ou máquina de ponto de extremidade.

Solucionar problemas de máquinas

June 28, 2023

> **Nota:**
>
> O **Citrix Health Assistant** é uma ferramenta para solucionar problemas de configuração em VDAs não registrados. A ferramenta automatiza várias verificações de integridade para identificar possíveis causas de falhas de registro do VDA e problemas na configuração de redirecionamento de fuso horário e início de sessão. O artigo do Knowledge Center Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém as instruções de download e uso da ferramenta **Citrix Health Assistant**.

A exibição **Filters > Machines** no console Director mostra as máquinas configuradas no site. A guia Multi-session OS Machines inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessão quando você passa o mouse sobre o link.

Clique na coluna **Failure Reason** de uma máquina com falha para obter uma descrição detalhada da falha e das ações recomendadas para solucionar o problema. Os motivos de falha e as ações recomendadas para falhas de máquina e na conexão estão disponíveis em Citrix Director 7.12 Failure Reasons Troubleshooting Guide.

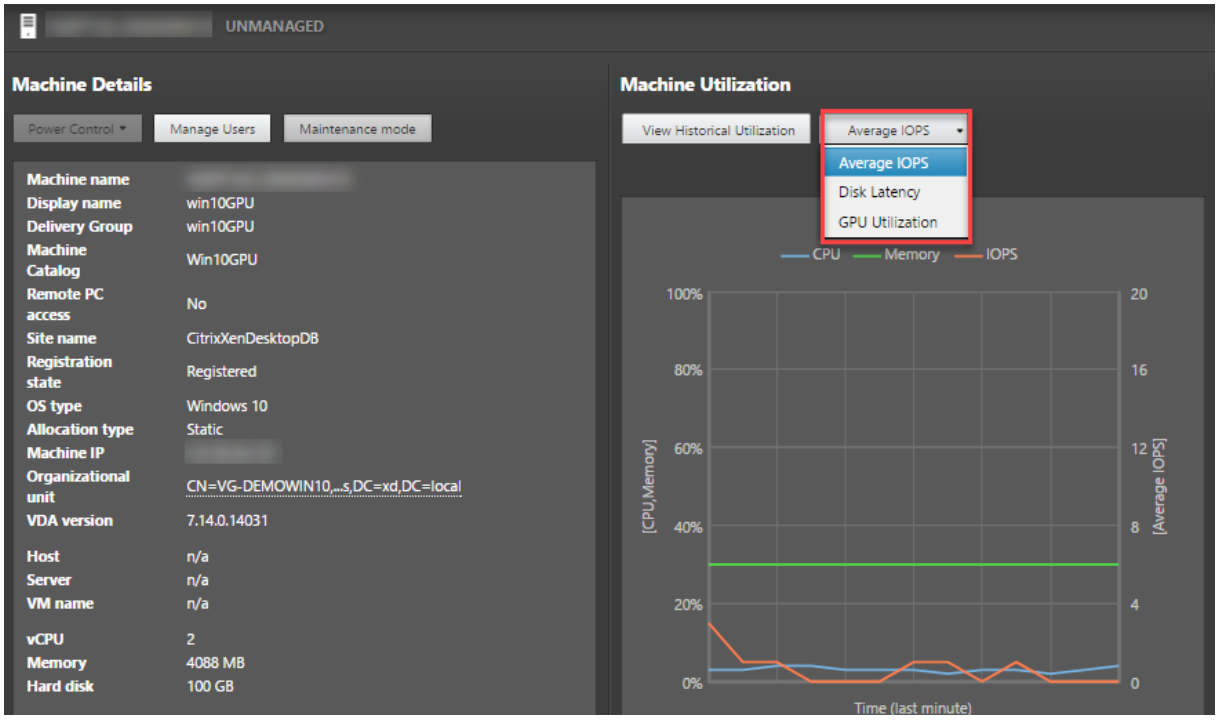
Clique no link do nome da máquina para ir para a página **Machine Details**.

A página Machine Details lista os detalhes da máquina, os detalhes da infraestrutura e os detalhes dos hotfixes aplicados na máquina.

Utilização em tempo real de recursos baseada em máquina

O painel **Machine Utilization** exibe gráficos que mostram a utilização em tempo real da CPU e da memória. Além disso, gráficos de monitoramento de disco e GPU estão disponíveis para sites com Delivery Controllers e VDA **7.14** ou versões posteriores.

Gráficos de monitoramento de disco, média de IOPS e latência de disco são medições de desempenho importantes que ajudam a monitorar e solucionar problemas relacionados aos discos VDA. O gráfico Average IOPS exibe o número médio de leituras e gravações em um disco. Selecione **Disk Latency** para ver um gráfico do atraso entre uma solicitação de dados e o seu retorno do disco, medido em milissegundos.



Utilização de GPU

Selecione **Utilização de GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do codificador e do decodificador para solucionar problemas relacionados à GPU em VDAs com SO multissessão ou de sessão única.

Versões de GPU suportadas:

- GPUs NVIDIA Tesla M60 executando o Display Driver versão 369.17 ou posterior. Para obter mais informações, consulte Software NVIDIA vGPU.
- GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12(Rome). Para obter mais informações, consulte Suporte e Drivers AMD.

Drivers:

Os drivers ou extensões apropriados devem ser instalados nos VDAs.

- Para GPUs NVIDIA, instale os drivers GRID manualmente ou por meio de extensões. Para obter mais informações, consulte Software NVIDIA vGPU.
  - Observe que, para NVIDIA, somente os drivers GRID são suportados. Os drivers CUDA não funcionam com a série NVadsA10 v5 e não são suportados.
  - Para ver um exemplo do processo de instalação de drivers da GPU Nvidia Grid por meio de extensões em máquinas baseadas no Azure, consulte Drivers NVIDIA GRID. Extensão de driver de GPU NVIDIA - VMs do Azure Windows - Máquinas virtuais do Azure.

  - Para ver um exemplo do processo para instalar manualmente os drivers da GPU Nvidia Grid, consulte Configuração de driver de GPU NVIDIA da série N do Azure para Windows - Máquinas virtuais do Azure.

- Para GPUs AMD, instale os drivers gráficos AMD manualmente ou por meio de extensões. Para obter mais informações, consulte Suporte e Drivers AMD.

  - Para ver um exemplo do processo de instalação de drivers de GPU AMD por meio de extensões em máquinas baseadas no Azure, consulte Extensão do Driver GPU AMD - VMs do Azure Windows - Máquinas virtuais do Azure.
  - Para ver um exemplo do processo de instalação manual de drivers de GPU AMD em máquinas do Azure, consulte Instalação de drivers de GPU AMD em VMs da série N executando Windows.

Notas de uso:

- Os gráficos de utilização de GPU estão disponíveis somente para VDAs que executam o Windows de 64 bits.
- Os VDAs devem ter o HDX 3D Pro habilitado para fornecer aceleração de GPU. Para obter mais informações, consulte Aceleração da GPU para SO Windows de sessão única e Aceleração da GPU para SO multissessão Windows.
- Quando um VDA acessa mais de uma GPU, o gráfico de utilização exibe a média das métricas da GPU coletadas das GPUs individuais. As métricas da GPU são coletadas para todo o VDA e não para processos individuais.
- Para AMD, o uso do codificador e o uso do decodificador não são suportados separadamente. Qualquer carga de trabalho de codificação/decodificação usando a GPU será relatada como a carga geral 3D no uso da GPU.
- Certifique-se de instalar o NVIDIA WMI durante a instalação. Essa janela está disponível somente durante a instalação manual.
- Se os drivers estiverem instalados, mas o Director não detectar a GPU

  - Verifique o Gerenciador de tarefas. Se os drivers estiverem instalados corretamente, a GPU deverá aparecer no Gerenciador de tarefas.
  - Verifique se a máquina está registrada. Às vezes, as máquinas podem levar algum tempo para serem detectadas como online.

- Se o uso da GPU não mostrar nenhuma atividade no Director, verifique se a carga de trabalho que você está executando está usando a GPU. Para cargas de trabalho gráficas, isso pode ser ativado em Configurações > Sistema > Tela > Configurações de elementos gráficos > Escolha um aplicativo para definir a preferência. Certifique-se de ativar Alto desempenho. Às vezes, o Windows usa a CPU como padrão para cargas de trabalho gráficas quando ela é definida como padrão do sistema ou economia de energia, com base em outras configurações.

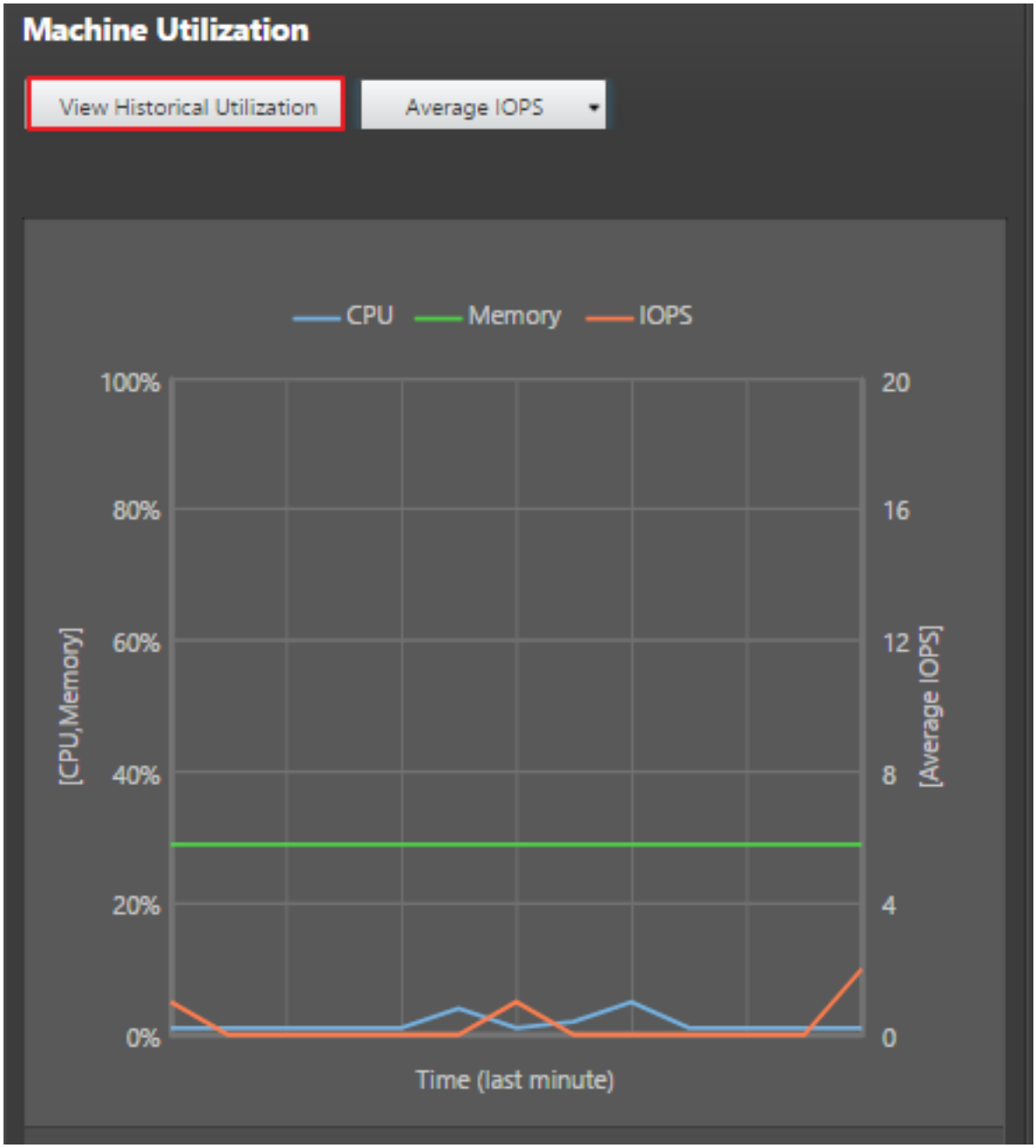
- Os dados são atualizados a cada minuto e a visualização dos dados começa um minuto após selecionar **Utilização de GPU**.

Utilização histórica de recursos baseada em máquina

No painel **Machine Utilization**, clique em **View Historical Utilization** para exibir o uso histórico de recursos na máquina selecionada.
Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, pico de sessões simultâneas, média de IOPS e latência de disco.

> **Nota:**
>
> A configuração de política de monitoramento **Enable Process Monitoring** deve ser definida como Allowed para coletar e exibir dados na tabela Top 10 Processes na página Historic Machine Utilization. A coleção é proibida por padrão.

Os dados de utilização da CPU e da memória, média de IOPS e latência de disco são coletados por padrão. Você pode desativar a coleta usando a configuração de política **Enable Resource Monitoring**.

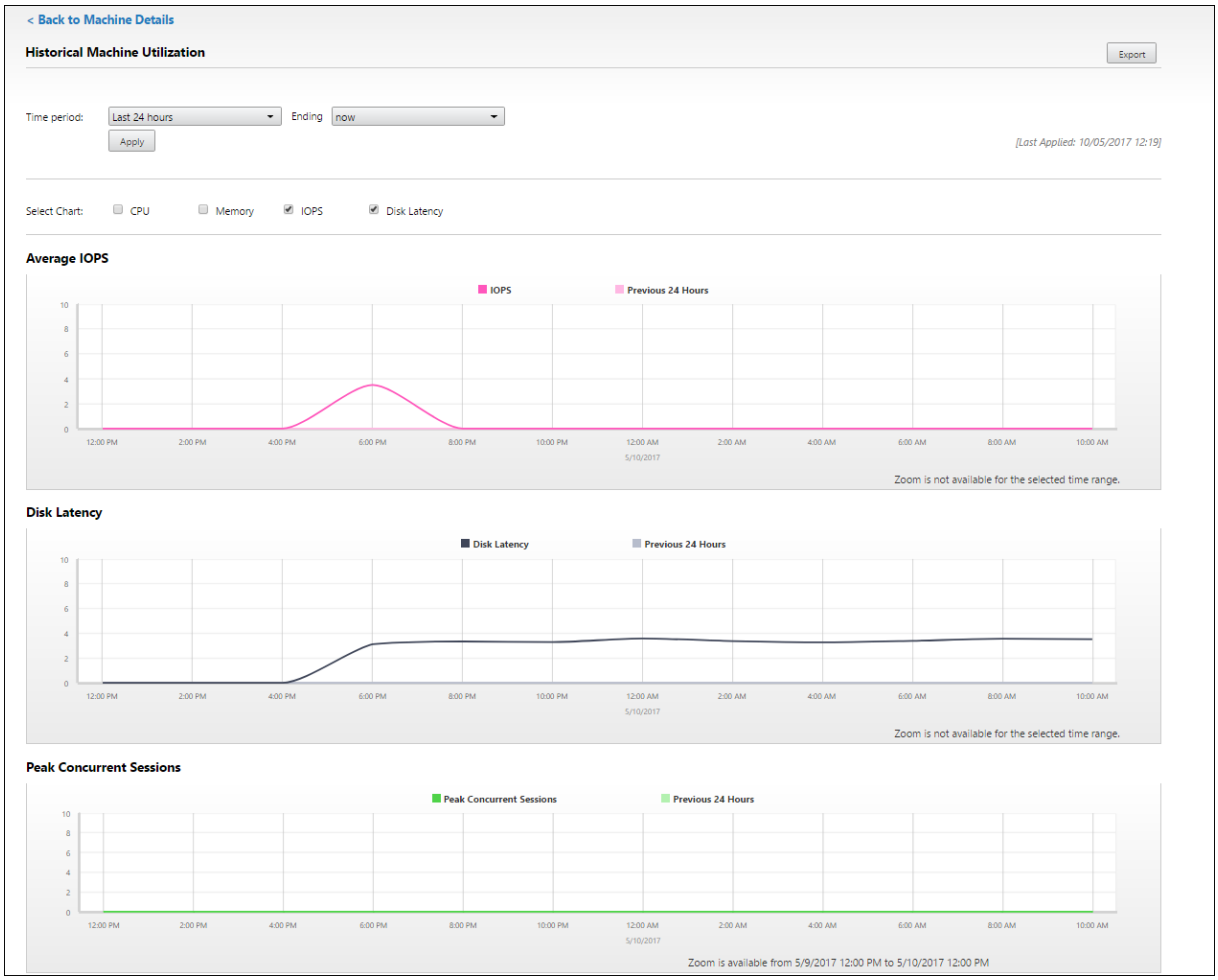


1. No painel **Machine Utilization**, na exibição **Machine Details**, selecione **View Historical Utilization**.
2. Na página **Historical Machine Utilization**, defina **Time Period** para ver o uso nas últimas 2 horas, 24 horas, 7 dias, mês ou ano.

> **Nota:**
>
> Os dados de uso médio de IOPS e latência de disco estão disponíveis somente para as últimas 24 horas, para o último mês e para o último ano até agora, onde Ending é definido

> como “now”. A hora de término personalizada não é suportada.

3. Clique em **Apply** e selecione os gráficos necessários.
4. Passe o mouse sobre diferentes seções do gráfico para exibir mais informações para o período selecionado.



Por exemplo, se você selecionar **Last 2 hours**, o período da linha de base será as 2 horas antes do intervalo de tempo selecionado. Exiba a tendência de CPU, memória e sessão nas últimas 2 horas e no horário da linha de base. Se você selecionar **Last month**, o período da linha de base será o mês anterior. Selecione para exibir a IOPS média e a latência do disco entre o último mês e o período da linha de base.

1. Clique em **Export** para exportar os dados de utilização do recurso para o período selecionado. Para obter mais informações, consulte a seção Exportar relatórios em Monitorar implantações.
2. Abaixo dos gráficos, a tabela lista os 10 principais processos com base na utilização da CPU ou da memória. Você pode classificar por qualquer uma das colunas: Application Name, User Name, Session ID, Average CPU, Peak CPU, Average Memory e Peak Memory para o período de tempo selecionado. As colunas IOPS e Disk Latency não podem ser ordenadas.

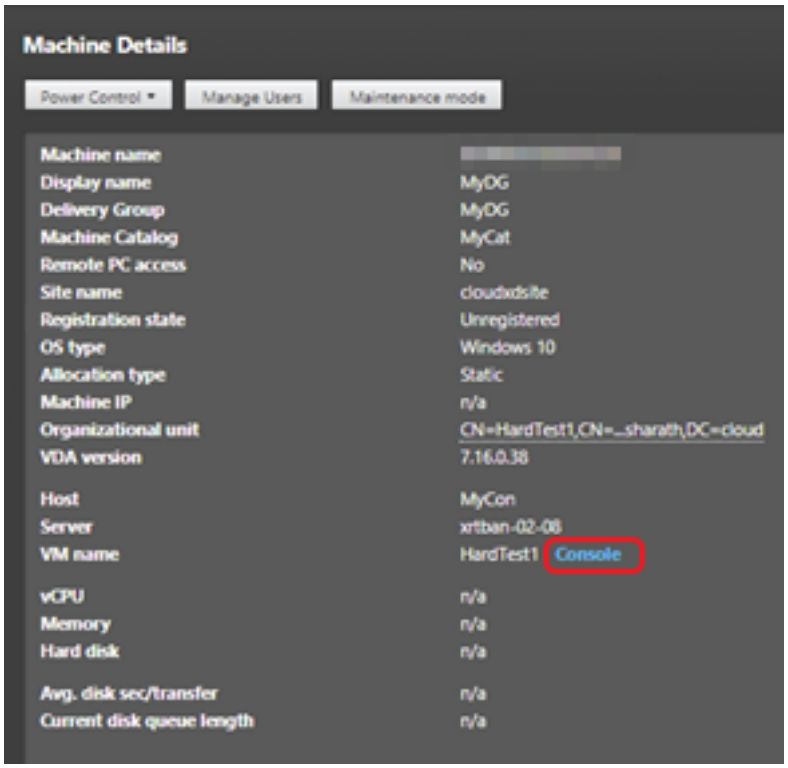
> **Nota:**
>
> O ID da sessão para processos do sistema é exibido como "0000".

3. Para exibir a tendência histórica de consumo de recursos de um processo específico, aprofunde-se nos detalhes de qualquer um dos 10 principais processos.

Acesso ao console da máquina

Você pode acessar os consoles de máquinas com SO de sessão única e 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 da versão 7.16 ou posterior.
- O XenServer que hospeda a máquina deve ser da versão 7.3 ou posterior e deve ser acessível a partir da interface do usuário do Director.



Para solucionar problemas de uma máquina, clique no link **Console** no painel Machine Details correspondente. Após a autenticação das credenciais de host fornecidas, o console da máquina é aberto em uma guia separada usando noVNC, um cliente VNC baseado na Web. Agora você tem acesso ao console pelo teclado e mouse.

> **Nota:**
>
> - Esse recurso não é suportado no Internet Explorer 11.
> - Se o ponteiro do mouse no console da máquina estiver desalinhado, consulte CTX230727 para ver as etapas para corrigir o problema.
> - O Director inicia o acesso ao console em uma nova guia, portanto, certifique-se de que as configurações do navegador permitam pop-ups.
> - Por motivos de segurança, a Citrix recomenda que você instale certificados SSL em seu navegador.

Integridade da licença do Microsoft RDS

Você pode exibir o status da licença do Microsoft RDS no painel Detalhes do computador na página **Detalhes do computador** e **Detalhes do usuário** para máquinas com SO multissessão.

Uma das seguintes mensagens é exibida:

- License available
- Not configured properly (aviso)
- License error (erro)
- Incompatible VDA version (erro)

> **Nota:**
>
> O status de integridade da licença do RDS para máquinas em período de tolerância com licença válida exibe a mensagem **License available** em verde. Renove sua licença antes que ela expire.

Nas mensagens de aviso e erro, passe o mouse sobre o ícone de informações para exibir informações adicionais conforme indicado na tabela a seguir.

Tipo da mensagem	Mensagens no Director
Erro	Disponível para VDAs versão 7.16 e posterior.
Erro	Novas conexões RDS não são permitidas.
Erro	O licenciamento do RDS excedeu seu período de tolerância.
Erro	Não há nenhum servidor de licenças configurado para o nível de SO necessário com o tipo de licenciamento Per Device Client Access.
Erro	O servidor de licenças configurado não é compatível com o nível RDS Host OS com o tipo de licenciamento Per Device Client Access.
Aviso	Personal Terminal Server não é um tipo de licenciamento RDS válido em uma implantação do Citrix Virtual Apps and Desktops.
Aviso	Remote Desktop for Administration não é um tipo de licenciamento válido em uma implantação do Citrix Virtual Apps and Desktops.
Aviso	Nenhum tipo de licenciamento RDS não está configurado.
Aviso	O controlador de domínio ou o servidor de licenças não pode ser acessado com o tipo de licenciamento RDS Per User Client Access.
Aviso	Com o tipo de licenciamento Per Device Client Access, a licença Client Device não pode ser determinada, pois o servidor de licenças para o nível de SO necessário não está acessível.

> **Nota:**
>
> Esse recurso é aplicável somente para Microsoft RDS CAL (Client Access License).

Resolução de problemas de usuário

June 28, 2023

No Director, usa a exibição **Help Desk** (página **Activity Manager**) para ver as informações sobre o usuário e:

- Verificar detalhes de logon, conexão e aplicativos do usuário.
- Fazer a sombra da máquina do usuário.
- Gravar uma sessão ICA.
- Solucionar problemas com as ações recomendadas na tabela a seguir e, se necessário, encaminhar um problema para o administrador apropriado.

Dicas de solução de problemas

Problema de usuário	Sugestões
O logon leva muito tempo ou falha intermitente ou repetidamente	Diagnosticar problemas de logon do usuário
A inicialização da sessão leva muito tempo ou falha intermitente ou repetidamente	Diagnosticar problemas de início da sessão
O aplicativo está lento ou não responde	Resolver falhas de aplicativos
Falha na conexão	Restaurar conexões de área de trabalho
A sessão está lenta ou não está respondendo	Restaurar sessões
Gravar sessões	Gravar sessões
O vídeo está lento ou com baixa qualidade	Executar relatórios do sistema de canais HDX

> **Nota:**
> Para garantir que a máquina não esteja no modo de manutenção, na exibição User Details, revise os dados no painel Machine Details.

Dicas de pesquisa

Quando você digita o nome do usuário em um campo de pesquisa, o Director procura usuários no Active Directory em todos os sites configurados para dar suporte ao Director.

Quando você digita um nome de máquina multiusuário em um campo de pesquisa, o Director exibe os detalhes da máquina em Machine Details para a máquina especificada.

Quando você digita um nome de ponto de extremidade em um campo de pesquisa, o Director usa as sessões não autenticadas (anônimas) e as sessões autenticadas que estão conectadas a um ponto de extremidade específico, o que permite solucionar problemas em sessões não autenticadas.

Certifique-se de que os nomes dos pontos de extremidade sejam exclusivos para habilitar a solução de problemas de sessões não autenticadas.

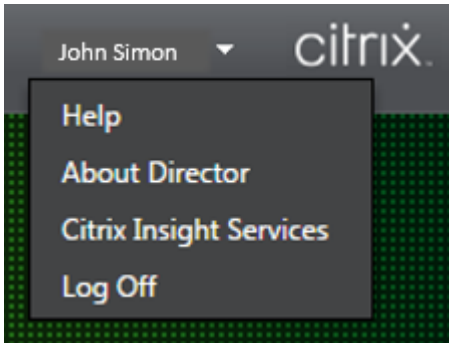
Os resultados da pesquisa também incluem usuários que não estão usando uma máquina no momento ou que não atribuídos a nenhuma máquina.

- As pesquisas não fazem distinção entre maiúsculas e minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome com duas partes (nome de usuário, nome da família e nome de exibição), separadas por um espaço, os resultados incluem correspondências para as duas cadeias de caracteres. Por exemplo, se você digitar jo rob, os resultados podem incluir cadeias de caracteres como "Joao Roberto"ou Roberta, Joana.

Para retornar à página inicial, clique no **logotipo do Director**.

Acessar o Citrix Insight Services

Você pode acessar o Citrix Insight Services (CIS) na lista suspensa **User** no Director para ter acesso a insights de diagnóstico extras. Os dados disponíveis no CIS vêm de fontes incluindo Call Home e Citrix Scout.



Carregar informações de solução de problemas para o Suporte Técnico da Citrix

Execute o Citrix Scout em um único Delivery Controller ou VDA para capturar os principais pontos de dados e rastreamentos do Citrix Diagnostics Facility (CDF) para solucionar problemas de computadores selecionados. O Scout oferece a capacidade de carregar os dados para a plataforma CIS com segurança para ajudar o pessoal do 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 pelo cliente.

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 ver as perguntas frequentes, consulte CTX130147.

Diagnosticar problemas de início da sessão

June 28, 2023

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. Essa se divide na duração em Workspace App Session Startup e em VDA Session Startup na página **User Details** e nas páginas **Machine Details**. Essas duas durações contêm outras fases individuais cujas durações de inicialização também são exibidas. Esses dados ajudam você a entender e solucionar problemas de alta duração na inicialização da sessão. Além disso, a duração de tempo de cada fase envolvida na inicialização da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de mapeamento da unidade for alto, você poderá verificar se todas as unidades válidas estão mapeadas corretamente no GPO ou no script. Esse recurso está disponível no Delivery Controller versão 7 1906 e posterior e em VDAs 1903 e posteriores.

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 de monitoramento da experiência do usuário final da Citrix (EUEM) deve estar em execução no VDA.

Limitações

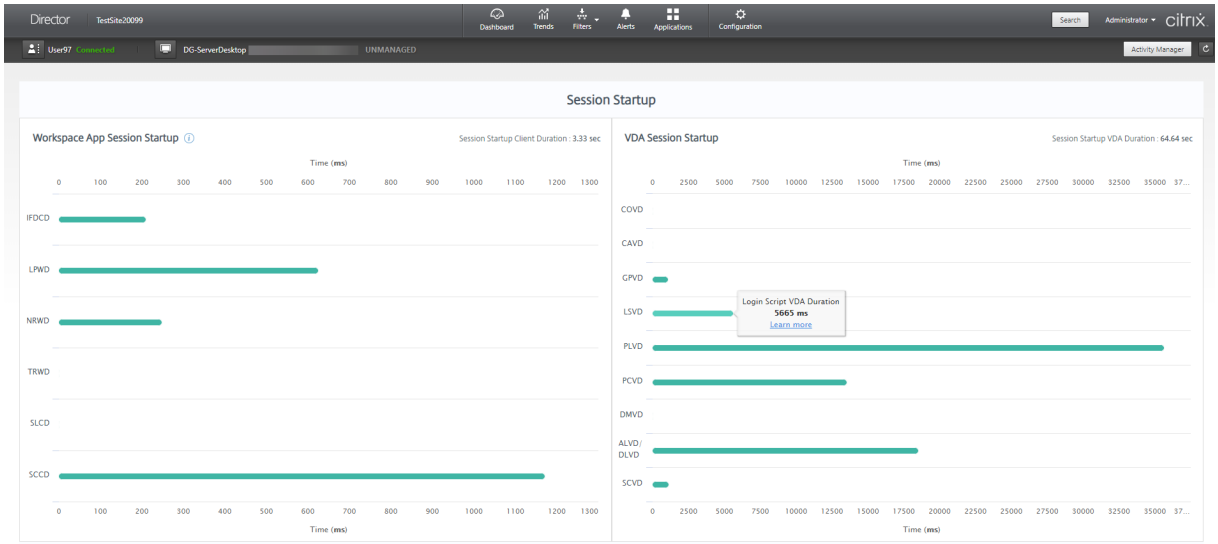
As seguintes limitações se aplicam quando o Director exibe os dados de duração da inicialização da sessão.

- A duração da inicialização da sessão está disponível somente para sessões HDX.
- Para inicializações de sessão a partir do iOS e do SO Android, somente a duração de inicialização do VDA está disponível.
- O IFDCD está disponível apenas quando o aplicativo Workspace é detectado durante a inicialização a partir de um navegador.

- Nas inicializações de sessão no macOS, o IFDCD está disponível apenas para o aplicativo Workspace 1902 ou posterior.
- Nas inicializações de sessão em SO Windows, o IFDCD está disponível para o aplicativo Workspace 1902 e posterior. Para versões anteriores, o IFDCD é exibido apenas para inicializações de aplicativos no navegador com o aplicativo Workspace detectado.

Observações:

- Se você tiver problemas na exibição da duração da inicialização das sessões depois que os pré-requisitos forem atendidos, consulte os logs do VDA e do servidor do Director conforme descrito em CTX130320.
  Para sessões compartilhadas (vários aplicativos iniciados na mesma sessão), as métricas de inicialização do aplicativo Workspace são exibidas para a conexão mais recente ou a inicialização mais recente do aplicativo.
- Algumas métricas na inicialização da sessão do VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.



Fases de inicialização da sessão do aplicativo Workspace

Session Startup Client Duration (SSCD)

Quando esta métrica é alta, ela indica um problema do lado do cliente que está causando tempos de inicialização prolongados. Revise as métricas subsequentes para determinar a provável causa raiz do problema. O SSCD começa o mais próximo possível da hora 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 muitos dos custos de configuração associados

à criação de uma nova conexão com o servidor não são incorridos. No nível abaixo, existem várias métricas detalhadas disponíveis.

ICA File Download Duration (IFDCD)

Este é o tempo necessário para o cliente baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou área de trabalho) no aplicativo Workspace.
2. Uma solicitação do usuário é enviada para o StoreFront por meio do Citrix Gateway (se configurado), que envia a solicitação para o Delivery Controller.
3. O Delivery Controller encontra uma máquina disponível para a solicitação e envia as informações da máquina e outros detalhes para o StoreFront. Além disso, o StoreFront solicita e recebe um ticket único da Secure Ticket Authority.
4. O StoreFront gera um arquivo ICA e o envia ao usuário via Citrix Gateway (se configurado).

O IFDCD representa o tempo necessário para o processo completo (etapas 1 a 4). A duração do IFDCD para de contar quando o cliente recebe o arquivo ICA.

LPWD é o componente StoreFront do processo.

Se o IFDCD for alto (mas o LPWD estiver normal), o processamento da inicialização no lado do servidor foi bem-sucedido, mas houve problemas de comunicação entre o dispositivo cliente e o StoreFront. Isso resulta de problemas de rede entre as duas máquinas. Portanto, você pode solucionar problemas potenciais de rede primeiro.

Launch Page Web Server Duration (LPWD)

Este é o tempo necessário para processar a página de inicialização (launch.aspx) no StoreFront. Se o LPWD estiver alto, pode haver um gargalo de informações no StoreFront.

As possíveis causas incluem:

- Alta carga no StoreFront. Tente identificar a causa da lentidão: verifique os logs e ferramentas de monitoramento dos Serviços de Informações da Internet (IIS), o Gerenciador de Tarefas, Monitor de Desempenho e outros.
- O StoreFront está tendo problemas para se comunicar com outros componentes, como o Delivery Controller. Verifique se a conexão de rede entre o StoreFront e o Delivery Controller está lenta ou se há Delivery Controllers inativos ou sobrecarregados.

Name Resolution Web Server Duration (NRWD)

Este é o tempo gasto pelo Delivery Controller para resolver o nome de um aplicativo/área de trabalho publicado para um endereço IP de uma máquina VDA.

Quando essa métrica está alta, isso indica que o Delivery Controller está demorando muito para resolver o nome de um aplicativo publicado para um endereço IP.

As possíveis causas incluem um problema no cliente, problemas com o Delivery Controller, por exemplo, o Delivery Controller está sobrecarregado, ou um problema com o link de rede entre eles.

Ticket Response Web Server Duration (TRWD)

Esta duração indica o tempo que leva para obter um tíquete (se necessário) do servidor do Secure Ticket Authority (STA) ou do Delivery Controller. Quando essa duração é alta, o servidor STA ou o Delivery Controller estão sobrecarregados.

Session Look-up Client Duration (SLCD)

Esta duração representa o tempo necessário para consultar todas as sessões para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode lidar com a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

Session Creation Client Duration (SCCD)

Esta duração representa o tempo necessário para criar uma sessão, do momento em que o wfica32.exe (ou um arquivo equivalente) é iniciado até o momento em que a conexão é estabelecida.

Fases de inicialização da sessão VDA

Session Startup VDA Duration (SSVD)

Esta duração é a métrica de inicialização de conexão do lado do servidor de alto nível que abrange o tempo que o VDA leva para executar toda a operação de inicialização. Quando essa métrica é alta, isso indica que há um problema com o VDA que aumenta os tempos de inicialização da sessão. Isso inclui o tempo gasto no VDA executando toda a operação de inicialização.

Credentials Obtention VDA Duration (COVD)

O tempo necessário para que o VDA obtenha as credenciais do usuário.

Essa duração pode aumentar artificialmente se um usuário não fornecer as credenciais em tempo hábil. Portanto, ele não está incluído na duração da inicialização do VDA. Esse tempo provavelmente será significativo somente se o login manual estiver sendo usado e a caixa de diálogo de credenciais do lado do servidor for exibida (ou se um aviso legal for exibido antes do início do login).

Credentials Authentication VDA Duration (CAVD)

Este é o tempo gasto pelo VDA para autenticar as credenciais do usuário em relação ao provedor de autenticação. Pode ser Kerberos, Active Directory ou SSPI (Security Support Provider Interface).

Group Policy VDA Duration (GPVD)

Esta duração é o tempo necessário para aplicar objetos de política de grupo durante o logon.

Login Script Execution VDA Duration (LSVD)

Este é o tempo gasto pelo VDA para executar os scripts de login do usuário.

Considere a possibilidade de tornar assíncronos os scripts de login do usuário ou do grupo. Considere a possibilidade de otimizar qualquer script de compatibilidade de aplicativos ou usar variáveis de ambiente.

Profile Load VDA Duration (PLVD)

Este é o tempo gasto pelo VDA para carregar o perfil do usuário.

Se essa duração for alta, verifique a configuração do seu perfil de usuário. O tamanho e a localização do perfil de roaming contribuem para o início lento da sessão. Quando um usuário faz logon em uma sessão em que os perfis de roaming e as pastas iniciais do Terminal Services estão habilitados, o conteúdo do perfil de roaming e o acesso à pasta são mapeados durante o logon. Isso requer recursos extras. Às vezes, isso pode consumir uma quantidade significativa do uso da CPU. Considere a possibilidade de usar as pastas **base do Terminal Services** com pastas pessoais redirecionadas para mitigar o 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 os tempos de logon estiverem lentos, verifique se o software antivírus está bloqueando a ferramenta Citrix Profile Management.

Printer Creation VDA Duration (PCVD)

Este é o tempo necessário para que o VDA mapeie as impressoras cliente do usuário de forma síncrona. Se a configuração estiver definida para que a criação da impressora seja executada de forma assíncrona, o valor não é registrado em PCVD, pois isso não afeta a conclusão da inicialização da sessão.

O tempo excessivo gasto em impressoras de mapeamento geralmente resulta das configurações da política de criação automática da impressora. O número de impressoras adicionadas localmente aos dispositivos cliente dos usuários e sua configuração de impressão podem afetar diretamente os tempos de início da sessão. Quando uma sessão é iniciada, o Citrix Virtual Apps and Desktops precisa criar todas as impressoras mapeadas localmente no dispositivo cliente. Considere reconfigurar suas políticas de impressão para reduzir o número de impressoras criadas, especificamente quando os usuários tiverem muitas impressoras locais. Para isso, edite a política de criação automática da impressora no Delivery Controller e no Citrix Virtual Apps and Desktops.

Drive Mapping VDA Duration (DMVD)

Este é o tempo gasto pelo VDA para mapear as unidades, dispositivos e portas do cliente do usuário.

Certifique-se de que suas políticas básicas incluam configurações para desativar canais virtuais não utilizados. Por exemplo, mapeamento de porta COM ou áudio, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

Application/Desktop Launch VDA Duration (ALVD/DLVD)

Esta fase é uma combinação da duração de Userinit e Shell. Quando um usuário faz logon em uma máquina Windows, o winlogon executa o userinit.exe. O usernit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe. Userinit representa a duração entre o início do userinit.exe e o início da interface do usuário da área de trabalho ou aplicativo virtual. A duração do Shell é o tempo entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

Session Creation VDA Duration (SCVD)

Este tempo inclui qualquer outro atraso no tempo de criação da sessão no VDA.

Diagnosticar problemas de logon do usuário

June 28, 2023

Use os dados em Logon Duration para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a uma área de trabalho ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o protocolo RDP ou reconectar-se de sessões desconectadas. Especificamente, a duração do logon não é medida quando um usuário se conecta inicialmente usando um protocolo não HDX e se reconecta usando HDX.

Na exibição User Details, a duração é exibida como um valor numérico. Abaixo desse número, é exibida a hora em que o logon ocorreu e um gráfico das fases do processo de logon.

À medida que os usuários fazem logon no Citrix Virtual Apps and Desktops, o Monitor Service acompanha as fases do processo de logon. As fases começam do momento em que o usuário se conecta do aplicativo Citrix Workspace ao 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 estabelecendo a conexão e obtendo uma área de trabalho do Delivery Controller com o tempo gasto para autenticar e fazer logon em uma área de trabalho virtual. As informações de duração são apresentadas em segundos (ou frações de segundo).

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que sejam exibidos os dados de duração de logon e os detalhes:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Citrix Profile Management Service esteja em execução.
3. Para os sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Do not process the legacy run list**.
4. O acompanhamento do processo de auditoria deve estar ativado para o detalhamento em Interactive Session.
5. Para o detalhamento do GPO, aumente o tamanho dos logs operacionais da política de grupo.

> **Observações:**
>
> - A duração do logon é suportada somente no shell padrão do Windows (explorer.exe) e não em shells personalizados.
> - A duração do logon no Remote PC Access 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 Remote PC Access. Para obter mais informações, consulte a Etapa 4 em Considerações e sequência de configuração do Remote PC Access.

Etapas para solucionar problemas de logon do usuário

1. Na exibição **User Details**, solucione os problemas de estado do logon usando o painel Logon Duration.
    - Se o usuário estiver fazendo logon, a exibição refletirá o processo de logon.
    - Se o usuário estiver conectado, o painel Logon Duration exibirá o tempo que foi necessário para o usuário fazer logon na sessão atual.
2. Examine as fases do processo de logon.

Fases do processo de logon

Brokering

Tempo que foi necessário para decidir qual área de trabalho atribuir ao usuário.

VM Start

Se a sessão exigir um início da máquina, VM Start é o tempo que foi necessário para iniciar a máquina virtual.

HDX Connection

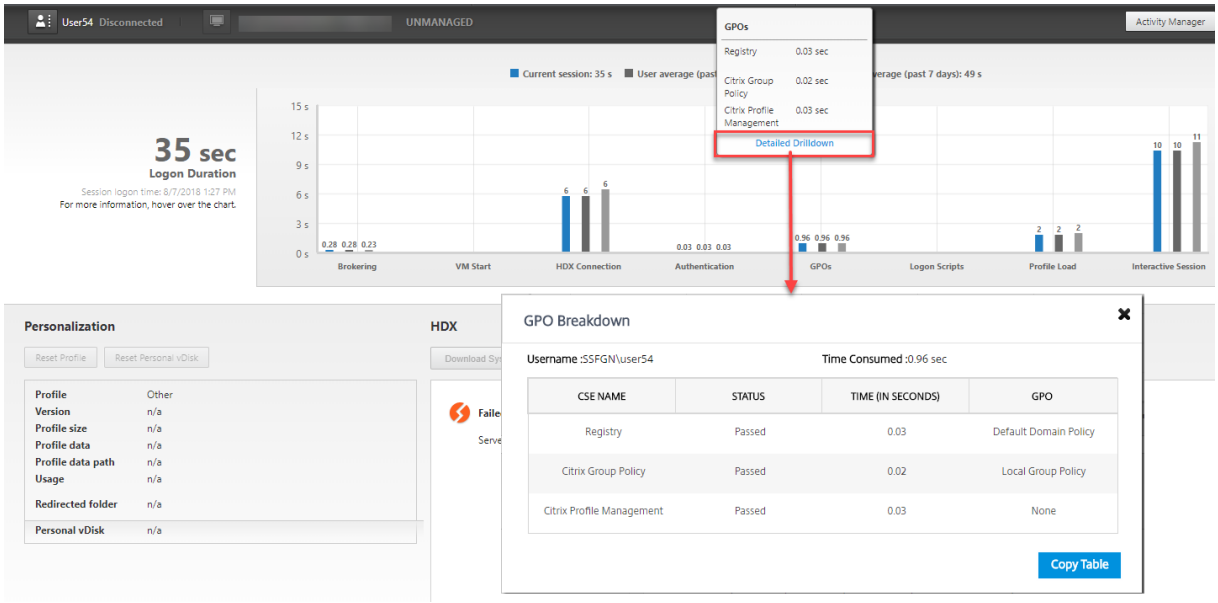
Tempo que foi necessário para concluir as etapas necessárias na configuração da conexão HDX do cliente com a máquina virtual.

Autenticação

Tempo que foi necessário para concluir a autenticação com a sessão remota.

GPOs

Se as configurações da política e grupo estiverem ativadas nas máquinas virtuais, esse é o tempo que foi necessário para aplicar objetos da política de grupo durante o logon. O detalhamento do tempo que foi necessário para aplicar cada política de acordo com os CSEs (extensão do lado do cliente) está disponível como dica de ferramenta quando você passa o mouse sobre a barra de GPO.



Clique em **Detailed Drilldown** para ver uma tabela com o status da política e o nome do objeto de política de grupo correspondente. As durações de tempo no detalhamento representam apenas o tempo de processamento do CSE e não somam o tempo total do GPO. Você pode copiar a tabela de detalhamento para a solução de problemas ou para usar em relatórios. O tempo de GPO para as políticas é recuperado dos logs no visualizador de eventos. Os logs podem ser substituídos dependendo da memória alocada para os logs operacionais (o tamanho padrão é de 4 MB). Para obter mais informações sobre como aumentar o tamanho de log para os logs operacionais, consulte o artigo do Microsoft TechNet Configuring the Event Logs.

Logon Scripts

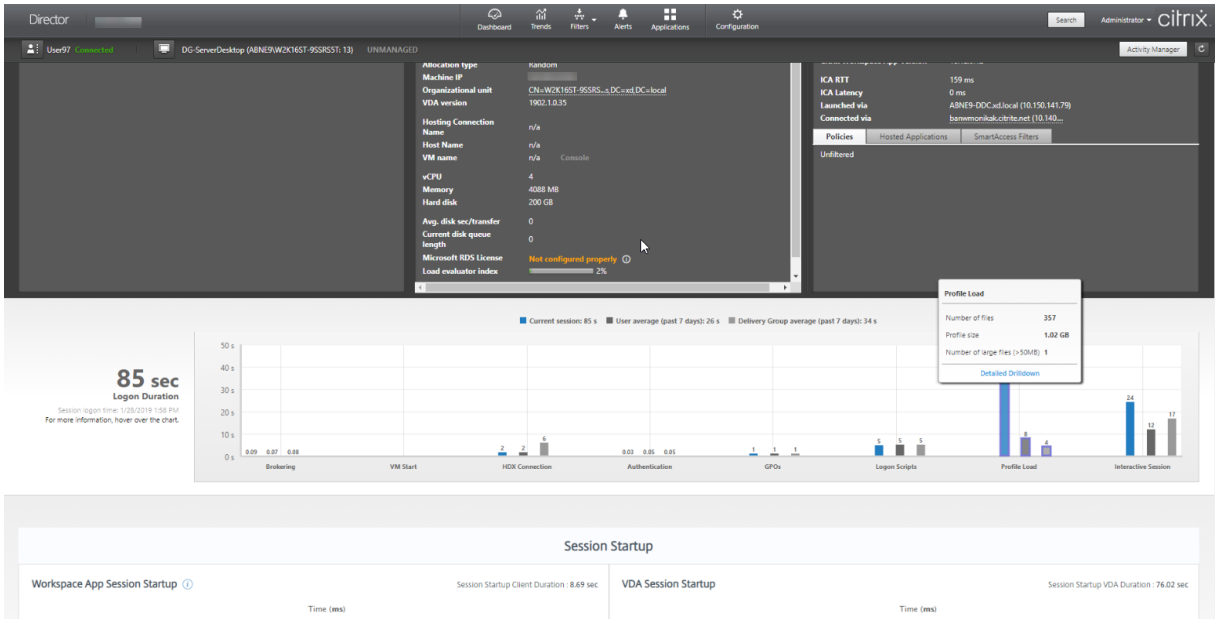
Se os scripts de logon estiverem configurados para a sessão, esse é o tempo que foi necessário para que os scripts de logon fossem executados.

Profile Load

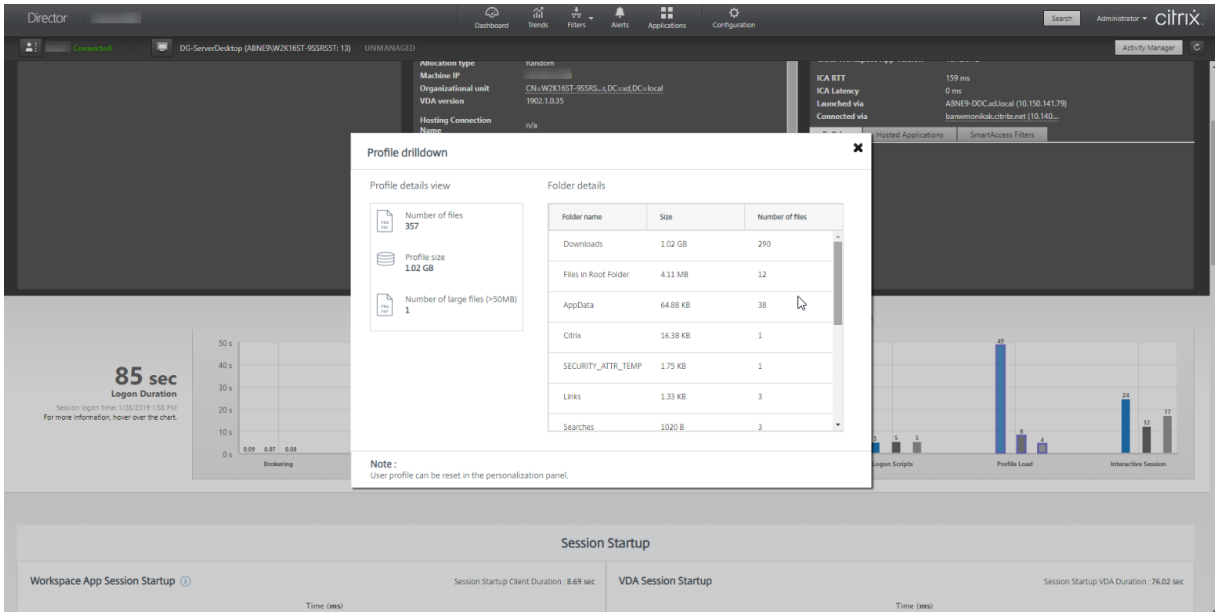
Se as configurações de perfil estiverem definidas para o usuário ou a máquina virtual, esse é o tempo que foi necessário para o perfil carregar.

Se o Citrix Profile Management estiver configurado, a barra de carregamento do perfil inclui o tempo gasto pelo Citrix Profile Management para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management é configurado, a barra de carregamento de perfil exibe uma duração maior. Esse aumento é causado por esse aprimoramento e não reflete degradação do desempenho. Esse aprimoramento está disponível em VDAs 1903 ou posteriores.

Passe o mouse sobre a barra Profile Load para ver uma dica de ferramenta mostrando os detalhes do perfil do usuário da sessão atual.



Clique em **Detailed Drilldown** para se aprofundar mais em cada pasta individual na pasta raiz do perfil (por exemplo, C:/Users/nome_de_usuário), ver seu tamanho e o número de arquivos (incluindo arquivos dentro das pastas aninhadas).



O detalhamento de perfil está disponível no Delivery Controller versão 7 1811 ou posterior e em VDAs 1811 ou posteriores. Usando as informações de detalhamento do perfil, você pode resolver problemas que envolvem um tempo longo de carregamento de perfil. Você pode:

- Redefinir o perfil do usuário

- Otimizar o perfil removendo arquivos grandes desnecessários
- Reduzir o número de arquivos para reduzir a carga da rede
- Usar streaming de perfil

Por padrão, todas as pastas na raiz do perfil são exibidas no detalhamento. Para ocultar a visibilidade das pastas, edite o seguinte valor de registro na máquina VDA:

> **Aviso:**
>
> Adicionar o registro incorretamente pode causar sérios problemas que podem exigir que você reinstale seu sistema operacional. A Citrix não garante que problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Tenha o cuidado de fazer backup do registro antes de editá-lo.

1. No VDA, adicione um novo valor de registro **ProfileFoldersNameHidden** HKEY_LOCAL_MACHINE\Software\C
2. Defina o valor como 1. Esse valor deve ser um valor DWORD (32 bits). A visibilidade do nome das pastas agora está desativada.
3. Para deixar o nome das pastas visível novamente, defina o valor como 0.

> **Nota:**
> Você pode usar os comandos GPO ou PowerShell para aplicar a alteração de valor do registro em várias máquinas. Para obter mais informações sobre como usar o objeto de política de grupo para implantar alterações no registro, consulte o blog.

Informações adicionais

- O detalhamento de perfil não considera as pastas redirecionadas.
- Os arquivos NTUser.dat na pasta raiz podem não estar visíveis para os usuários finais. No entanto, eles são incluídos no detalhamento do perfil e exibidos na lista de arquivos em **Root Folder**.
- Determinados arquivos ocultos na pasta AppData não estão incluídos no Profile Drilldown.
- O número de arquivos e dados do tamanho do perfil talvez não correspondam aos dados no painel Personalization devido a certas limitações do Windows.

Interactive Session

Este é o tempo que foi necessário para “entregar”o controle do teclado e do mouse para o usuário após o carregamento do perfil do usuário. Normalmente, esta é a duração mais longa de todas as fases do processo de logon e é calculada como **duração da sessão interativa = carimbo de data/hora de Desktop Ready Event (EventId 1000 no VDA) - carimbo de data/hora de User Profile Loaded Event (EventId 2 no VDA)**. Interactive Session tem três subfases: Pre-userinit, Userinit e Shell. Passe o mouse sobre Interactive Session para ver uma dica de ferramenta mostrando o seguinte:

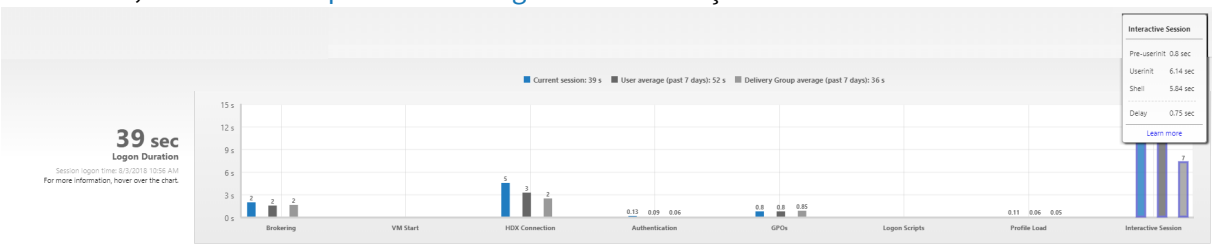
- subfases
- tempo que foi necessário para cada subfase
- tempo total de atraso acumulado entre essas subfases

> **Nota:**
>
> Esse recurso está disponível nos VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores a 7.18 e depois atualizou para a versão 7.18 ou posterior, é exibida a mensagem "Drilldown unavailable due to server error". No entanto, se você iniciou as sessões após a atualização, nenhuma mensagem de erro é exibida.

Para exibir a duração do tempo de cada subfase, ative o acompanhamento do processo Audit na máquina virtual (VDA). Quando o acompanhamento do processo de auditoria está desativado (padrão), a duração de Pre-userinit e a duração combinada de Userinit e Shell são exibidas. Você pode ativar o acompanhamento do processo de auditoria através de um objeto de política de grupo (GPO) da seguinte forma:

1. Crie um objeto de política de grupo e edite-o usando o editor de GPO.
2. Vá para **Configuração do computador > Configurações do Windows > Configurações de segurança > Políticas locais > Política de auditoria**.
3. No painel direito, clique duas vezes em **Auditoria de acompanhamento de processos**.
4. Selecione **Sucesso** e clique em OK.
5. Aplique este objeto de política de grupo aos VDAs ou grupo necessários.

Para obter mais informações sobre a auditoria de acompanhamento de processos e ativá-la ou desativá-la, consulte Audit process tracking na documentação da Microsoft.



Painel Logon Duration na exibição User Details.

- **Interactive Session –Pre-userinit:** o segmento de Interactive Session que se sobrepõe a objetos de política de grupo e scripts. Essa subfase pode ser reduzida otimizando os GPOs e os scripts.
- **Interactive Session –Userinit:** quando um usuário faz logon em uma máquina Windows, o Winlogon executa o userinit.exe. O userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface de usuário do Windows. Essa subfase do Interactive Session representa a duração entre o início do userinit.exe e o início da interface do usuário da área de trabalho ou aplicativo virtual.

- **Interactive Session –Shell:** na fase anterior, o Userinit inicia a inicialização da interface do usuário do Windows. A subfase Shell captura a duração entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.
- **Delay:** este é o atraso de tempo cumulativo entre as subfases **Pre-userinit e Userinit** e as subfases **Userinit e Shell**.

O tempo total de logon não é a soma exata dessas fases. Por exemplo, algumas fases ocorrem em paralelo e, em algumas fases, ocorre mais processamento que pode resultar em uma duração de logon mais longa do que a somatória.
O tempo total de logon não inclui o tempo ocioso do ICA, que é o tempo entre o download do arquivo ICA e o início do arquivo ICA para um aplicativo.
Para habilitar a abertura automática do arquivo ICA no momento da inicialização do aplicativo, configure seu navegador para iniciar o arquivo ICA automaticamente após o download de um arquivo ICA. Para obter mais informações, consulte CTX804493.

> **Nota:**
> O gráfico Logon Duration mostra as fases de logon em segundos. Os valores de duração abaixo de um segundo são exibidos como valores de subsegundo. Os valores acima de um segundo são arredondados para o 0,5 segundo mais próximo. O gráfico foi projetado para mostrar o maior valor do eixo y em 200 segundos. Qualquer valor maior que 200 segundos é mostrado com o valor real exibido acima da barra.

Dicas de solução de problemas

Para identificar valores incomuns ou inesperados no gráfico, compare a quantidade de tempo gasto em cada fase da sessão atual com a duração média do usuário nos últimos sete dias e a duração média de todos os usuários no grupo de entrega nos últimos sete dias.

Encaminhe a outros colegas conforme necessário. Por exemplo, se a inicialização da máquina virtual estiver lenta, o problema pode estar no Hypervisor, portanto, você pode encaminhá-lo para o administrador do Hypervisor. Ou, se o tempo de intermediação do agente for lento, você pode encaminhar o problema para o administrador do site para verificar o balanceamento de carga no Delivery Controller.

Examine diferenças incomuns, incluindo:

- Barras de logon ausentes (atuais)
- Grande discrepância entre a duração atual e a duração média do usuário. As causas incluem:
  - Um novo aplicativo foi instalado.
  - Ocorreu uma atualização do sistema operacional.
  - Foram feitas mudanças de configuração.

  - O tamanho do perfil do usuário é alto. Nesse caso, a carga do perfil em Profile Load está alta.

- Grandes discrepâncias entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

Se necessário, clique em **Restart** para observar o processo de logon do usuário para solucionar os problemas, por exemplo, em VM Start ou Brokering.

Sombrear usuários

June 28, 2023

No Director, use o recurso de sombreamento de usuário para exibir ou trabalhar diretamente na sessão ou na máquina virtual de um usuário. Você pode sombrear VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja sombrear. Para confirmar, verifique o nome da máquina listado na barra de título do usuário.

O Director inicia o sombreamento em uma nova guia, atualiza as configurações do navegador para permitir pop-ups do URL do Director.

Acesse o recurso de sombreamento na exibição **User Details**. Selecione a sessão do usuário e clique em **Shadow** na exibição do Activity Manager ou no painel Session Details.

Sombreamento de Linux VDAs

O sombreamento, ou shadowing, está disponível para Linux VDAs versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu versão 16.04

> **Nota:**
>
> - O VDA deve estar acessível a partir da IU do Director para que o sombreamento funcione. Portanto, o sombreamento só é possível para Linux VDAs na mesma intranet que o cliente do Director.
> - O Director usa o FQDN para se conectar ao Linux VDA de destino. Certifique-se de que o cliente do Director pode resolver o FQDN do Linux VDA.
> - O VDA deve ter os pacotes python websockify e x11vnc instalados.
> - A conexão do noVNC com o VDA usa o protocolo WebSocket. Por padrão, o protocolo WebSocket **ws://** é usado. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro **wss://**. Instale certificados SSL em cada cliente do Director e Linux VDA.

Siga as instruções em Session Shadowing para configurar seu VDA para sombreamento.

1. Depois que você clicar em **Shadow**, a conexão de sombreamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
3. O administrador só pode visualizar a sessão sombreada.

Sombreamento de Windows VDAs

As sessões do Windows VDA são sombreadas usando a Assistência Remota do Windows. Ative o recurso **User Windows Remote Assistance** durante a instalação do VDA. Para obter mais informações, consulte Ativar ou desativar recursos.

1. Depois de clicar em **Shadow**, a conexão de sombreamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo de incidente .msrc.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ainda não estiver selecionado por padrão. Um prompt de confirmação é exibido no dispositivo do usuário.
3. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
4. Para obter mais controle, peça ao usuário que compartilhe o controle do teclado e do mouse.

Agilizar os navegadores Microsoft Internet Explorer para o sombreamento

Configure o navegador Microsoft Internet Explorer para abrir automaticamente o arquivo Microsoft Remote Assistance (.msra) baixado com o cliente de Assistência Remota.

Para isso, você deve ativar a configuração de aviso automático para o download de arquivos no editor de política de grupo:

Configuração do computador > Modelos Administrativos > Componentes do Windows > Internet Explorer > Painel de Controle da Internet > Página de Segurança > Zona da Internet > Aviso automático para downloads de arquivo.

Por padrão, essa opção está ativada para sites na zona da intranet local. Se o site do Director não estiver na zona da intranet local, considere adicionar manualmente o site a essa zona.

Enviar mensagens para usuários

June 28, 2023

No Director, envie uma mensagem para um usuário conectado a uma ou mais máquinas. Use esse recurso para enviar avisos imediatos sobre ações administrativas, como manutenção iminente da área de trabalho, logoffs e reinicializações de máquinas e redefinições de perfis.

1. Na exibição Activity Manager, selecione o usuário e clique em Details.
2. Na exibição User Details, localize o painel Session Details e clique em Send Message.
3. Digite as informações da mensagem nos campos Subject e Message e clique em Send.

Se a mensagem for enviada com sucesso, uma mensagem de confirmação é exibida no Director. A mensagem aparece na máquina do usuário.

Se a mensagem não for enviada com sucesso, uma mensagem de erro aparece no Director. Solucione o problema de acordo com a mensagem de erro. Quando terminar, digite o assunto e o texto da mensagem novamente e clique em **Try** novamente.

Resolver falhas de aplicativos

June 28, 2023

Na exibição **Activity Manager**, clique na guia Applications. Você pode visualizar todos os aplicativos em todas as máquinas às quais o usuário tem acesso, incluindo aplicativos locais e hospedados para a máquina conectada atualmente e o status de cada um.

> **Nota:**
>
> Se a guia Applications estiver acinzentada, 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 multissessão e máquinas com SO de sessão única, os aplicativos são listados para cada sessão desconectada. Se o usuário não estiver conectado, nenhum aplicativo será exibido.

Ação	Descrição
Encerrar o aplicativo que não está respondendo	Escolha o aplicativo que não está respondendo e clique em End Application. Depois que o aplicativo for encerrado, peça ao usuário para iniciá-lo novamente.

Ação	Descrição
Encerrar processos que não estão respondendo	Se você tiver a permissão necessária, clique na guia Processes. Selecione um processo relacionado ao aplicativo ou usando uma grande quantidade de recursos da CPU ou memória e clique em End Process. No entanto, se você não tiver a permissão necessária para encerrar o processo, a tentativa de encerrar um processo falhará.
Reiniciar a máquina do usuário	Apenas em máquinas com SO de sessão única, para a sessão selecionada, clique em Restart. Como alternativa, na exibição Machine Details, use os controles de energia para reiniciar ou desligar a máquina. Instrua o usuário a fazer logon novamente para que você possa verificar novamente o aplicativo. Para máquinas com SO multissessão, a opção de reinicialização não está disponível. Em vez disso, faça logoff do usuário e deixe que o usuário faça logon novamente.
Colocar a máquina no modo de manutenção	Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina no modo de manutenção. Na exibição Machine Details, clique em Details e ative a opção de modo de manutenção. Encaminhe para o administrador apropriado.

Restaurar conexões de área de trabalho

June 28, 2023

No Director, verifique o status da conexão do usuário da máquina atual na barra de título do usuário.

Se a conexão da área de trabalho falhar, o erro que causou a falha é exibido e pode ajudá-lo a decidir como solucionar o problema.

Ação	Descrição
Assegurar que a máquina não está no modo de manutenção	Na página User Details, verifique se o modo de manutenção está desativado.
Reiniciar a máquina do usuário	Selecione a máquina e clique em **Restart**. Use essa opção se a máquina do usuário não responder ou não conseguir se conectar. Por exemplo, quando a máquina está usando uma quantidade excepcionalmente alta de recursos da CPU, o que pode tornar a CPU inutilizável.

Restaurar sessões

June 28, 2023

Se uma sessão for desconectada, ela permanece ativa e seus aplicativos continuam em execução, mas o dispositivo do usuário não se comunica mais com o servidor.

Na exibição User Details, solucione problemas de falhas de sessão no painel **Session Details**. Você pode exibir os detalhes da sessão atual, indicados pelo ID da sessão.

Ação	Descrição
Encerrar aplicativos e processos que não estão respondendo	Clique na guia **Applications**. Selecione o aplicativo que não está respondendo e clique em **End Application**. Da mesma forma, selecione um processo correspondente que não esteja respondendo e clique em **End Process**. Além disso, encerre os processos que estão consumindo uma quantidade excepcionalmente alta de memória ou recursos de CPU, o que pode tornar a CPU inutilizável.
Desconectar a sessão do Windows	Clique em **Session Control** e selecione **Disconnect**. Essa opção está disponível somente para máquinas com SO multissessão intermediado pelo agente. Para sessões não intermediadas, a opção está desativada.
Fazer logoff da sessão do usuário	Clique em **Session Control** e selecione **Log Off**.

Para testar a sessão, o usuário pode tentar fazer logon novamente. Você também pode sombrear o usuário para monitorar a sessão mais de perto.

Executar relatórios do sistema de canais HDX

June 28, 2023

Na exibição **User Details**, verifique o status dos canais HDX na máquina do usuário no painel **HDX**. Esse painel só estará disponível se a máquina do usuário estiver conectada usando HDX.

Se aparecer uma mensagem indicando que as informações não estão disponíveis no momento, aguarde um minuto até que a página seja recarregada ou selecione o botão **Atualizar**. Os dados HDX demoram um pouco mais para serem atualizados do que outros dados.

Clique em um ícone de erro ou aviso para obter mais informações.

> Dica:
>
> Você pode exibir informações sobre outros canais na mesma caixa de diálogo clicando nas setas esquerda e direita no canto esquerdo da barra de título.

Os relatórios do sistema de canal HDX são usados principalmente pelo suporte Citrix para solucionar problemas.

1. No painel HDX, clique em Download System Report.
2. Você pode exibir ou salvar o arquivo de relatório .xml.
    - Para visualizar o arquivo .xml, clique em Open. O arquivo .xml aparece na mesma janela que o aplicativo Director.
    - Para salvar o arquivo .xml, clique em Save. A janela Save As é exibida, solicitando um local na máquina do Director para baixar o arquivo.

Redefinir um perfil de usuário

June 28, 2023

> **CUIDADO:**
>
> Quando um perfil é redefinido, as pastas e arquivos do usuário são salvos e copiados para o

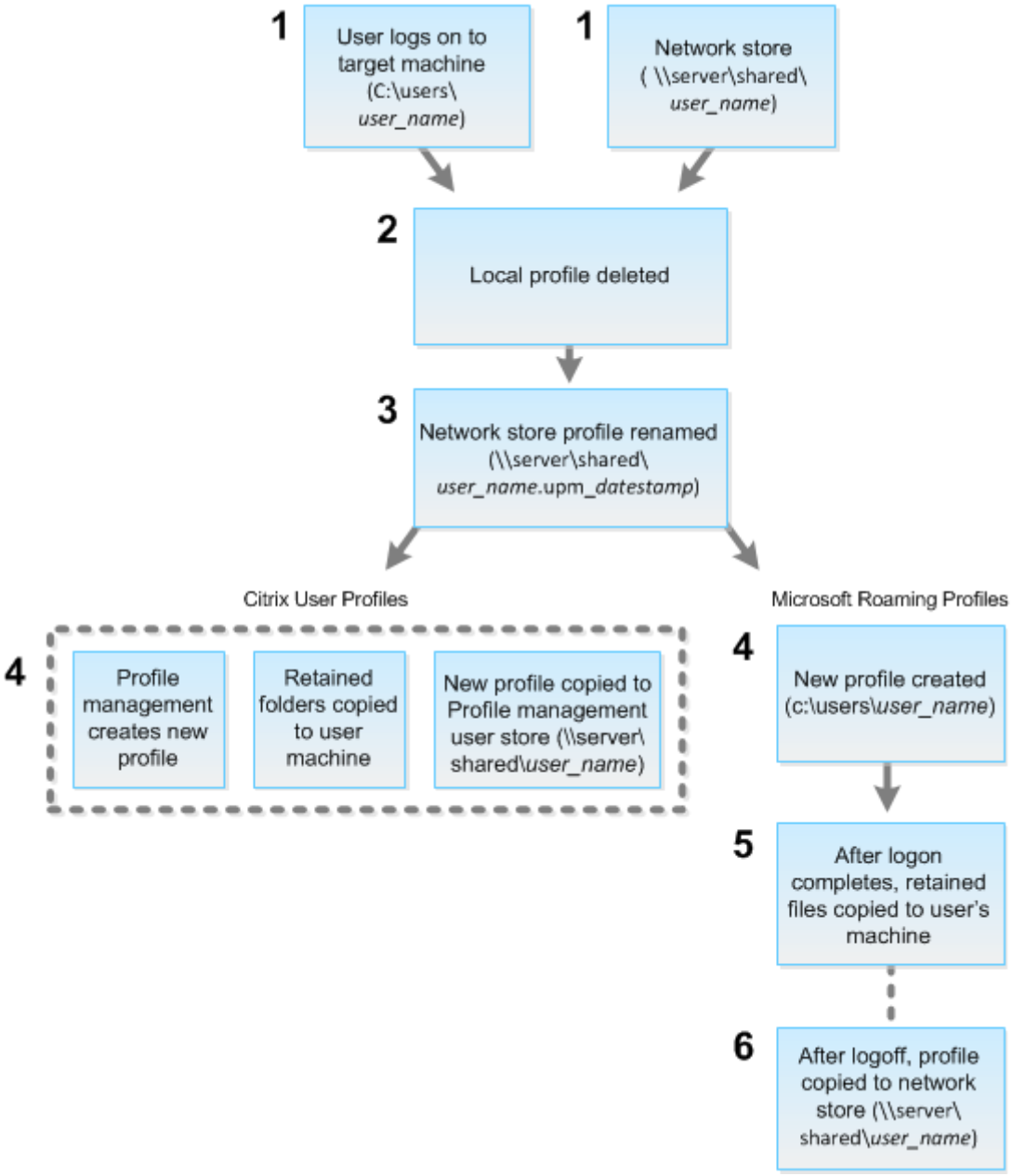
> novo perfil. No entanto, a maioria dos dados do perfil do usuário estará faltando (por exemplo, o registro é redefinido e as configurações do aplicativo podem ser excluídas).

A partir do Profile Management 2106, a função de redefinição está disponível para a solução de perfil de usuário baseada em contêiner do perfil do Citrix Management.

Como os perfis de redefinição são processados

Qualquer perfil de usuário da Citrix ou perfil de roaming da Microsoft pode ser redefinido. Depois que o usuário fizer logoff e você selecionar o comando reset (no Director ou usando o PowerShell SDK), o Director primeiro identifica o perfil do usuário em uso e emite um comando de redefinição apropriado. O Director recebe as informações através do Profile Management, incluindo informações sobre o tamanho do perfil, o tipo e os horários de logon.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.



O comando reset emitido pelo Director especifica o tipo de perfil. Depois, o serviço Profile Management tenta redefinir um perfil desse tipo e procura o compartilhamento de rede apropriado (armazenamento do usuário). Se o usuário for processado pelo Profile Management, mas receber um comando de perfil de roaming, ele será rejeitado (ou vice-versa).

1. Se um perfil local estiver presente, ele será excluído.
2. O perfil de rede é renomeado.
3. A próxima ação depende se o perfil que está sendo redefinido é um perfil de usuário da Citrix ou um perfil de roaming da Microsoft.

Para perfis de usuário da 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 de roaming for usado para a redefinição, todas as configurações do registro no perfil de roaming serão preservadas no perfil redefinido. Você pode configurar o Profile Management de modo que um perfil de modelo substitua o perfil de roaming, se necessário.

Para perfis de roaming da Microsoft, o Windows cria um 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 (VDA de área de trabalho), faça o seguinte:

1. No **Director**, procure o usuário cujo perfil você deseja redefinir e selecione a sessão desse usuário.
2. Clique em **Reset Profile**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente.
   As pastas e os arquivos que foram salvos do perfil do usuário são copiados para o novo perfil.

Se você estiver usando o Citrix Virtual Desktops (VDA de servidor), deverá estar conectado para executar a redefinição do perfil. O usuário precisa fazer logoff e logon novamente para concluir a redefinição do perfil.

> **Importante:**
>
> Se o usuário tiver perfis em várias plataformas (como Windows 8 e Windows 7), instrua o usuário a fazer logon novamente na mesma área de trabalho ou aplicativo que o usuário informou como um problema. Essa ação de logon garante que o perfil correto seja redefinido. Se o perfil for um perfil de usuário da Citrix, o perfil já estará redefinido no momento em que a área de trabalho do usuário for exibida. Se o perfil for um perfil de roaming da Microsoft, a restauração da pasta poderá continuar em andamento por um breve período. O usuário deve permanecer conectado até que a restauração esteja concluída.

Se o perfil não for redefinido com êxito (por exemplo, o usuário não puder efetuar logon novamente na máquina ou alguns dos arquivos estiverem ausentes), você deverá restaurar manualmente o perfil original.

Observe o seguinte:

- Se o armazenamento do 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 inteira, 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 houver um.
3. Localize a pasta arquivada no compartilhamento de rede que contém a data e a hora anexadas ao nome da pasta, a pasta com a extensão .upm_datahora.
4. Exclua o nome de perfil atual. Ou seja, aquele sem a extensão .upm_datahora.
5. Renomeie a pasta arquivada usando o nome de perfil original. Ou seja, remova a extensão de data e hora. Você retornou o perfil ao estado original de pré-redefinição.

Para redefinir um perfil usando o PowerShell SDK

Você pode redefinir um perfil usando o Broker PowerShell SDK.

New-BrokerMachineCommand

Cria um comando enfileirado para entrega a um usuário, sessão ou máquina específica. Para obter mais informações sobre esse 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 New-BrokerMachineCommand do PowerShell. Por exemplo:

```
New-BrokerMachineCommand -Category UserProfileManager -CommandName
 "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -
SendTrigger logon -user domain1\user1
```

> **Importante:**
>
> `CommandData $byteArray` deve estar no seguinte formato: `<SID>[,<backup path>]`. Se você não fornecer o caminho do backup, o Profile Management gera uma pasta de backup com a data e hora atuais no nome.

Redefinir um perfil de roaming do Windows

- Suponha que você queira redefinir o perfil de roaming para user1. Use o comando New-BrokerMachineCommand do PowerShell. Por exemplo:

```
New-BrokerMachineCommand -Category UserProfileManager -CommandName
 "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray
 -SendTrigger logon -user domain1\user1
```

Gravar sessões

June 28, 2023

Você pode gravar sessões ICA usando os controles Session Recording na tela **User Details** e **Machine Details** no Director. Esse recurso está disponível para clientes em sites **Premium** .

Para configurar o Session Recording no Director usando a ferramenta DirectorConfig, consulte a seção **Configure Director to use the Session Recording Server** em Configure session recording policies. Os controles do Session Recording estarão disponíveis no Director somente se o usuário conectado tiver permissão para modificar as políticas de Session Recording. Essa permissão pode ser definida no console Session Recording Authorization, conforme descrito em Authorize users.

> **Nota:**
> As alterações feitas nas configurações do Session Recording através do Director ou do console Session Recording Policy entram em vigor a partir da sessão ICA subsequente.

Controles Session Recording no Director

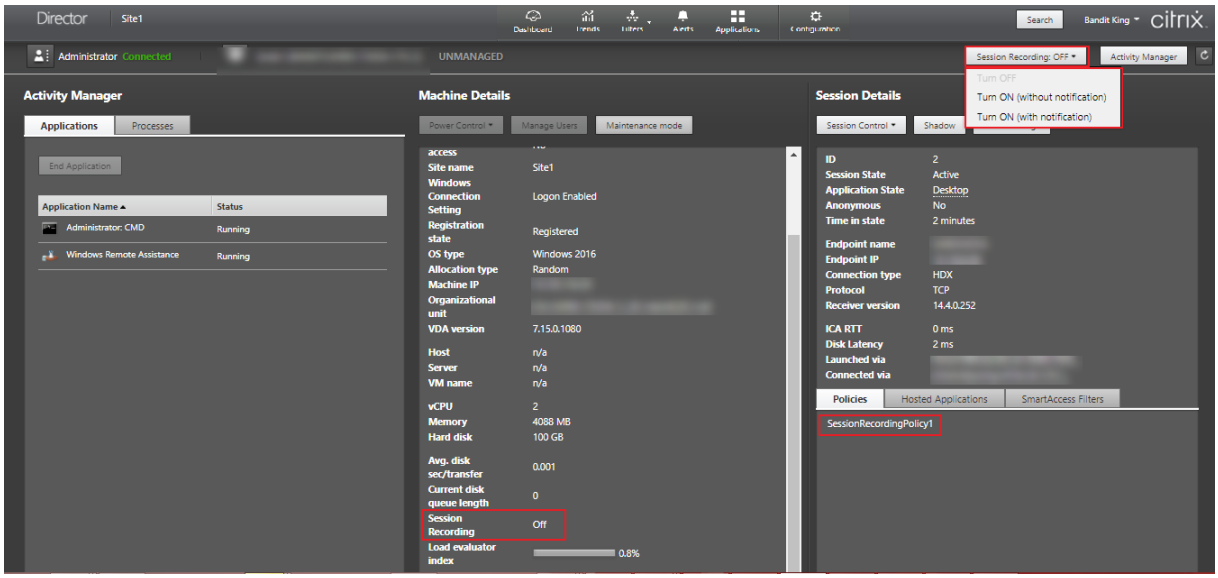
Você pode ativar o Session Recording para um usuário específico no **Activity Manager** ou na tela **User Details**. Sessões subsequentes são gravadas para o usuário específico em todos os servidores

suportados.

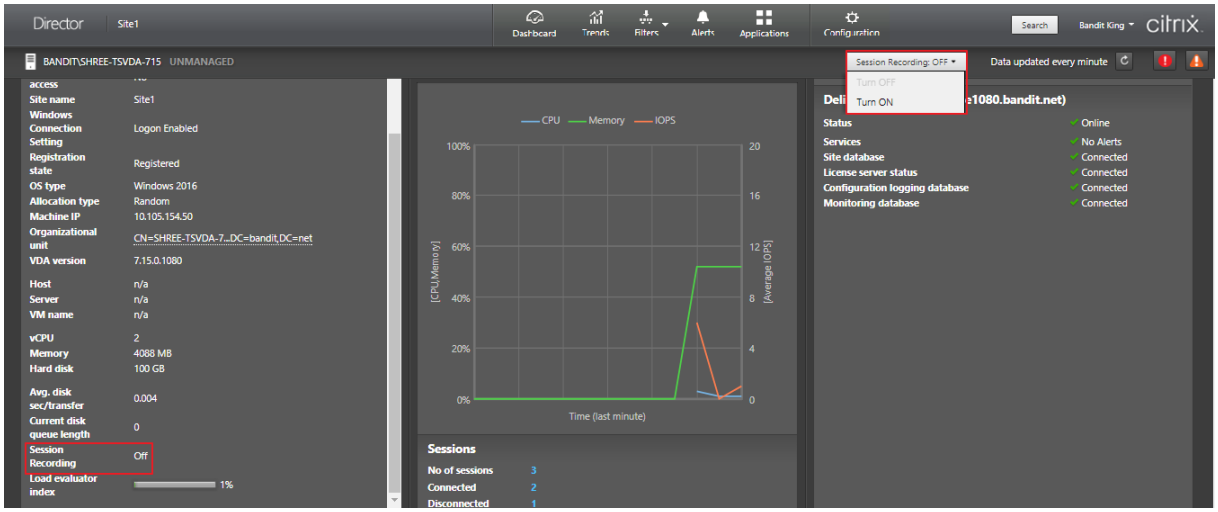
Você pode:

- Turn ON (with notification) –o usuário é notificado sobre a sessão que está sendo gravada ao fazer login na sessão ICA.
- Turn ON (without notification) –a sessão é gravada silenciosamente sem notificar o usuário.
- Turn OFF –desativa a gravação de sessões para o usuário.

O painel **Policies** exibe o nome da política Session Recording ativa.



Você pode ativar Session Recording para uma máquina específica na página Machine Details. As sessões subsequentes na máquina são gravadas. O painel **Machine Details** exibe o status da política Session Recording para a máquina.



Matriz de compatibilidade de recursos

June 28, 2023

O Citrix Director 7 2203 é compatível com:

- Citrix Virtual Apps and Desktops 7 2112 e posterior
- Citrix Virtual Apps and Desktops 7 1912 LTSR

Em cada site, embora você possa usar o Director com versões anteriores do Delivery Controller, nem todos os recursos da versão mais recente do Director estarão disponíveis. A Citrix recomenda que a versão do Director, Delivery Controller e VDAs seja a mesma.

> **Nota:**
>
> 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, é realizada a verificação de versão nos sites configurados. Se um site estiver executando uma versão do Controller anterior à do Director, o console Director exibe uma mensagem recomendando a atualização do site. Além disso, enquanto a versão do site for mais antiga do que a versão do Director, uma nota permanecerá no Dashboard do Director indicando a incompatibilidade.

> **Nota:**
>
> Versões anteriores do Citrix Director não exibem políticas aplicadas a sessões de usuário em execução em versões recentes do VDA. O Citrix Director 1912 e versões anteriores não exibem políticas aplicadas a sessões de usuário em execução no VDA versões 2003 e posteriores. Use o Citrix Director versões 2003 e posteriores para ver essas políticas.

Abaixo estão listados os recursos específicos do Director com a versão mínima do Delivery Controller (DC), VDA e outros componentes dependentes necessários juntamente com a edição da licença.

Versão do Director	Recurso	Dependências – versão mínima necessária	Edição
2303	Alerta de máquinas com falha	DC 7 2303	Premium
2203	Suporte a TLS 1.3	-	Todos

Versão do Director	Recurso	Dependências – versão mínima necessária	Edição
2212	Utilização de GPU em tempo real disponível para GPUs AMD	DC 7.14 e VDA 7.14 executando Windows de 64 bits e HDX 3D Pro habilitado	Todos
2212	Programação avançada de investigação	DC 7 1906 e Citrix Probe Agent 2209	Premium
1909	Configurar sites locais com o Citrix Analytics for Performance	DC 7 1906 e VDA 1906	Todos
1906	Reconexão automática de sessão	DC 7 1906 e VDA 1906	Todos
1906	Duração do início da sessão	DC 7 1906 e VDA 1903	Todos
1906	Investigação da área de trabalho	DC 7 1906 e Citrix Probe Agent 1903	Premium
7.9 e posterior	Duração do Citrix Profile Management no carregamento do perfil	VDA 1903	Todos
1811	Análise detalhada de perfil	DC 7 1811 e VDA 1811	Todos
1811	Monitoramento de alertas do Hypervisor	DC 7 1811	Premium
1811	Investigação de aplicativo	DC 7 1811 e Citrix Application Probe Agent 1811	Premium
1811	Integridade da licença do Microsoft RDS	DC 7 1811 e VDA 7.16	Todos
1811	Exibição dos principais dados RTOP	DC 7 1811 e VDA 1808	Premium
1808	Exportação de dados de filtros	DC 7 1808	Todos

Versão do Director	Recurso	Dependências – versão mínima necessária	Edição
1808	Análise detalhada da sessão interativa	DC 7 1808 e VDA 1808	Todos
1808	Análise detalhada de GPO	DC 7 1808 e VDA 1808	Todos
1808	Dados históricos da máquina disponíveis usando a API OData	DC 7 1808	Todos
7.18	Investigação de aplicativo	DC 7.18	Premium (anteriormente Platinum)
7.18	Políticas de alertas inteligentes	DC 7.18	Premium (anteriormente Platinum)
7.18	Link do Health Assistant	Nenhuma	Todos
7.18	Análise detalhada da sessão interativa	Nenhuma	Todos
7.17	Autenticação por cartão inteligente PIV	Nenhuma	Todos
7.16	Análise de aplicativos	DC 7.16 e VDA 7.15	Todos
7.16	OData API V.4	DC 7.16	Todos
7.16	Sombrear usuários Linux VDA	VDA 7.16	Todos
7.16	Suporte a grupos locais de domínio	Nenhuma	Todos
7.16	Acesso ao console da máquina	DC 7.16	Todos
7.15	Monitoramento de falhas de aplicativo	DC 7.15 e VDA 7.15	Todos
7.14	Solução de problemas centrada no aplicativo	DC 7.13 e VDA 7.13	Todos

Versão do Director	Recurso	Dependências – versão mínima necessária	Edição
7.14	Monitoramento de disco	DC 7.14 e VDA 7.14	Todos
7.14	Monitoramento de GPU	DC 7.14 e VDA 7.14	Todos
7.13	Protocolo de transporte no painel de detalhes da sessão	DC 7.x e VDA 7.13	Todos
7.12	Descrições claras de falhas de máquina e conexão	DC 7.12 e VDA 7.x	Todos
7.12	Maior disponibilidade de dados históricos na edição Enterprise	DC 7.12 e VDA 7.x	Enterprise
7.12	Relatórios personalizados	DC 7.12 e VDA 7.x	Premium (anteriormente Platinum)
7.11	Relatórios de utilização de recursos	DC 7.11 e VDA 7.11	Todos
7.11	Alertas estendidos para condições de CPU, memória e ICA RTT	DC 7.11 e VDA 7.11	Premium (anteriormente Platinum)
7.11	Melhorias de exportação de relatórios	DC 7.11 e VDA 7.x	Todos
7.11	Integração com o Citrix ADM	DC 7.11, VDA 7.x e MAS versão 11.1 compilação 49.16	Premium (anteriormente Platinum)
7.9	Detalhamento da duração do logon	DC 7.9 e VDA 7.x	Todos
7.7	Monitoramento e alertas proativos	DC 7.7 e VDA 7.x	Premium (anteriormente Platinum)

Versão do Director	Recurso	Dependências – versão mínima necessária	Edição
7.7	Integração com SCOM	DC 7.7, VDA 7.x, SCOM 2012 R2 e PowerShell 3.0	Premium (anteriormente Platinum)
7.7	Integração com autenticação do Windows	DC 7.x e VDA 7.x	Todos
7.7	Uso de SO de sessão única e multissessão	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 Session Recording	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

June 28, 2023

Agregação de valores de dados

O Monitor Service coleta vários dados, incluindo uso de sessão do usuário, detalhes do desempenho de logon do usuário, detalhes do balanceamento de carga da sessão e informações de falha de máquina e conexão. Os dados são agregados de forma diferente, dependendo de sua categoria. Compreender a agregação de valores dos dados apresentados usando as APIs do método OData é fundamental para interpretar os dados. Por exemplo:

- Connected Sessions e Machine Failures ocorrem ao longo de um período. Portanto, são exibidas como máximos ao longo de um período de tempo.

- Duração do logon é uma medida de tempo, portanto, é exposta como uma média ao longo de um período de tempo.
- Contagem de logon e falhas de conexão são contagens de ocorrências ao longo de um período, portanto, são expostas como somas ao longo de um período de tempo.

Avaliação simultânea de dados

As sessões devem estar sobrepostas para serem consideradas simultâneas. No entanto, quando o intervalo de tempo é 1 minuto, todas as sessões nesse minuto (caso se sobreponham) são consideradas simultâneas. O tamanho do intervalo é tão pequeno que a sobrecarga de desempenho envolvida no cálculo da precisão não vale o valor adicionado. Se as sessões ocorrerem na mesma hora, mas não no mesmo minuto, elas não são consideradas sobrepostas.

Correlação de tabelas de resumo com dados brutos

O modelo de dados representa as métricas de duas maneiras diferentes:

- As tabelas de resumo representam exibições agregadas das métricas granulares por minuto, hora e dia.
- Os dados brutos representam eventos individuais ou o estado atual rastreado na sessão, conexão, aplicativo e outros objetos.

Ao tentar correlacionar dados entre chamadas de API ou dentro do próprio modelo de dados, é importante entender os seguintes conceitos e limitações:

- **Não há dados resumidos para intervalos parciais.** Os resumos de métricas são projetados para atender às necessidades das tendências históricas por longos períodos de tempo. Essas métricas são agregadas na tabela de resumo para intervalos completos. Não há dados resumidos para um intervalo parcial no início (dados disponíveis mais antigos) da coleta de dados nem no final. Ao visualizar agregações de um dia (Intervalo=1440), isso significa que o primeiro dia e os dias incompletos mais recentes não têm dados. Embora possam existir dados brutos para esses intervalos parciais, eles nunca são resumidos. Você pode determinar o intervalo agregado mais antigo e mais recente para uma granularidade de dados específica, extraindo o SummaryDate mínimo e máximo de uma tabela de resumo específica. A coluna SummaryDate representa o início do intervalo. A coluna Granularity representa o comprimento do intervalo para os dados agregados.
- **Correlação por tempo.** As métricas são agregadas na tabela de resumo para intervalos completos, conforme descrito na seção anterior. Elas podem ser usadas para tendências históricas, mas eventos brutos podem ser mais atuais no estado do que o que foi resumido para a análise

de tendências. Qualquer comparação baseada em tempo entre dados de resumo e dados brutos deve 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.** Métricas que são agregadas na tabela de resumo podem ser um pouco imprecisas se houver eventos perdidos ou latentes no período de agregação. Embora o Monitor Service tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo dos eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a alta disponibilidade de conexão, haverá lacunas nas contagens de dados resumidas das conexões atuais, mas as instâncias da sessão continuarão em execução nos dados brutos.
- **Períodos de retenção de dados.** Os dados nas tabelas de resumo são retidos em uma programação de limpeza diferente da programação para dados brutos do evento. Os dados podem estar ausentes porque foram eliminados das tabelas de resumo ou de dados brutos. Os períodos de retenção também podem diferir para diferentes granularidades de dados de resumo. Dados de granularidade mais baixa (minutos) são eliminados mais rapidamente do que os dados de granularidade mais alta (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles podem ser encontrados em uma granularidade maior. Como as chamadas de API retornam apenas a granularidade específica solicitada, não receber dados para uma granularidade não significa que os dados não existam para uma granularidade maior para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não caem em limites por hora, pode haver alguma discrepância quanto ao local em que os dados são agregados.

Granularidade e retenção

A granularidade dos dados agregados recuperados pelo 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 somente dados relevantes sejam mantidos a longo prazo. A limpeza garante melhor desempenho, mantendo a granularidade necessária para a emissão de relatórios. Os clientes em sites licenciados Premium podem alterar a retenção de limpeza para o número desejado de dias de retenção, caso contrário, o padrão é usado. Caso tenha havido uma perda de conectivi-

dade com o banco de dados do Site, o Monitor Service usará os dias de retenção padrão para o direito Premium, conforme especificado na tabela abaixo.

Para acessar as configurações, execute os seguintes comandos do PowerShell no Delivery Controller:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

	Nome do parâmetro	Limpeza afetada	Valor padrão Premium (dias)	Valor padrão não Premium (dias)
1	GroomSessionsRetentionDays	Retenção de registros de sessão e conexão após o encerramento da sessão	90	7
2	GroomFailuresRetentionDays	Registros de MachineFailureLog e ConnectionFailureLog	90	7
3	GroomLoadIndexesRetentionDays	Registros LoadIndex	90	7

	Nome do parâmetro	Limpeza afetada	Valor padrão Premium (dias)	Valor padrão não Premium (dias)
4	GroomDeletedRetentionDays	Entidades de máquina, catálogo, grupo de áreas de trabalho e Hypervisor que têm LifecycleState como “Deleted”. Essa configuração também exclui todos os registros relacionados a Session, SessionDetail, Summary, Failure ou LoadIndex.	90	7
5	GroomSummariesRetentionDays	Registros Desktop-GroupSum-mary, FailureLog-Summary e LoadIndex-Summary. Dados agregados - granularidade diária.	90	7

	Nome do parâmetro	Limpeza afetada	Valor padrão Premium (dias)	Valor padrão não Premium (dias)
6	GroomMachineHotfixLogRetentionDays	Hotfixes aplicados às máquinas VDA e Controller	90	90
7	GroomMinuteRetentionDays	Dados agregados - granularidade por minuto	3	3
8	GroomHourlyRetentionDays	Dados agregados - granularidade por hora	32	7
9	GroomApplicationInstanceRetentionDays	Histórico de instância do aplicativo	90	0
10	GroomNotificationLogRetentionDays	Registro de log de notificação	90	
11	GroomResourceUsageRawDataRetentionDays	Dados brutos de utilização do recurso - dados brutos	1	1
12	GroomResourceUsageMinuteDataRetentionDays	Dados de resumo da utilização do recurso - granularidade por minuto	7	7
13	GroomResourceUsageHourDataRetentionDays	Dados de resumo de utilização do recurso - granularidade por hora	30	7

	Nome do parâmetro	Limpeza afetada	Valor padrão Premium (dias)	Valor padrão não Premium (dias)
14	GroomResourceUsageDaySummaryDataRetentionDays	Dados de resumo de utilização do recurso - granularidade por dia	90	7
15	GroomProcessUsageRawDataRetentionDays	Dados de utilização do processo - dados brutos	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Dados de utilização do processo - granularidade por minuto	3	3
17	GroomProcessUsageHourDataRetentionDays	Dados de utilização do processo - granularidade por hora	7	7
18	GroomProcessUsageDayDataRetentionDays	Dados de utilização do processo - granularidade por dia	30	7
19	GroomSessionMetricsDataRetentionDays	Dados de métricas de sessão	1	1
20	GroomMachineMetricsDataRetentionDays	Dados de métricas de máquina	3	3
21	GroomMachineMetricsDaySummaryDataRetentionDays	Dados de resumo de métricas de máquina	90	7

	Nome do parâmetro	Limpeza afetada	Valor padrão Premium (dias)	Valor padrão não Premium (dias)
22	GroomApplicationErrorsRetentionDays	Dados de erro do aplicativo	1	1
23	GroomApplicationFaultsRetentionDays	Dados de falha do aplicativo	1	1

> **Cuidado:**
>
> A modificação de valores no banco de dados do Monitor Service requer a reinicialização do serviço para que os novos valores entrem em vigor. Recomendamos que você faça alterações no banco de dados do Monitor Service somente sob a direção do Suporte Citrix.

As configurações de GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays e GroomSessionMetricsDataRetentionDays são limitadas aos seus valores padrão de 1, enquanto GroomProcessUsageMinuteDataRetentionDays é limitado ao seu valor padrão de 3. Os comandos do PowerShell para definir esses valores foram desativados, pois os dados de uso do processo tendem a crescer rapidamente.
Além disso, as configurações de retenção baseadas em licença são as seguintes:

- **Sites licenciados Premium** – a retenção de limpeza para todas as configurações é limitada a 1000 dias (a Citrix recomenda 365 dias).
- **Sites licenciados 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 só pode ser definido em sites licenciados Premium.
- GroomApplicationErrorsRetentionDays e GroomApplicationFaultsRetentionDays são limitados a 31 dias em sites licenciados Premium.

A retenção de dados por longos períodos tem as seguintes implicações nos tamanhos das tabelas:

- **Dados por hora.** Se os dados por hora puderem permanecer no banco de dados por até dois anos, um site de 1000 grupos de entrega pode fazer com que o banco de dados cresça da seguinte forma:

  1000 grupos de entrega x 24 horas/dia x 365 dias/ano x 2 anos = 17.520.000 linhas de dados. O impacto no desempenho de uma quantidade tão grande de dados nas tabelas de agregação é

significativo. Como os dados do painel são extraídos dessa tabela, os requisitos no servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto drástico no desempenho.

- **Dados de sessão e evento.** Dados coletados toda vez que uma sessão é iniciada e uma conexão/reconexão é feita. Em um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, em dois anos, essas tabelas reuniriam mais de um TB de dados, exigindo um banco de dados de nível empresarial de alta capacidade.

Motivo de falhas e solução de problemas no Citrix Director

June 28, 2023

As tabelas a seguir descrevem as várias categorias de falha, os motivos e a ação que você precisa tomar para resolver os problemas. Para obter mais informações, consulte Enums, códigos de erro e descrições.

Erros de falha na conexão

Categoria	Motivo	Problema	Ação
N/A	[0] Unknown. Esse código de erro não está mapeado.	O Monitoring Service não pode determinar o motivo da falha de conexão ou inicialização relatada pelas informações compartilhadas pelo Broker Service.	Colete logs de CDF no Controller e entre em contato com o suporte Citrix.
[0] None	[1] None	Nenhuma	N/A

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[2] SessionPreparation	Solicitação de preparação da sessão do Delivery Controller para o VDA falhou. Possíveis causas: problemas de comunicação entre o Controller e o VDA, problemas enfrentados pelo Broker Service ao criar uma solicitação de preparação ou problemas de rede resultando na não aceitação da solicitação pelo VDA.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops, para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
[2] MachineFailure	[3] RegistrationTimeout	O VDA foi ligado, mas o tempo limite esgotou durante a tentativa de se registrar no Delivery Controller.	Verifique se o Citrix Broker Service está em execução no Delivery Controller e se o Desktop Service está em execução no VDA. Se interrompido, inicie cada um deles.

Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[4] ConnectionTimeout	O cliente não se conectou ao VDA depois que o VDA foi preparado para o início da sessão. A sessão foi intermediada com sucesso, mas o tempo limite esgotou enquanto aguardava o cliente se conectar ao VDA. Possíveis causas: configurações do firewall, interrupções de rede ou configurações que impedem conexões remotas.	Verifique o console Director para confirmar se o cliente tem uma conexão ativa atualmente, o que significa que nenhum usuário é afetado. Se não existir nenhuma sessão, revise os logs de eventos no cliente e no VDA em busca de erros. Resolva os problemas de conectividade de rede entre o cliente e o VDA.
[4] NoLicensesAvailable	[5] Licensing	A solicitação de licenciamento falhou. Possíveis causas: número insuficiente de licenças ou o servidor de licenças ficou inativo por mais de 30 dias.	Verifique se o servidor de licenças está online e acessível. Resolva os problemas de conectividade de rede com o servidor de licenças ou reinicialize o servidor de licenças se apresentar mau funcionamento. Verifique se há licenças suficientes no ambiente e aloque mais, se necessário.

Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[6] Ticketing	Ocorreu uma falha durante a emissão de tickets, indicando que a conexão do cliente com o VDA não corresponde à solicitação do agente. Um ticket de solicitação de inicialização é preparado pelo Broker e entregue no arquivo ICA. Quando o usuário tenta iniciar uma sessão, o VDA valida o ticket de inicialização no arquivo ICA com o Broker. Possíveis causas: o arquivo ICA está corrompido ou o usuário está tentando estabelecer uma conexão não autorizada.	Verifique se o usuário tem acesso ao aplicativo ou à área de trabalho com base nos grupos de usuários definidos nos grupos de entrega. Instrua o usuário a reiniciar o aplicativo ou a área de trabalho para determinar se o problema já se resolveu. Se o problema ocorrer novamente, revise os logs de eventos do dispositivo cliente em busca de erros. Verifique se o VDA ao qual o usuário está tentando se conectar está registrado. Se não estiver registrado, revise os logs de eventos no VDA e resolva os problemas de registro.
[1] ClientConnection-Failure	[7] Other	Uma sessão foi relatada como encerrada a partir do VDA depois que o cliente entrou em contato com o VDA inicialmente, mas antes de concluir a sequência de conexão.	Verifique se a sessão não foi encerrada pelo usuário antes da inicialização. Tente reiniciar a sessão, se o problema persistir, colete registros de CDF e entre em contato com o suporte Citrix.

Categoria	Motivo	Problema	Ação
[1] ClientConnection-Failure	[8] GeneralFail	A sessão não foi iniciada. Possíveis causas: um início intermediado foi solicitado enquanto o agente ainda estava iniciando ou inicializando, ou erro interno durante a fase de intermediação de um início.	Verifique se o Citrix Broker Service está em execução e tente iniciar a sessão novamente.
[5] Configuration	[9] MaintenanceMode	O VDA, ou o grupo de entrega ao qual o VDA pertence, é definido no modo de manutenção.	Determine se o modo de manutenção é necessário. Desative o modo de manutenção no grupo de entrega ou na máquina em questão se não for necessário e instrua o usuário a tentar reconectar.
[5] Configuration	[10] ApplicationDisabled	O aplicativo não pode ser acessado por usuários finais porque ele foi desativado pelo administrador.	Se o aplicativo tiver que estar disponível para uso em produção, habilite o aplicativo e instrua o usuário a se reconectar.
[4] NoLicensesAvailable	[11] LicenseFeature Refused	O recurso que está sendo usado não é coberto pelas licenças existentes.	Entre em contato com um representante de vendas da Citrix para confirmar os recursos cobertos pela edição e tipo da licença existente do Citrix Virtual Apps and Desktops.

Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[13] SessionLimitReached	Todos os VDAs estão em uso e não há capacidade de hospedar mais sessões. Causas possíveis: todos os VDAs estão em uso (para VDAs com SO de sessão única) ou todos os VDAs atingiram o máximo de sessões simultâneas configuradas permitidas (para VDAs com SO multissessão).	Verifique se há algum VDA no modo de manutenção. Desative o modo de manutenção se não for necessário para liberar mais capacidade. Considere aumentar o valor de **Maximum Number of Sessions** na configuração de política Citrix para permitir mais sessões por VDA de servidor. Considere adicionar mais VDAs com SO multissessão. Considere adicionar mais VDAs com SO de sessão única.
[5] Configuration	[14] DisallowedProtocol	Os protocolos ICA e RDP não são permitidos.	Execute o comando **Get-BrokerAccessPolicyRule** do PowerShell no Delivery Controller e verifique se o valor **AllowedProtocols** tem todos os protocolos desejados listados. Esse problema ocorre somente se houver uma configuração incorreta.

Categoria	Motivo	Problema	Ação
[5] Configuration	[15] ResourceUnavailable	O aplicativo ou a área de trabalho ao qual o usuário está tentando se conectar não está disponível. Esse aplicativo ou área de trabalho pode não existir, ou não há VDAs disponíveis para executá-lo. Possíveis causas: a publicação do aplicativo ou da área de trabalho foi cancelada, ou os VDAs que hospedam o aplicativo ou a área de trabalho atingiram a carga máxima, ou o aplicativo ou a área de trabalho está definida no modo de manutenção.	Verifique se o aplicativo ou a área de trabalho ainda está publicado e se os VDAs não estão no modo de manutenção. Determine se os VDAs com SO multissessão estão em carga total. Em caso afirmativo, provisione mais VDAs com SO multissessão. Verifique se há VDAs com SO de sessão única disponíveis para conexões. Provisione mais VDAs com SO de sessão única, se necessário.
[5] Configuration	[16] ActiveSessionReconnectDisabled	A sessão ICA está ativa e conectada a um ponto de extremidade diferente. No entanto, como **Active Session Reconnection** está desativada, o cliente não pode se conectar à sessão ativa.	No Delivery Controller, verifique se **Active Session Reconnection** está ativada. Verifique se o valor de **DisableActiveSessionReconnect** no registro sob **HKEY_LOCAL_MACHINE\Software** está definido como 0.
[2] MachineFailure	[17] NoSessionToReconnect	O cliente tentou se reconectar a uma sessão específica, mas a sessão foi encerrada.	Repita a reconexão do controle do espaço de trabalho.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[18] SpinUpFailed	O VDA não pode ser ligado a partir do início da sessão. Este é um problema relatado pelo hipervisor.	Se a máquina ainda estiver desligada, tente iniciar a máquina a partir do Citrix Studio. Se isso falhar, revise a conectividade e as permissões do hipervisor. Se o VDA for uma máquina provisionada por PVS, verifique no console PVS se a máquina está em execução. Caso contrário, verifique se a máquina recebeu um Personal vDisk; faça login no hipervisor para redefinir a VM.
[2] MachineFailure	[19] Refused	O Delivery Controller envia uma solicitação ao VDA para se preparar para uma conexão de um usuário final, mas o VDA recusa ativamente essa solicitação.	Verifique via ping se o Delivery Controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva os problemas de roteamento de rede ou firewall.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[20] ConfigurationSet Failure	O Delivery Controller não enviou os dados de configuração necessários, como configurações de política e informações de sessão, para o VDA durante o início da sessão. Possíveis causas: problemas de comunicação entre o Controller e o VDA, problemas que o Broker Service ao criar uma solicitação de configuração ou problemas de rede resultando não aceitação da solicitação pelo VDA.	-
[3] NoCapacityAvailable	[21] MaxTotalInstance-sExceeded	O número máximo de instâncias de um aplicativo foi atingido. Nenhuma instância adicional do aplicativo pode ser aberta no VDA. Esse problema está relacionado ao recurso de limites de aplicativos.	Considere aumentar a configuração do aplicativo, **Limit the number of instances running at the same time**, para um valor maior se o licenciamento permitir.

Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	O usuário está tentando abrir mais do que uma instância de um aplicativo, mas o aplicativo está configurado para permitir apenas uma única instância do aplicativo por usuário. Esse problema está relacionado ao recurso de limites de aplicativos.	Por padrão, apenas uma instância do aplicativo é permitida por usuário. Se forem necessárias várias instâncias por usuário, considere limpar a configuração de **Limit to one instance per user** na configuração do aplicativo.
[1] ClientConnectionFailure	[23] Communication error	O Delivery Controller tentou enviar informações para o VDA, como uma solicitação para se preparar para uma conexão, mas ocorreu um erro durante a tentativa de comunicação. Isso pode ser causado devido a interrupções na rede.	Se já iniciado, reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verificar se o VDA se registra com êxito. Confirme se os Delivery Controllers configurados para o VDA estão precisos por meio dos detalhes no log de eventos do aplicativo.

Categoria	Motivo	Problema	Ação
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring Service converte [12] NoDesktopAvailable para esse código de erro.	O VDA atribuído para iniciar a sessão está em um estado inválido ou está indisponível. Possíveis causas: o estado de energia do VDA é desconhecido ou indisponível, o VDA não foi reinicializado desde a última sessão do usuário, o compartilhamento de sessão está desativado, mas a sessão atual exige que esteja ativado, ou o VDA foi removido do grupo de entrega ou do site.	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se há VDAs suficientes registrados e no estado pronto para poder iniciar a área de trabalho compartilhada publicada ou o aplicativo solicitado pelo usuário. Verifique se o hipervisor que hospeda o VDA não está no modo de manutenção.

Categoria	Motivo	Problema	Ação
[2] MachineFailure	[101] MachineNotFunctional. Monitoring Service converte [12] NoDesktopAvailable para esse código de erro.	O VDA não está operacional. Possíveis causas: o VDA foi removido do grupo de entrega, o VDA não está registrado, o estado de energia do VDA não está disponível ou o VDA está tendo problemas internos.	Verifique se o VDA está em um grupo de entrega. Caso contrário, adicione-o ao grupo de entrega apropriado. Verifique se o VDA é exibido como ativado no Citrix Studio. Se o estado de energia for desconhecido para várias máquinas, resolva os problemas de conectividade com o hipervisor ou as falhas do host. Verifique se o hipervisor que hospeda o VDA não está no modo de manutenção. Reinicialize o VDA depois que os problemas tiverem sido resolvidos.

Tipo de falha na máquina

Código de erro	ID do código de erro	Problema	Ação
Unknown	-	-	-
Unregistered	3	-	-

Código de erro	ID do código de erro	Problema	Ação
MaxCapacity (representado como carga máxima no Director)	4	A máquina atingiu sua capacidade máxima, ou seja, Max Load Index	Certifique-se de que todos os hipervisores estejam ligados. Adicione mais máquinas aos grupos de entrega afetados adicionando mais capacidade ao hipervisor ou adicionando mais hipervisores.
StuckOnBoot	2	A VM não completou sua sequência de inicialização e não está se comunicando com o hipervisor.	Certifique-se de que a VM seja inicializada com sucesso no hipervisor. Verifique se há outras mensagens na VM, como, por exemplo, problemas do sistema operacional. Certifique-se de que as ferramentas do hipervisor estejam instaladas na VM. Certifique-se de que o VDA esteja instalado na VM.
FailedToStart	1	A VM teve problemas ao tentar iniciar no hipervisor.	Verifique os logs do hipervisor.
Nenhuma	0	-	-

Motivo do cancelamento do registro da máquina (aplicável quando o tipo de falha for Unregistered ou Unknown)

Código de erro	ID do código de erro	Problema	Ação
AgentShutdown	0	O VDA desligou no período de tolerância.	Ligue o VDA se você não deseja que ele esteja desligado com base nas políticas de gerenciamento de energia existentes. Revise os erros nos logs de eventos.
AgentSuspended	1	O VDA está em modo de hibernação ou suspensão.	Retire o VDA do modo de hibernação. Considere desativar a hibernação nos VDAs do Citrix Virtual Apps and Desktops usando as configurações de energia.
IncompatibleVersion	100	O VDA não pode se comunicar com o Delivery Controller devido a uma incompatibilidade de versões do protocolo da Citrix.	Alinhe as versões do VDA e do Delivery Controller.

Código de erro	ID do código de erro	Problema	Ação
AgentAddressResolutionFailed	1011	O Delivery Controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão precisos. Caso contrário, corrija-os. Se for generalizado, valide as configurações de DNS nos Delivery Controllers. Verifique a resolução de DNS do Controller executando o comando `nslookup`.
	101	O Delivery Controller não conseguiu resolver o endereço IP do VDA.	Verifique se a conta da máquina VDA existe no AD. Caso contrário, crie-a. Verifique se o nome e o endereço IP do VDA no DNS estão precisos. Caso contrário, corrija-os.

Código de erro	ID do código de erro	Problema	Ação
AgentNotContactable	102	Ocorreu um problema de comunicação entre o Delivery Controller e o VDA.	Use ping para verificar se o Delivery Controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva os problemas de firewall ou rede. Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.

Código de erro	ID do código de erro	Problema	Ação
	102	Ocorreu um problema de comunicação entre o Delivery Controller e o VDA.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA. Entre em contato com o suporte Citrix.
AgentWrongActiveDirectoryOU	103	Houve uma configuração incorreta de descoberta do Active Directory. A unidade organizacional específica do site (onde as informações do Controller do site são armazenadas no AD) configurada no registro do VDA é para um site diferente.	Verifique se a configuração do Active Directory está correta ou verifique as configurações do registro.

Código de erro	ID do código de erro	Problema	Ação
EmptyRegistrationReques	104	A solicitação de registro enviada do VDA para o Delivery Controller estava vazia. Isso pode ser devido a uma instalação de software do VDA corrompida.	Reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verifique se o VDA se registra com êxito através do log de eventos do aplicativo.
MissingRegistrationCapabilities	105	A versão VDA não é compatível com o Delivery Controller.	Atualize o VDA ou remova o VDA e reinstale-o.
MissingAgentVersion	106	A versão VDA não é compatível com o Delivery Controller.	Reinstale o software do VDA se o problema estiver afetando todas as máquinas.
InconsistentRegistrationCapabilities	107	O VDA não pode comunicar seus recursos ao Broker. Isso pode ser devido à incompatibilidade entre as versões do VDA e do Delivery Controller. Os recursos de registro, que mudam a cada versão, são expressos em um formato que não corresponde à solicitação de registro.	Alinhe as versões do VDA e do Delivery Controller.
NotLicensedForFeature	108	O recurso que você está tentando usar não está licenciado.	Verifique a edição do seu Citrix Licensing ou remova o VDA e reinstale-o.
	108	O recurso que você está tentando usar não está licenciado.	Entre em contato com o suporte Citrix.

Código de erro	ID do código de erro	Problema	Ação
UnsupportedCredentialSecurityversion	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 para o Broker, mas o conteúdo da solicitação está corrompido ou é inválido.	Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
SingleMultiSessionMismatch	111	O tipo de sistema operacional do VDA não é compatível com o catálogo de máquinas ou o grupo de entrega.	Adicione o VDA ao tipo de catálogo de máquinas correto ou grupo de entrega contendo máquinas com o mesmo sistema operacional.
FunctionalLevelTooLowForCatalog	112	O catálogo de máquinas é definido a um nível funcional de VDA mais alto do que a versão do VDA instalada.	Verifique se o nível funcional do catálogo de máquinas do VDA corresponde ao do VDA. Faça upgrade ou downgrade do catálogo de máquinas para corresponder ao do VDA.

Código de erro	ID do código de erro	Problema	Ação
FunctionalLevelTooLowForDesktopGroup	112	O grupo de entrega é definido a um nível funcional de VDA mais alto do que a versão do VDA instalada.	Verifique se o nível funcional do grupo de entrega do VDA corresponde ao do VDA. Faça upgrade ou downgrade do catálogo de máquinas para corresponder ao do VDA.
PowerOff	200	O VDA não desligou no período de tolerância.	Se o VDA deveria estar ligado, tente iniciar o VDA a partir do Citrix Studio e verifique se ele inicializa e se registra corretamente. Solucione os problemas de inicialização ou registro. Revise os logs de eventos no VDA assim que for feito backup para ajudar a determinar a causa raiz do desligamento.
AgentRejectedSettingsUpdate	203	Configurações como políticas da Citrix foram alteradas ou atualizadas, mas houve um erro ao enviar as atualizações para o VDA. Isso pode ocorrer se as atualizações forem incompatíveis com a versão do VDA instalada.	Atualize o VDA, se necessário. Verifique se as atualizações que foram aplicadas são suportadas com a versão do VDA.

Código de erro	ID do código de erro	Problema	Ação
SessionPrepareFailure	206	O Broker não concluiu a auditoria das sessões que estão em execução no VDA.	Se for generalizado, reinicie o Citrix Broker Service no Delivery Controller.
	206	O Broker não concluiu a auditoria das sessões que estão em execução no VDA.	Entre em contato com o suporte Citrix.
ContactLost	207	O Delivery Controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções na rede.	Verifique se o Citrix Broker Service está em execução no Delivery Controller e se o Desktop Service está em execução no VDA. Se interrompido, inicie cada um deles. Se já iniciado, reinicialize o Desktop Service no VDA para reinicializar o processo de registro e verificar se o VDA se registra com êxito. Confirme se os Delivery Controllers configurados para o VDA estão precisos por meio dos detalhes no log de eventos do aplicativo. Use ping para verificar se o Delivery Controller e o VDA podem se comunicar com sucesso. Caso contrário, resolva os problemas de firewall ou rede.

Código de erro	ID do código de erro	Problema	Ação
	207	O Delivery Controller perdeu a conexão com o VDA. Isso pode ser causado por interrupções na rede.	Verifique se o Desktop Service está em execução no VDA. Se interrompido, inicie.
BrokerRegistrationLimitReached	301	O Delivery Controller atingiu o número máximo configurado de VDAs que têm permissão para se registrar simultaneamente. Por padrão, o Delivery Controller permite 10.000 registros simultâneos de VDA.	Considere adicionar Delivery Controllers ao Site ou criar um Site. Você também pode aumentar o número de VDAs autorizados a se registrar simultaneamente no Delivery Controller por meio da chave de registro **HKEY_LOCAL_MACHINE\Software** Consulte o artigo do Knowledge Center, Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446), para obter mais informações. Aumentar esse número pode exigir mais recursos de CPU e memória para o Controller.

Código de erro	ID do código de erro	Problema	Ação
SettingsCreationFailure	208	O Broker não construiu um conjunto de definições e configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falha, resultando em um VDA sem registro.	Verifique os logs de eventos no Delivery Controller em busca de erros. Reinicie o Broker Service se um problema específico não estiver evidente nos registros. Depois que o Broker Service for reiniciado, reinicie o Desktop Service nos VDAs afetados e verifique se eles se registram corretamente.
	208	O Broker não construiu um conjunto de definições e configurações para enviar ao VDA. Se o Broker não conseguir coletar os dados, o registro falha, resultando em um VDA sem registro.	Reinicie o Desktop Service nos VDAs afetados e verifique se eles se registram corretamente. Entre em contato com o suporte Citrix.

Código de erro	ID do código de erro	Problema	Ação
SendSettingsFailure	204	O Broker não enviou definições e dados de configuração para o VDA. Se o Broker conseguir coletar os dados, mas não conseguir enviá-los, o registro falha.	Se limitado a um único VDA, reinicialize o Desktop Service no VDA para forçar o novo registro e validar se o VDA se registra com êxito por meio do log de eventos do aplicativo. Solucione os problemas ocorridos. Consulte as etapas de solução de problemas listadas no artigo no Knowledge Center, Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668), para ver os problemas comuns que causam problemas de comunicação entre o Controller e o VDA.
AgentRequested	2	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
DesktopRestart	201	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
DesktopRemoved	202	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
SessionAuditFailure	205	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
UnknownError	300	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.

Código de erro	ID do código de erro	Problema	Ação
RegistrationStateMismatch	302	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.
Unknown	-	Ocorreu um erro desconhecido.	Entre em contato com o suporte Citrix.

Notas para terceiros

June 28, 2023

Esta versão do Citrix Virtual Apps and Desktops pode incluir software de terceiros licenciado sob os termos definidos nos seguintes documentos:

- Notas para terceiros do Citrix Virtual Apps and Desktops (PDF para download)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (PDF para download)
- FlexNet Publisher Documentation Supplement Third Party e Open Source Software usado no FlexNet Publisher 11.15.0 (PDF para download)

SDKs e APIs

June 28, 2023

Vários SDKs e APIs estão disponíveis nesta versão. Para acessar os SDKs e as APIs, acesse Build anything with Citrix. Selecione **Citrix Workspace** para acessar as informações de programação do Citrix Virtual Apps and Desktops e seus componentes relacionados.

> **Nota:**
>
> O Citrix Virtual Apps and Desktops SDK e o Citrix Group Policy SDK podem ser instalados como um módulo ou um snap-in. Vários componentes SDK (como Citrix Licensing, Citrix Provisioning e StoreFront) são instalados usando apenas um snap-in.

Este produto oferece suporte ao PowerShell versões 3 a 5.

Citrix Virtual Apps and Desktops SDK

Esse SDK é instalado automaticamente como um módulo do PowerShell quando você instala um Delivery Controller ou Studio. Isso permite que você use os cmdlets desse SDK sem precisar adicionar snap-ins. (As instruções são fornecidas abaixo se você optar por instalar este SDK como um snap-in.)

Permissions

Você deve executar o shell ou script usando uma identidade que tenha direitos de administração Citrix. Embora os membros do grupo de administradores locais no Controller tenham automaticamente privilégios administrativos completos para permitir a instalação do Citrix Virtual Apps ou Citrix Virtual Desktops, a Citrix recomenda que, para a operação normal, você crie administradores Citrix com os direitos apropriados, em vez de usar a conta de administradores locais.

Acessar e executar os cmdlets

1. Inicie um shell no PowerShell: abra o Studio, selecione a guia **PowerShell** e clique em **Launch PowerShell**.
2. Para usar cmdlets do SDK em scripts, defina a política de execução no PowerShell. Para obter informações sobre a política de execução do PowerShell, consulte a documentação da Microsoft.
3. Se você quiser usar o snap-in (em vez do módulo), adicione o snap-in usando o cmdlet `Add-PSSnapin` (ou `asnp`).

   V1 e V2 indicam a versão do snap-in. Os snap-ins do XenDesktop 5 são da versão 1. O Citrix Virtual Apps and Desktops e snap-ins anteriores à versão XenDesktop 7 são da versão 2 Por exemplo, para instalar o snap-in 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 desse SDK, selecione o produto ou componente na lista Categories e selecione **Citrix Virtual Apps and Desktops SDK**.
- Para obter orientação sobre o PowerShell, consulte Windows PowerShell Integrated Scripting Environment (ISE).

Group Policy SDK

O Citrix Group Policy SDK permite exibir e configurar os filtros e as configurações da política de grupo. Esse SDK usa um provedor do PowerShell para criar uma unidade virtual que corresponde a configu-

rações e filtros de máquina e usuário. O provedor aparece como uma extensão a `New-PSDrive`.

Para usar o Group Policy SDK, o Studio ou o Citrix Virtual Apps and Desktops SDK devem estar instalados.

O provedor do Citrix Group Policy PowerShell está disponível como um módulo ou um snap-in.

- Para usar o módulo, não é necessário nenhum trabalho adicional.
- Para adicionar o snap-in, digite `Add-PSSnapin citrix.common.grouppolicy`.

Para acessar a ajuda, digite: `help New-PSDrive -path localgpo:/`.

Para criar uma unidade virtual e carregá-la com configurações, digite `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`, onde a cadeia de caracteres Controller é o nome de domínio totalmente qualificado de um Controller no site ao qual você deseja se conectar e do qual deseja carregar configurações.

APIs REST do Citrix Virtual Apps and Desktops

Com as APIs REST do Citrix Virtual Apps and Desktops, você pode automatizar o gerenciamento de recursos em uma implantação do Citrix Virtual Apps and Desktops.

As APIs REST do Citrix Virtual Apps and Desktops estão disponíveis em https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis. As APIs não aplicáveis ao Citrix Virtual Apps and Desktops estão marcadas de acordo. Siga as orientações fornecidas para configurar o acesso ao serviço de API e usar as APIs para gerenciar e otimizar seus recursos.

Monitor Service OData

A API Monitor permite o acesso aos dados do Monitor Service usando a versão 3 ou 4 da API OData. Você pode criar painéis personalizados de monitoramento e relatórios com base nos dados consultados a partir dos dados do Monitor Service. O OData V.4 é baseado na ASP.NET Web API e oferece suporte a consultas de agregação.

Para obter mais informações, consulte Monitor Service OData API.