Citrix Virtual Apps and Desktops 7 2402 LTSR

Contents

Citrix Virtual Apps and Desktops 7 2402 LTSR

August 22, 2024

Sobre este lançamento de versão

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

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

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

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

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

Para obter instruções de instalação e atualização:

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

Citrix Virtual Apps and Desktops 7 2402 LTSR

Secure HDX (versão prévia)

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

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

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

Novo política de modo de tolerância a perdas de áudio

O modo de tolerância a perdas de áudio agora está disponível para permitir a entrega de áudio por meio da política de modo tolerante a perdas.
Para obter mais informações, consulte Modo de tolerância a perdas de áudio.

Binários assinados por terceiros

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

Logs aprimorados do sistema para redirecionamento de conteúdo do navegador

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

Configuração aprimorada de redirecionamento de conteúdo bidirecional

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

Redutor HDX

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

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

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

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

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

Para obter mais informações, consulte a documentação da Microsoft.

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

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

Citrix Secure Private Access no local

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

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

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

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

Para obter mais informações, consulte Citrix Secure Private Access no local —Disponibilidade geral.

Virtual Delivery Agents (VDAs) 2402 LTSR

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

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

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

Suporte do WebSocket para VDAs

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

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

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

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

Web Studio

Suporte para provisionamento de VMs da VMware usando perfis de máquina

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

As configurações herdadas incluem:

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

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

Gerenciamento de imagens preparadas com o nó Imagens

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

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

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

Políticas relacionadas

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

Recursos preteridos

Os seguintes recursos e configurações foram descontinuados no Web Studio:

- Ambientes do Azure:

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

- Ambientes da AWS:

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

- Todos os ambientes de hipervisor e serviço de nuvem:

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

Citrix Director

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

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

As ações disponíveis incluem a exibição dos detalhes do seguinte:

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

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

Painel aprimorado de métricas de desempenho

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

Suporte para a versão mais recente do Microsoft Teams

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

Machine Creation Services (MCS)

Gerenciamento de imagens (prévia)

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

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

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

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

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

Configurar as permissões de conexão de host do Azure necessárias

Anteriormente, o teste de conexão do host validou se a credencial é boa para se conectar ao hipervisor. O teste não realizou a validação das permissões reais que talvez sejam necessárias para realizar operações do MCS relevantes, como gerenciamento de energia, criação de VMs e muito mais.

Com esse recurso, agora você pode configurar facilmente todas as permissões mínimas necessárias para uma conta de entidade de serviço ou de usuário no Azure vinculada a uma conexão de host para

realizar todas as operações do MCS usando um modelo do ARM. Esse modelo do ARM automatiza o seguinte:

- Criação de uma função do Azure com as permissões mínimas necessárias para as operações.
- Atribuição dessa função a uma entidade de serviço existente do Azure no nível da assinatura.

Você pode implantar esse modelo do ARM usando o Portal do Azure ou os comandos do PowerShell. Para obter mais informações, consulte Modelo do ARM para operações do CVAD.

Verificar se há várias NICs na VMware

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

Suporte para criar VMs do Windows 11 no GCP

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

Esse recurso é aplicável a:

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

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

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

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

Essa implementação oferece as seguintes vantagens:

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

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

Profile Management

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

Linux VDA

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

Session Recording

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

Workspace Environment Management

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

Citrix Provisioning

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

Serviço de autenticação federada

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

Componentes da linha de base da versão inicial 2402 LTSR

Componente de linha de base 2402	Versão conforme mostrada em programas e recursos	Documentação
VDA de sessão única	2402.0.4000.4310	VDA de sessão única
VDA de várias sessões	2402.0.4000.4310	VDA de várias sessões

Componente de linha de base 2402	Versão conforme mostrada em programas e recursos	Documentação
Delivery Controller	7.41.100.229	Delivery Controller
Citrix Studio	7.41.100.251	Citrix Studio
Citrix Director	7.33.4000.26	Citrix Director
Gerenciamento de políticas de grupo Citrix	7.41.100.115	Gerenciamento de políticas de grupo Citrix
Extensão do lado do cliente da Política de Grupo Citrix	7.41.100.115	
Citrix StoreFront	2402.0.100.64	Citrix StoreFront
Citrix Provisioning	7.41.100	Citrix Provisioning
Servidor de impressão universal	7.33.4000.11	Servidor de impressão universal
Session Recording	24.2.100.35	Session Recording
Linux VDA	24.02.0.93	Linux Virtual Delivery Agent
Profile Management	24.2.100.52	Profile Management
Serviço de autenticação federada da Citrix	10.17.100.90	Serviço de autenticação federada (FAS) da Citrix
Redirecionamento de conteúdo do navegador	15.32.4000.12	Redirecionamento de conteúdo do navegador
Citrix Probe Agent 2402	7.41.100.78	Download

Componentes compatíveis com a versão inicial 2402 LTSR

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

Componentes e recursos compatíveis	Versão conforme mostrada em programas e recursos	Documentação
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack

Componentes e recursos compatíveis	Versão conforme mostrada em programas e recursos	Documentação
Servidor de licenças	11.17.2.0_BUILD_47000	Servidor de licenças
Camada de personalização de usuário	23.9.1	Camada de personalização de usuário
Player da web do Session Recording	22.3.4000.4	Player da web do Session Recording
Otimização do Microsoft Teams	15.32.3000.9	Otimização do Microsoft Teams
Workspace Environment Management	2402.1.100.1	Workspace Environment Management

Exclusões notáveis da versão inicial 2402 LTSR

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

Componentes e recursos excluídos
AppDisks
AppDNA
Citrix SCOM Management Pack
Framehawk
Personal vDisk
Integração com o StoreFront Citrix Online

Plataformas Windows excluídas *
Windows 2008 de 32 bits (para Universal Print Server)

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

Problemas resolvidos

August 22, 2024

O Citrix Virtual Apps and Desktops 7 2402 LTSR inclui os seguintes problemas corrigidos:

Geral

- Quando o nome do dispositivo de áudio tem mais de 200 caracteres, o dispositivo pode não conseguir redirecionar para a sessão virtual. [HDX-58341]
- Para redirecionamento de webcam, não há suporte para o cliente RDP para o segundo salto. [HDX-55630]
- Quando você digitaliza uma imagem em uma sessão de área de trabalho com o ambiente configurado conforme descrito abaixo, a imagem pode não ser digitalizada. Esse problema é intermitente.

  - Instalação do driver do scanner e do aplicativo de imagem.
  - Política de direção USB ativada no DDC.
  - Configuração do ambiente:
    - DDC: Win2k19 + 7.33CU4
    - VDA: Win2k19/Win2k16+ 7.40.0.191
    - Cliente: Win10x64 22H2 + CWA 24.1.0.597

  [HDX-58888]
- A inicialização de um segundo aplicativo contínuo falhará se o SSL estiver ativado e a confiabilidade da sessão estiver desativada. Se um aplicativo integrado for iniciado, a inicialização subsequente de outro aplicativo contínuo no mesmo servidor deverá ser realizada na sessão existente (compartilhamento de sessão), enquanto o cliente tende a iniciar o aplicativo em uma nova sessão, fazendo com que uma solicitação de validação inesperada seja enviada ao agente. [HDX-52439].
- Se você estiver usando áudio mono para fluxos de áudio estéreo, poderá ouvir apenas um canal de áudio em um fone de ouvido em vez de receber os dois canais nos dois ouvidos. [HDX-56344]

Delivery Controller

- As atualizações na tabela `MonitorData.ResourceUtilization` do banco de dados de monitoramento estão atrasadas. [CVADHELP-22724]

- Quando você usar um VDA versão 2203 CU3 com o Windows 10, o instalador do VDA não hospedará a porta WCF personalizada se o Proxy do Rendezvous estiver configurado. [CVADHELP-24199]

Director

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

Gráficos

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

Política

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

Studio

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

- Quando você adiciona o endereço do servidor StoreFront por meio do Citrix Studio e o atribui a um grupo de entrega, o armazenamento é definido como desativado por padrão. [CVADHELP-24862]

Servidor de impressão universal

Impressão

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

VDA para SO de sessão única

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

- Quando você usa um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de bug com a seguinte mensagem a qualquer momento no início ou durante uma sessão.

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

[CVADHELP-24891]

- Quando você usa uma máquina, a inicialização da sessão do usuário falha de forma intermitente. [CVADHELP-23922]
- Durante a reconexão de uma sessão do ICA, a janela de chat de um aplicativo de mensagens de terceiros pode aparecer automaticamente em primeiro plano. [CVADHELP-24000]
- O processo `Wfshell.exe` pode falhar quando você copia e cola arquivos de uma estação de trabalho local na sessão da Citrix para VDA LTSR 2203. [CVADHELP-24146]
- Quando você usa um Windows 10 VDA versão 2308, o processo `ctxappvservice.exe` pode falhar. [CVADHELP-24575]
- A cópia do conteúdo de um aplicativo Microsoft Visio ou Visio publicado em uma área de trabalho para um aplicativo no dispositivo do usuário pode falhar. [CVADHELP-23647]
- O WebSocketService (serviço WebSocker de redirecionamento de vídeo HTML5) pode falhar. [CVADHELP-23917]
- Um aplicativo definido na metade esquerda do monitor esquerdo aparece incorretamente nesse centro da tela depois que você se reconecta ao usar o Virtual Apps and Desktops 2203 LTSR, o aplicativo Citrix Workspace 2203 LTSR CU3 (2303 ou 2205) e o VDA 2203 LTSR com Windows 11 22h2. [CVADHELP-23878]

VDA para SO multissessão

- O processo `WebSocketService.exe` pode consumir mais memória do que o esperado nos VDAs. [CVADHELP-23870]
- `CSEngine.exe` está consumindo mais memória do que o esperado no VDA. [CVADHELP-19916]
- Um impasse no Broker Agent impede que as máquinas se registrem novamente em uma alteração de IP do DNS. [CVADHELP-18952]
- O processo `WebSocketService.exe` falha ao iniciar após a reinicialização do VDA. [CVADHELP-24771]
- Quando você usa um VDA versão LTSR 2203 CU 4.1, o VDA pode realizar uma verificação de bug com a seguinte mensagem a qualquer momento no início ou durante uma sessão.
  `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys`
  [CVADHELP-24891]

- Alguns processos do aplicativo Citrix Workspace podem não fechar conforme o esperado quando são executados em uma sessão de aplicativo publicada. [CVADHELP-24225]
- No Server 2019 VDA versão LTSR 2203 CU3, `WmiPrvSE.exe` falha. [CVADHELP-24436]
- O processo `Wfshell.exe` pode falhar quando você copia e cola arquivos de uma estação de trabalho local na sessão da Citrix para VDA LTSR 2203. [CVADHELP-24146]
- O processo dos Serviços de Terminal pode falhar após uma reconexão do ACR. [CVADHELP-24364]
- No Windows Server 2022, se um mouse for movido para uma posição dedicada pelo aplicativo ou sistema operacional, você não poderá movê-lo para a posição novamente até que o mouse seja movido para outro local pelo aplicativo ou sistema operacional. [CVADHELP-24444]
- A caixa de diálogo **Mensagem de aviso de tempo ocioso expirado** não aparece na sessão do ICA no OS VDA 2022, embora o limite de tempo de **Sessão ociosa** entre em vigor. [CVADHELP-24646]
- A cópia do conteúdo de um aplicativo Microsoft Visio ou Visio publicado em uma área de trabalho para um aplicativo no dispositivo do usuário pode falhar. [CVADHELP-23647]

Profile Management

- A documentação do Profile Management 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Linux VDA

- A documentação do Linux VDA 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Session Recording

- A documentação do Session Recording 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Workspace Environment Management

- A documentação do Workspace Environment Management 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Citrix Provisioning

- A documentação do Citrix Provisioning 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Serviço de autenticação federada

- A documentação do Federated Authentication Service 2402 LTSR fornece informações específicas sobre as atualizações nesta versão.

Requisitos do sistema

August 22, 2024

Introdução

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

Revise Preparar a instalação antes de iniciar uma instalação.

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

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

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

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

Requisitos de hardware

Os valores de RAM e espaço em disco são além dos requisitos para a imagem do produto, sistema operacional e outros softwares no computador. Seu desempenho varia, dependendo da sua configu-

ração. 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	8 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 Core 2022
- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter, e com a opção Server Core
- Windows Server 2016, edições Standard e Datacenter, e com a opção Server Core

Requisitos:

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

Bancos de dados

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

- SQL Server 2022, edições Express, Standard e Enterprise.
- SQL Server 2019, edições Express, Standard e Enterprise.
- SQL Server 2017, edições Express, Standard e Enterprise.
  - Para novas instalações: por padrão, o SQL Server Express 2017 com atualização cumulativa 16 é instalado ao instalar o Controller, se uma instalação existente suportada do SQL Server não for detectada.
  - Para atualizações, nenhuma versão existente do SQL Server Express é atualizada.
- SQL Server 2016 SP2, edições Express, Standard e Enterprise.

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

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

- Espelhamento de banco de dados do SQL Server

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

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

- Ao instalar um 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:

- Bancos de dados
- CTX114501 lista os bancos de dados com suporte mais atual
- Orientação de dimensionamento do banco de dados
- Cache do host local

Web Studio

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

Sistemas operacionais compatíveis:

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

Citrix Director

Sistemas operacionais compatíveis:

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

Requisitos:

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

Citrix Profile Management:

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

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

- System Center 2012 R2 Operations Manager

Navegadores compatíveis para visualização do Director:

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

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

Virtual Delivery Agent (VDA) para SO de sessão única

Sistemas operacionais compatíveis:

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

Requisitos:

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

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

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

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

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

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

Virtual Delivery Agent (VDA) para SO multissessão

Sistemas operacionais compatíveis:

- Windows 11 (compatível somente com Citrix DaaS)
- Windows 10 (somente x64; compatível somente com o Citrix DaaS), qualquer versão que esteja atualmente no suporte principal.

- Windows Server 2022
- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter

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

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

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

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

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

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

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

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

Recursos de virtualização e hosts

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

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

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

Hipervisores compatíveis:

- **XenServer (anteriormente Citrix Hypervisor)**

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

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

- **Microsoft System Center Virtual Machine Manager**

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

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

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

- **Nutanix Acropolis**

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

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

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

  Não há suporte para 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 a AWS para provisionar máquinas virtuais, consulte Ambientes de virtualização da Amazon Web Services.

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

- **Microsoft Azure Resource Manager**

  Para obter informações sobre como usar Microsoft Azure Resource Manager para provisionar máquinas virtuais, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

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

  Para obter informações sobre como usar as soluções de nuvem e parceiros da Nutanix, consulte Soluções de nuvem e parceiros da Nutanix.

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

  Para obter informações sobre o uso de soluções de nuvem e parceiros do VMware, consulte Soluções de nuvem e parceiros do VMware.

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

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

Níveis funcionais do Active Directory

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

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

HDX

Áudio

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

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

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

HDX e entrega do Windows Media

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

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

HDX 3D Pro

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

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

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

Veja https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2402-ltsr/graphics/hdx-3d-pro.

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

Unidade de processamento gráfico (GPU):

- Para aceleração gráfica virtualizada usando a API NVIDIA GRID, você pode usar o HDX 3D Pro com todas as GPUs NVIDIA GRID com suporte pelo software NVIDIA Virtual GPU (vGPU) versão 13 ou superior, consulte https://docs.nvidia.com/grid/index.html.
  Para obter uma lista detalhada de hipervisores e hardware compatíveis, consulte a documentação do software NVIDIA vGPU.
- A aceleração gráfica virtualizada tem suporte na família de processadores Intel Xeon E3 de plataformas gráficas de data center e na série Intel Data Center GPU Flex. Para obter mais informações, consulte Série GPU Flex.
- As GPUs AMD são compatíveis com a virtualização MxGPU da AMD. Para obter mais informações sobre o hardware compatível, consulte a documentação da AMD.

Dispositivo do usuário:

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

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

Servidor de impressão universal

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.

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.

Ambientes de virtualização do Microsoft System Center Virtual Machine Manager

August 22, 2024

Siga estas instruções se você usa o Hyper-V com Microsoft System Center Virtual Machine Manager (VMM) para fornecer máquinas virtuais.

Esta versão oferece suporte às versões do VMM listadas em Requisitos do sistema.

> **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.

Provisionar o 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.

Considerações

Considere o seguinte:

- Não há suporte para a carga de trabalho multissessão do Windows 10 Enterprise e a carga de trabalho multissessão do Windows 11 Enterprise.
- O suporte para o gerenciamento do cluster Azure Stack HCI 23H2 virá com o SCVMM 2025.

Integrar o Azure Stack HCI ao SCVMM

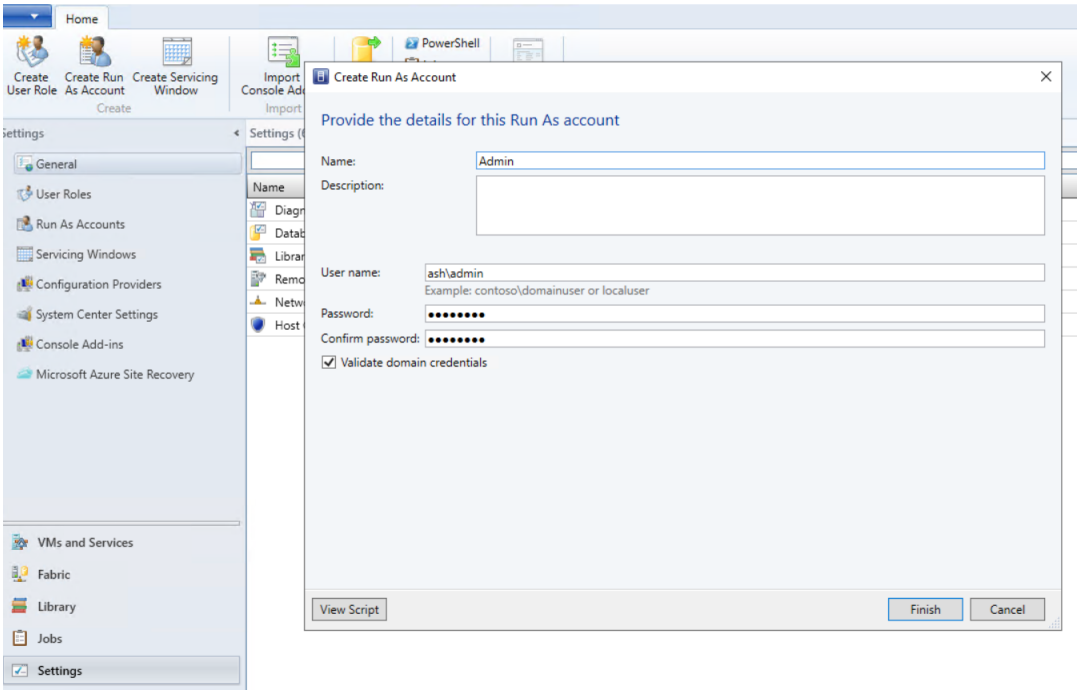
Para integrar o Azure Stack HCI ao SCVMM, você precisa primeiro criar um cluster do Azure Stack HCI e, em seguida, integrar esse cluster ao SCVMM.

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.

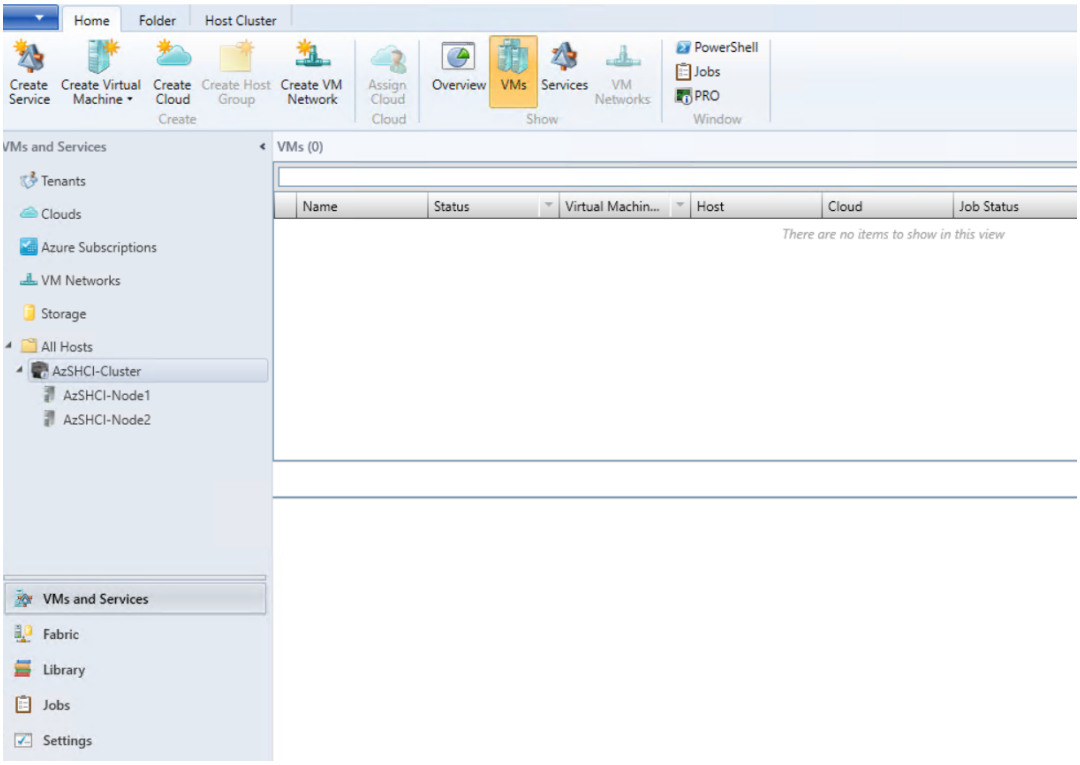
b) Na página **Settings** do console do VMM, crie uma conta Executar como.



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
```

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 no Web Studio e, em seguida, crie um catálogo de máquinas do MCS.

O que fazer a seguir

- Instalar componentes principais
- Instalar VDAs
- Criar um site
- Para criar e gerenciar uma conexão no SCVMM, consulte Conexão com o Microsoft System Center Virtual Machine Manager.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

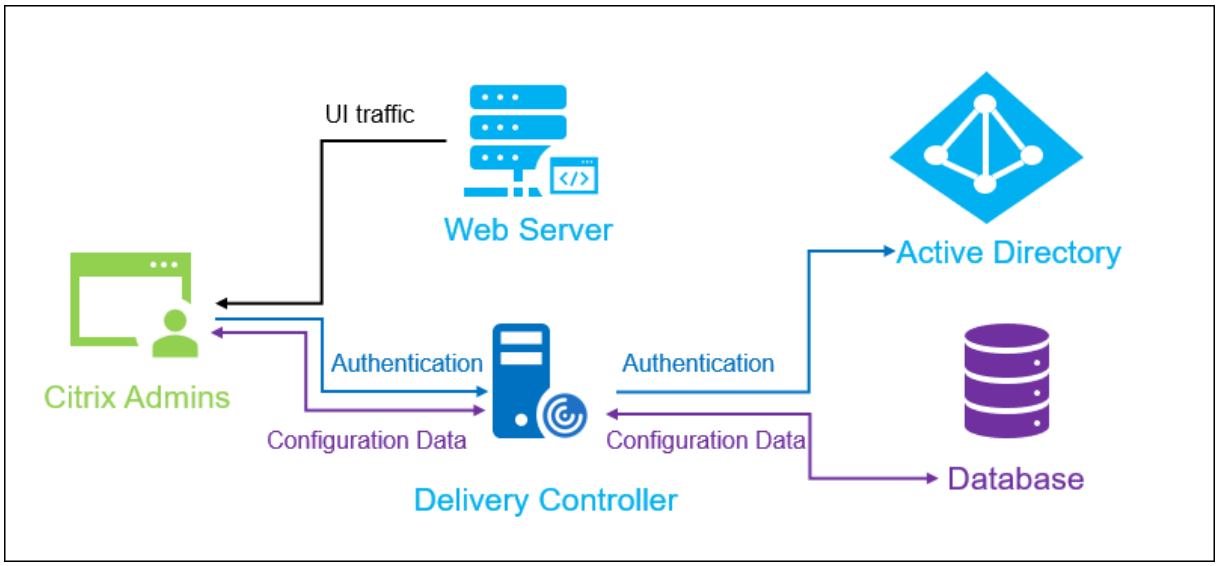
Instalar o Web Studio

August 23, 2024

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.

Para configurar uma implantação do Web Studio com balanceamento de carga, consulte este artigo.

Novos recursos disponíveis no Web Studio

Veja o artigo Novidades.

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

Navegadores com suporte:

- Microsoft Edge 92
- Firefox ESR (Extended Support Release) 90
- Google Chrome 92
- Safari 14

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

Pré-requisitos

Esta versão do Web Studio é compatível com 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.

Limitações conhecidas

Se você usa o Web Studio e o Citrix Studio de forma intercambiável, considere a seguinte limitação: um modelo criado no Web Studio não é exibido no Citrix Studio e vice-versa. Isso ocorre porque o Web Studio usa um banco de dados diferente do Citrix Studio para armazenar modelos. Como solução alternativa, crie uma política a partir de um modelo no Web Studio e, em seguida, crie um modelo a partir dessa política no Citrix Studio, e vice-versa.

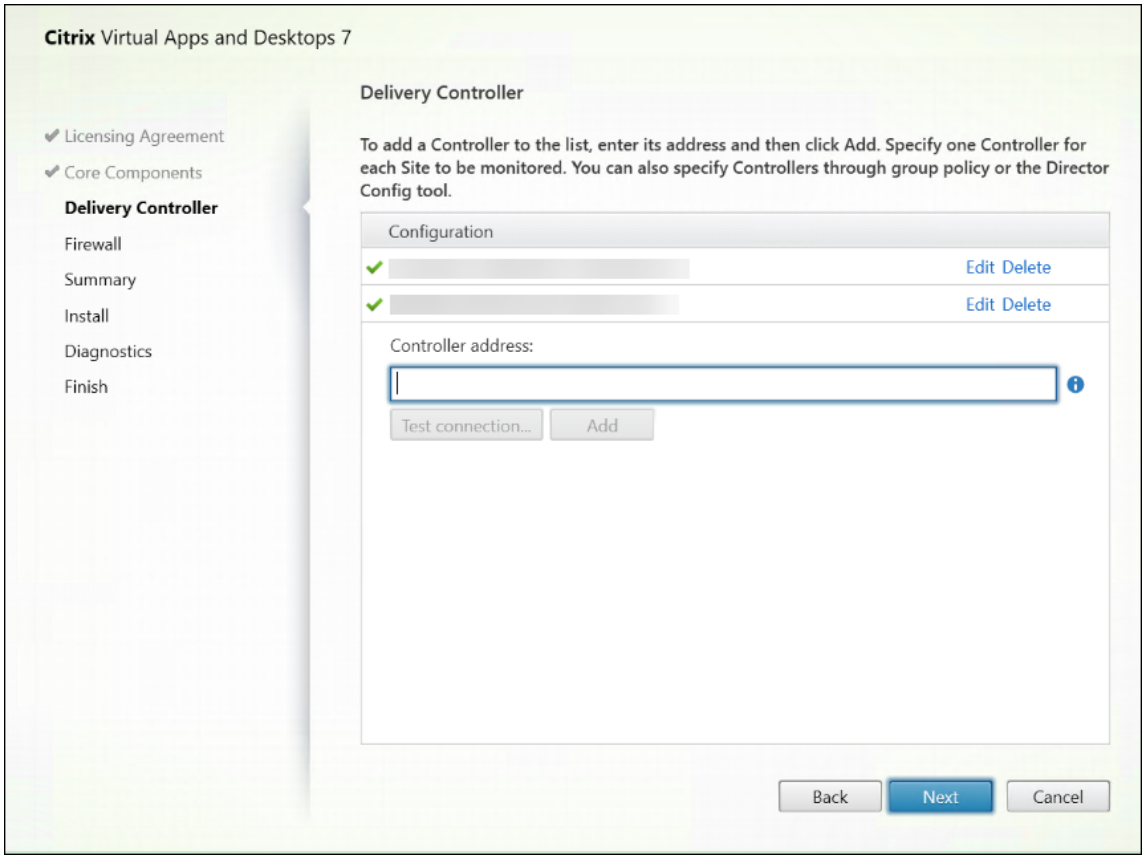
- Para garantir uma instalação bem-sucedida do Web Studio, não altere o nome do site padrão (**Default Web Site**) no Gerenciador de Serviços de Informações da Internet (IIS). Qualquer alteração no nome do site padrão resultará em falhas na instalação.

Instalar o Web Studio

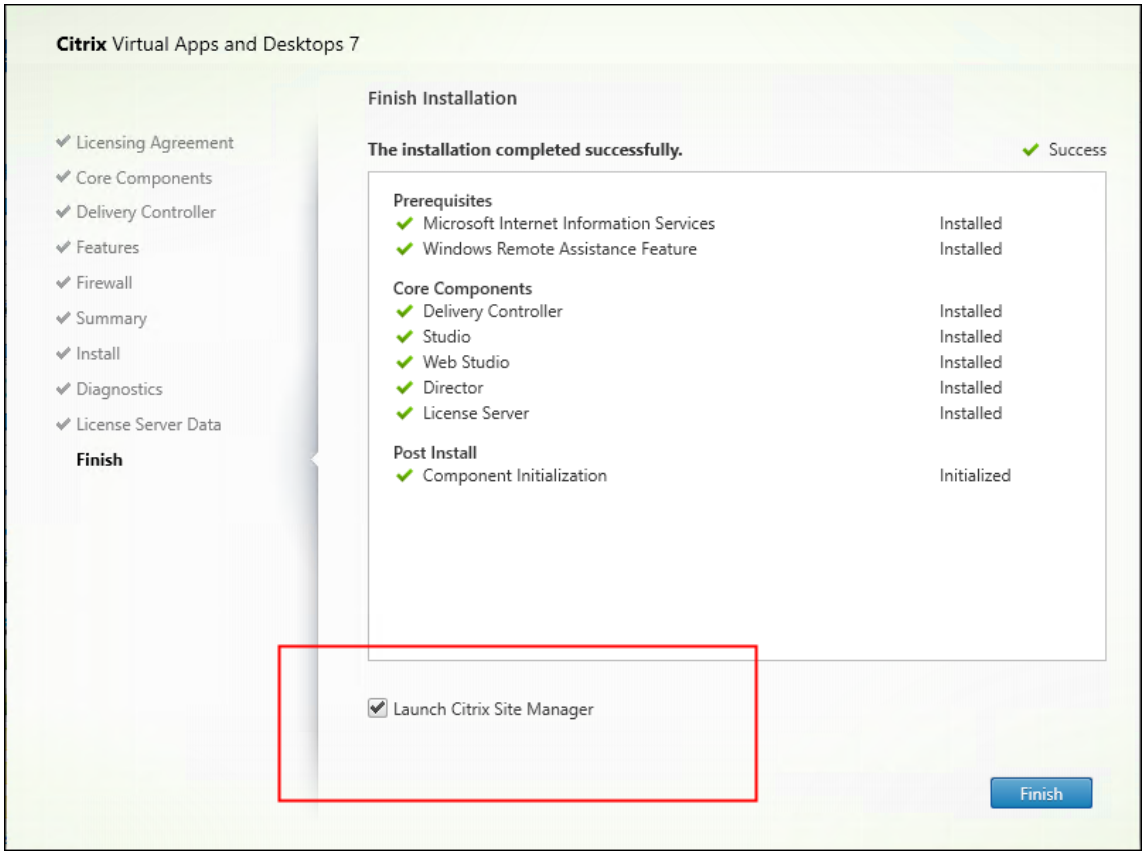
As informações a seguir são um complemento à orientação em Instalar componentes principais. Para instalar o Web Studio:

- 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.

> - Para ver todos os parâmetros com suporte, execute `StudioConfig.exe --help`.

Configurar o Web Studio como um proxy para Delivery Controllers (opcional)

Por padrão, ao gerenciar sua implantação usando o console do Web Studio, você se conecta ao servidor do Web Studio e aos Delivery Controllers por meio do navegador da Web. 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. No servidor Web Studio, execute o Windows PowerShell como administrador.
2. Execute o comando a seguir para substituir `fqdn_of_webstudio_machine` pelo FQDN do seu servidor Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

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

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

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

> **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/Studio`.

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)

Conexão com o Microsoft Azure

August 22, 2024

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

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

> **Nota:**
>
> Antes de criar uma conexão com o Microsoft Azure, você precisa concluir a configuração da sua conta do Azure como um local de recursos. Consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Criar entidades de serviço e conexões

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

- Criar uma entidade de serviço e uma conexão juntas usando o Web Studio
- Criar uma conexão usando uma entidade de serviço criada anteriormente

Esta seção mostra como realizar essas tarefas:

- Criar uma entidade de serviço e uma conexão usando o Web Studio
- Criar uma entidade de serviço usando o PowerShell
- Obter o segredo do aplicativo no Azure
- Criar uma conexão usando uma entidade de serviço existente

Considerações

- A Citrix recomenda usar o 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.

Criar uma entidade de serviço e uma conexão usando o Web Studio

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

No Web Studio, você pode criar uma entidade de serviço e uma conexão em um único fluxo de trabalho. As entidades de serviço dão às conexões o acesso aos recursos do Azure. Quando você se autentica no Azure para criar uma entidade de serviço, um aplicativo é registrado no Azure. Uma chave secreta (chamada segredo do cliente ou segredo do aplicativo) é criada para o aplicativo registrado. O aplicativo registrado (nesse caso, uma conexão) usa o segredo do cliente para se autenticar no Azure AD.

Antes de começar, verifique se você atende aos seguintes 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.

Use o assistente **Add Connection and Resources.** para criar uma entidade de serviço e uma conexão juntas:

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.

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

Na lista **Add Connection and Resources**, selecione a conexão para exibir os detalhes. A guia **Details** mostra a ID do aplicativo.

Criar uma entidade de serviço usando o PowerShell

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

Verifique se você tem esses itens prontos:

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

As etapas detalhadas são as seguintes:

Conecte-se à sua assinatura do Azure Resource Manager.

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

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

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

2. Crie o aplicativo em seu locatário do AD.

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

3. Crie uma entidade de serviço.

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

4. Atribua uma função à entidade de serviço.

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

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

Obter o segredo do aplicativo no Azure

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

As etapas detalhadas são as seguintes:

1. Obtenha o **ID do aplicativo** no Web Studio ou usando o PowerShell.
2. Faça login no portal do Azure.
3. No Azure, selecione **Azure Active Directory**.
4. Em **App registrations** no Azure AD, selecione o seu aplicativo.
5. Acesse **Certificates & secrets**.
6. Clique em **Client secrets**.

Criar uma conexão usando uma entidade de serviço existente

Se você já tem uma entidade de serviço, pode usá-la para criar uma conexão usando o Web Studio.

Verifique se você tem esses itens prontos:

- SubscriptionId
- ActiveDirectoryID (ID do locatário)
- ID do aplicativo
- Segredo do aplicativo

  Para obter mais informações, consulte Obter o segredo do aplicativo.
- Data de expiração do segredo

As etapas detalhadas são as seguintes:

No assistente **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.

Gerenciar entidades de serviço e conexões

Esta seção detalha como você pode gerenciar as entidades de serviço e conexões:

- Definir as configurações de limitação do Azure
- Habilitar o compartilhamento de imagens no Azure
- Adicionar locatários compartilhados a uma conexão usando Full Configuration
- Implementar o compartilhamento de imagens usando o PowerShell
- Gerenciar o segredo do aplicativo e data de expiração do segredo

Definir as configurações de 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.

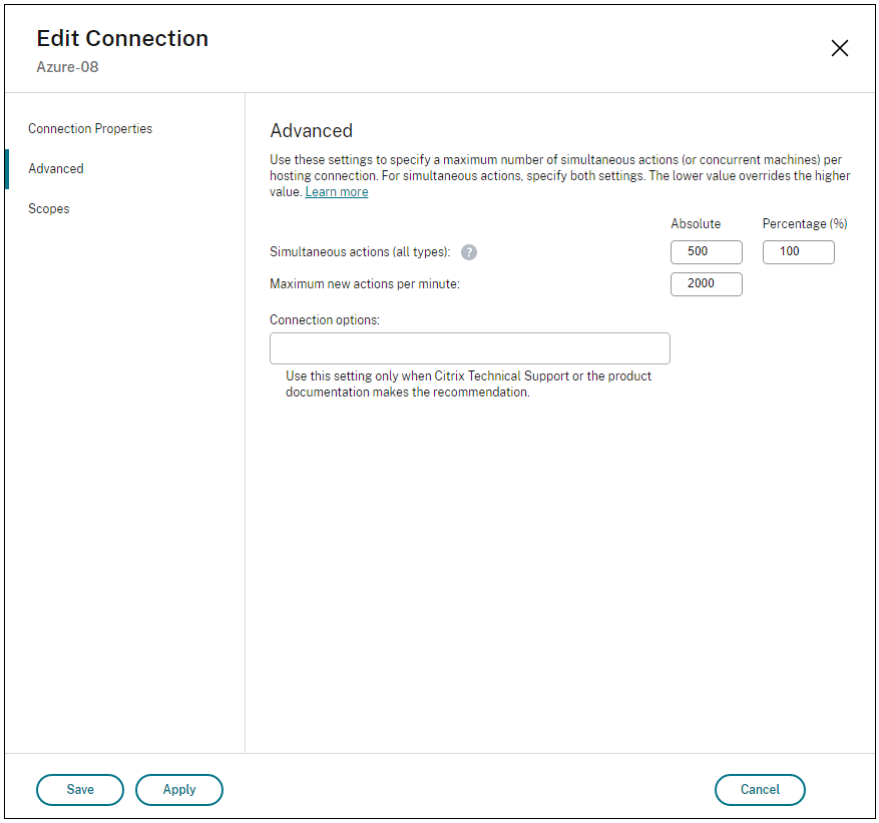
Para ajudar a mitigar esses problemas, você pode remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

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

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

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



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`.

Habilitar o compartilhamento de imagens no Azure

Ao criar ou atualizar catálogos de máquinas, você pode selecionar imagens compartilhadas de diferentes locatários do Azure e assinaturas (compartilhadas através da Galeria de Computação do Azure). Para habilitar o compartilhamento de imagens dentro ou entre locatários, você deve aplicar as configurações necessárias no Azure:

- Compartilhar imagens com um locatário (entre assinaturas)
- Compartilhar imagens entre locatários

Compartilhar imagens com um locatário (entre assinaturas) Para selecionar uma imagem na Galeria de Computação do Azure que pertença a uma assinatura diferente, a imagem deve ser compartilhada com a entidade de serviço (SPN) dessa assinatura.

Por exemplo, se houver uma entidade de serviço (SPN 1) configurada no Studio como:

Entidade de serviço: SPN 1

Assinatura: subscription 1

Locatário: tenant 1

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

Assinatura: subscription 2

Locatário: tenant 1

Se você quiser compartilhar a imagem em subscription 2 com subscription 1 (SPN 1), vá para subscription 2 e compartilhe o grupo de recursos com SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em função (RBAC) do Azure. O Azure RBAC é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o Azure RBAC, consulte o documento da Microsoft O que é o RBAC do Azure (controle de acesso baseado em função do Azure)?. Para conceder acesso, você atribui funções às entidades de serviço no escopo do grupo de recursos com a função de Colaborador. Para atribuir funções do Azure, você deve ter permissão `Microsoft.Authorization/roleAssignments/write`, como Administrador de Acesso do Usuário ou Proprietário. Para obter

mais informações sobre como compartilhar imagens com outro SPN, consulte o documento da Microsoft Atribuir funções do Azure usando o portal do Azure.

Para obter informações sobre como selecionar uma imagem de uma assinatura diferente, consulte Selecionar uma imagem de uma assinatura diferente.

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

Por exemplo, se houver dois locatários (locatário 1 e locatário 2) e você quiser compartilhar sua galeria de imagens com Tenant 1:

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

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
       client_id=<Application (client) ID>&response_type=code&
       redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   Para obter mais informações, consulte Dar acesso ao locatário 2.
3. Dê ao aplicativo acesso ao grupo de recursos em Tenant 2. Faça login como Tenant 2 e dê ao registro do aplicativo acesso ao grupo de recursos que tem a imagem da galeria. Para obter mais informações, consulte Autenticar solicitações entre locatários.

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

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

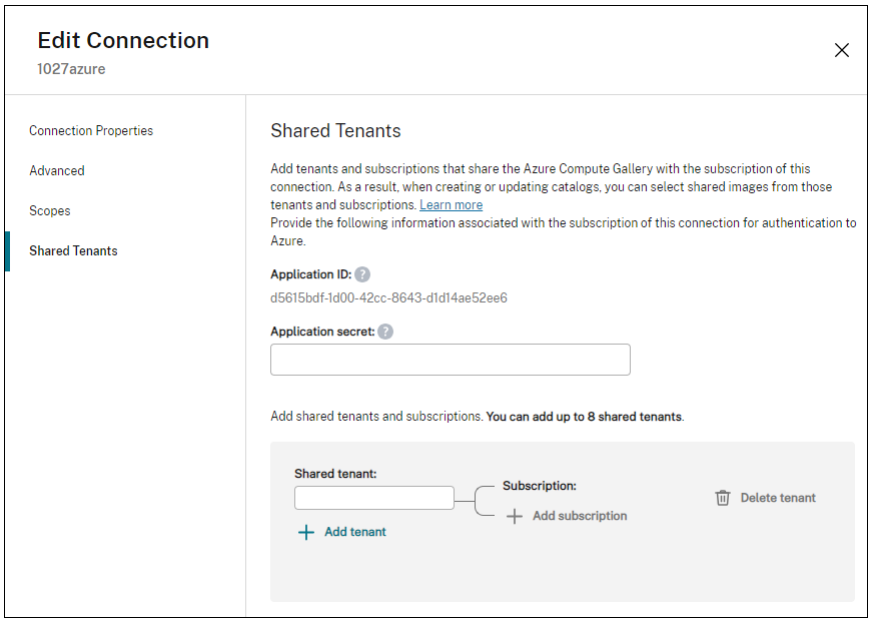
Adicionar locatários compartilhados a uma conexão usando Full Configuration

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

> **Nota:**
>
> Verifique se você definiu as configurações necessárias no Azure para permitir o compartilhamento de imagens entre locatários. Para obter mais informações, consulte Compartilhar imagens entre locatários.

Siga estas etapas para a conexão:

1. No Web Studio, selecione **Hosting** no painel esquerdo.
2. Selecione a conexão e selecione **Edit Connection** na barra de ações.



3. Em **Shared Tenants**, faça o seguinte:
   - Forneça o ID do aplicativo e o segredo do aplicativo associado à assinatura da conexão. O Citrix Virtual Apps and Desktops usa essas informações para se autenticar no Azure AD.
   - Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura da conexão. Você pode adicionar até 8 locatários compartilhados e 8 assinaturas para cada locatário.
4. Quando terminar, selecione **Apply** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Implementar o compartilhamento de imagens usando o PowerShell

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

- Selecionar uma imagem de uma assinatura diferente

- Atualizar propriedades personalizadas da conexão de hospedagem com IDs de locatários compartilhados
- Selecionar uma imagem de um locatário diferente

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

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

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

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados da assinatura compartilhada.

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

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

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

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

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

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

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\sigtestdef.imagedefinition"
```

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

   - 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/.

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

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
```

Por exemplo:

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

> **Nota:**
>
> Você pode adicionar mais de um locatário. Cada locatário pode ter mais de uma assinatura.

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

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


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

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados da assinatura compartilhada.

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

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

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

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

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

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

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

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

   - 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/.

Gerenciar o segredo do aplicativo e data de expiração do segredo

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

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

1. Selecione **Azure Active Directory**.
2. Em **App registrations** no Azure AD, selecione o seu aplicativo.

3. Acesse **Certificates & secrets**.
4. Clique em **Client secrets > New client secret**.
5. Forneça uma descrição do segredo e especifique uma duração. Quando terminar, selecione **Add**.

   > **Nota:**
   >
   > Lembre-se de salvar o segredo do cliente porque você não pode recuperá-lo mais tarde.

6. Copie o valor do segredo do cliente e a data de expiração.
7. No Web Studio, edite a conexão correspondente e substitua o conteúdo no campo **Application secret** e **Secret expiration date** pelos valores copiados.

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

1. No assistente **Add Connection and Resources**, clique com o botão direito do mouse em uma conexão e clique em **Edit Connection**.
2. Na página **Connection Properties**, clique em **Secret expiration date** para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

Permissões necessárias do Azure

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

Permissões mínimas

As permissões mínimas oferecem melhor controle de segurança. No entanto, novos recursos que exigem permissões adicionais falham 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",
```


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

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
```

Criar, atualizar ou excluir VMs Crie um catálogo de máquinas 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",
```

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

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

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


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

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
```

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

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
```

- Se você usar o grupo de recursos gerenciados pela Citrix:

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

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

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
```

- Se você usar o suporte a host dedicado do Azure:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

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

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

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

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
```

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

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


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"
```

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",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```

Configurar as permissões de conexão de host do Azure necessárias

Você pode configurar facilmente todas as permissões mínimas necessárias para uma conta de entidade de serviço ou de usuário no Azure vinculada a uma conexão de host para realizar todas as operações do MCS usando um modelo do ARM. Esse modelo do ARM automatiza o seguinte:

- Criação de uma função do Azure com as permissões mínimas necessárias para as operações.
- Atribuição dessa função a uma entidade de serviço existente do Azure no nível da assinatura.

Você pode implantar esse modelo do ARM usando o Portal do Azure ou os comandos do PowerShell. Para obter mais informações, consulte Modelo do ARM para operações do CVAD.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para obter informações específicas do Azure, consulte Criar um catálogo do Microsoft Azure

Mais informações

- Conexões e recursos
- Criar catálogos de máquinas

Gerenciamento de imagens (prévia)

August 22, 2024

Introdução

O processo de criação ou atualização do catálogo do MCS tem duas fases:

- Masterização: uma imagem de origem é convertida em uma imagem publicada
- Clonagem: novas VMs são criadas a partir da imagem publicada

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

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

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

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

> **Nota:**
>
> - Atualmente, esse recurso é aplicável aos ambientes de virtualização do Azure e da VMware.
> - Você pode criar um catálogo de máquinas do MCS sem usar imagens preparadas. Nesse caso, você não pode obter os benefícios do recurso.

Casos de uso

Alguns dos casos de uso da funcionalidade de gerenciamento de imagens são:

- *Gerenciamento de versões* —As versões de imagem permitem que você:
  - gerencie diferentes iterações ou atualizações em uma imagem específica.
  - mantenha várias versões de uma imagem para finalidades diferentes.
- *Agrupamento lógico* —Você pode criar várias definições de imagem para:
  - agrupar logicamente versões de imagens com base em vários critérios, como projeto, departamento ou aplicativo e tipo de área de trabalho.
  - gerenciar imagens com mais eficiência dentro de uma organização.

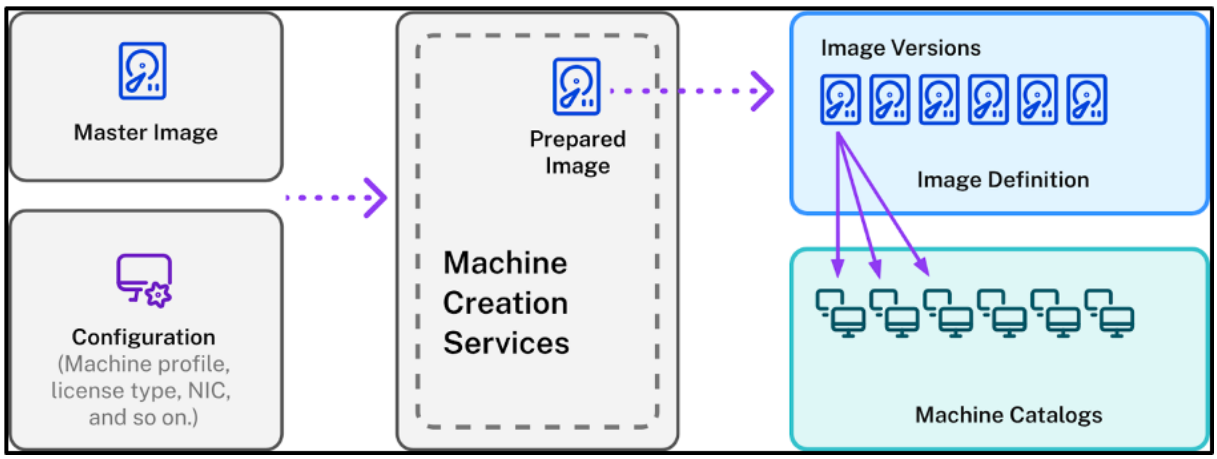
O que é uma imagem preparada?

Com a funcionalidade de gerenciamento de imagens, o MCS separa a fase de masterização do fluxo de trabalho geral de criação ou atualização do catálogo e divide o processo em dois estágios:

1. Crie imagens preparadas a partir de uma única imagem de origem.
2. Use a imagem preparada para criar ou atualizar um catálogo de máquinas do MCS.

Você pode criar as imagens preparadas com antecedência. Você pode usar uma única imagem preparada para criar ou atualizar vários catálogos de máquinas provisionados pelo MCS.

Entenda como uma imagem preparada é usada em vários catálogos de máquinas do MCS quando você usa o Web Studio a partir da imagem:



Definição de imagem: as definições de imagem são um agrupamento lógico de versões de uma imagem. A definição de imagem contém informações sobre:

- por que a imagem foi criada

- para que serve o sistema operacional
- outras informações sobre o uso da imagem.

Um catálogo não é criado a partir de uma definição de imagem, mas das versões de imagem que são criadas com base na definição de imagem.

Versão da imagem: as versões da imagem gerenciam as versões para a definição de imagem. Uma definição de imagem pode ter várias versões de imagem. Use as versões de imagem como imagens preparadas para criar ou atualizar um catálogo.

Como alternativa, se você quiser usar os comandos do PowerShell para criar um esquema de provisionamento para criar ou atualizar um catálogo, deverá criar uma especificação de versão de imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para seu ambiente.

Participar do Tech Preview

Se você estiver interessado em participar do Tech Preview, forneça suas informações de contato aqui.

Ajudaremos você a configurar o ambiente de teste e forneceremos suporte técnico, se necessário.

Requisito

- Para a imagem mestre do Windows, somente imagens do VDA com a versão 2311 e posterior e o MCS/IO habilitado são permitidas.

Limitações

Atualmente, o recurso não oferece suporte ao seguinte:

- Várias NICs no Azure
- Recurso de disco de dados persistente
- Hibernação para várias sessões
- Alteração do tipo de imagem

Gerenciamento do ciclo de vida de imagens usando o Web Studio

O ciclo de vida da imagem quando você usa o Web Studio é:

1. Crie uma imagem preparada: crie uma definição de imagem e sua versão inicial da imagem.
2. Crie versões de imagem a partir da versão inicial da imagem.

3. Use uma versão de imagem como uma imagem preparada para criar catálogos.
4. Atualize um catálogo de máquinas com uma imagem preparada diferente.
5. Gerencie as definições e versões da imagem: edite o nome e a descrição das versões da imagem e a descrição de uma definição de imagem.
6. Exclua uma versão da imagem.
7. Exclua uma definição de imagem.

Como alternativa, você também pode gerenciar imagens usando o PowerShell. Consulte Gerenciamento do ciclo de vida de imagens usando o PowerShell.

Criar ou atualizar um catálogo usando uma imagem preparada

Crie imagens preparadas e use as imagens preparadas para criar ou atualizar um catálogo de máquinas do MCS usando:

- O Web Studio
- Os comandos do PowerShell

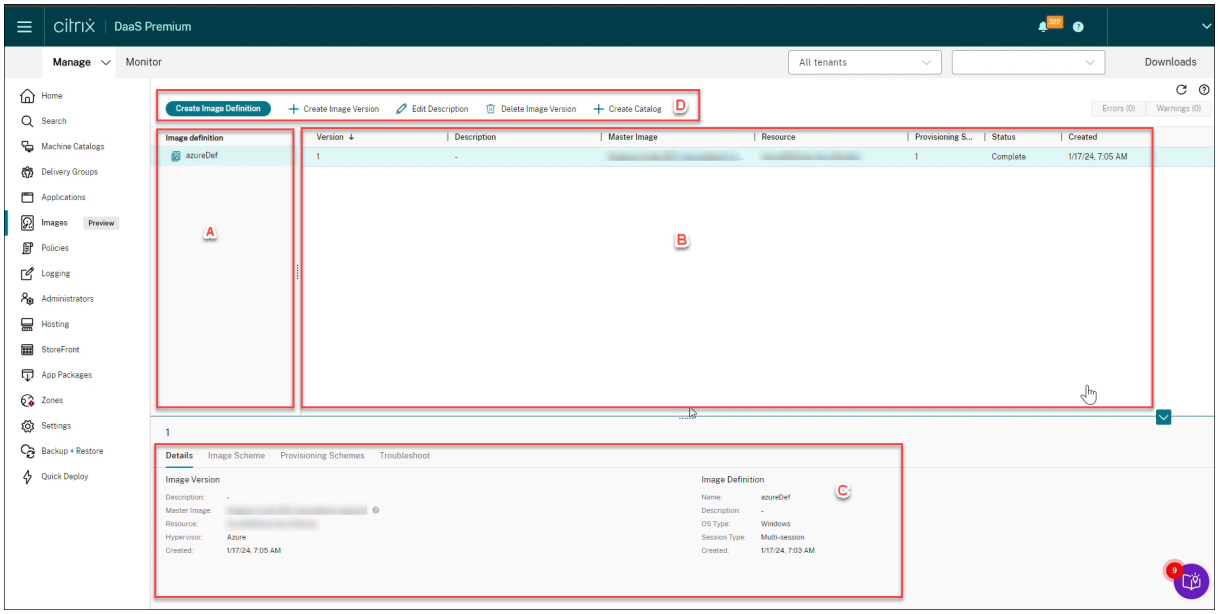
Usar o Web Studio

Veja os tópicos a seguir:

- Entender o nó Imagens
- Criar uma definição de imagem e uma versão inicial da imagem
- Criar versões de imagem
- Criar um catálogo de máquinas a partir do nó Imagens
- Criar um catálogo de máquinas a partir do nó Catálogos de computadores
- Atualizar um catálogo de máquinas com uma imagem preparada diferente
- Gerenciar as definições e versões da imagem

Entender o nó Imagens

Use o nó **Imagens** para criar e gerenciar imagens preparadas pelo MCS. Sua visão principal é dividida em quatro partes:



Rótulo	Parte	Descrição
A	Definições de imagem	Lista as definições de imagem criadas anteriormente.
B	Versões de imagem	Exibe as versões de imagem da definição de imagem selecionada.
C	Detalhes	• A guia **Detalhes** exibe informações detalhadas sobre a definição ou versão de imagem selecionada, como imagem mestre, recurso, hipervisor, nome da definição de imagem, tipo de sistema operacional e tipo de sessão. • A guia **Esquema de imagem** exibe informações sobre o modelo usado para preparar imagens, como disco rígido, tamanho da máquina, tipo de licença, conjunto de criptografia de disco, perfil da máquina e assim por diante. • A guia **Esquemas de provisionamento** exibe o nome do esquema de
D	Barra de ação	Lista as ações que você pode realizar nas definições e versões de imagem, como **Criar versão da imagem**, **Editar descrição**, **Excluir versão da imagem** e **Criar catálogo**.

Criar um catálogo de máquinas usando a imagem preparada

As principais etapas para criar um catálogo de máquinas do MCS usando a imagem preparada são:

1. Crie a definição de imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo.

Criar uma definição de imagem e uma versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. Entre no Web Studio e selecione o nó **Imagens**. Clique em **Avançar** na página de **introdução**.
2. Na página **Definição de imagem**, especifique o **Tipo de sistema operacional** e o **Tipo de sessão** para a definição de imagem.
3. Na página **Imagem**, selecione **Recursos** e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecione um perfil de máquina.

   > **Nota:**
   >
   > Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. (Somente para Azure) Na página **Tipos de armazenamento e licenças**, selecione o tipo de armazenamento e licença a ser usado como parte do processo de preparação da imagem.

   > **Nota:**
   >
   > Se você selecionar um perfil de máquina na página **Imagem**, o tipo de licença do perfil da máquina será pré-selecionado com base na configuração do perfil.

5. Na página **Especificações da máquina**:

   - Para o Azure, selecione um tamanho de máquina. Se você selecionar um perfil de máquina na página **Imagem**, o tamanho da máquina do perfil da máquina será selecionado por padrão.
   - Para a VMware, se você selecionar um perfil de máquina, poderá ver a contagem de CPUs virtuais derivada do perfil da máquina e ela permanecerá inalterável. Se você não selecionar um perfil de máquina, poderá ver somente o tamanho da memória derivado da imagem mestre.

6. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada.

   Para a VMware, se você não selecionar um perfil de máquina, a NIC associada à imagem mestre será selecionada por padrão. Se você selecionar um perfil de máquina, as NICs serão derivadas do perfil de máquina e a contagem será imutável.

   > **Nota:**
   >
   > Várias NICs não são permitidas no Azure.

7. (Somente para Azure) Na página **Configurações do disco**, selecione a chave de criptografia gerenciada pelo cliente (CMEK). Se o perfil de máquina não tiver uma CMEK, mas a imagem mestre tiver, ele pré-selecionará a CMEK da imagem mestre.
8. Na página **Descrição da versão**, insira uma descrição para a versão inicial da imagem criada.
9. Na página **Resumo**, verifique os detalhes da definição de imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição de imagem. Clique em **Finish**.

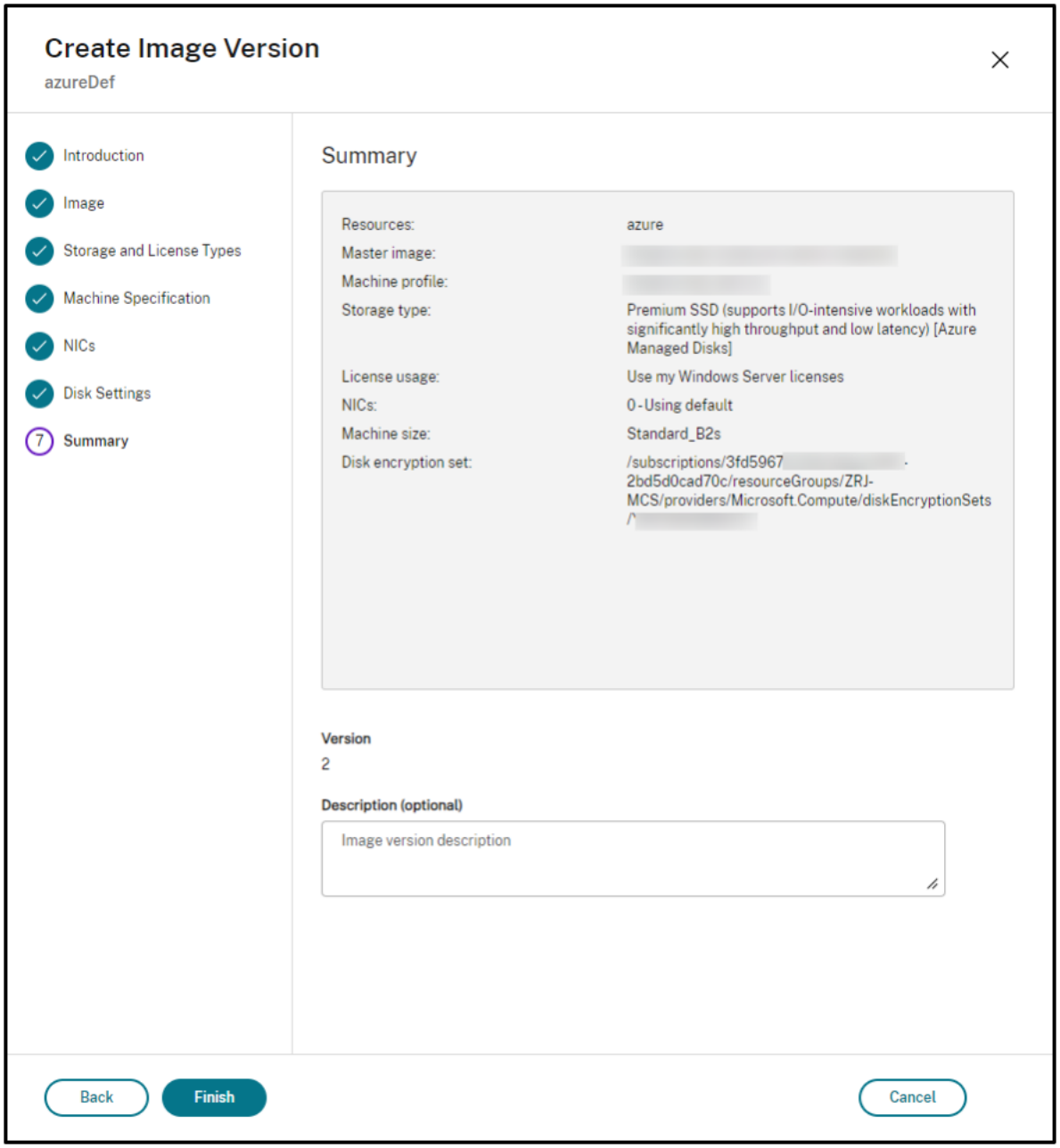
Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações em uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para finalidades diferentes.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Nota:**
>
> A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá até o nó **Imagens**, selecione uma versão da imagem e selecione **Criar versão da imagem**.
2. Se você quiser que a configuração da versão de imagem seja diferente da versão inicial da imagem configurada, defina as configurações nas páginas **Imagem**, **Armazenamento e tipos de licença**, **Especificação da máquina**, **NICs** e **Configurações do disco** da caixa de diálogo **Criar versão da imagem**.
3. Adicione uma descrição para a versão da imagem. Clique em **Finish**.



Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Como alternativa, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de computadores**, vinculando à opção de imagem preparada no fluxo de trabalho de criação do catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de computadores

Para criar um catálogo de máquinas do MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página de **introdução**.
2. Na página **Experiência de área de trabalho**, selecione a experiência de área de trabalho necessária.
3. Da página **Imagem** até a página **Configurações do disco**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. (Para Azure) Na página **Grupo de recursos**, você pode escolher criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos desse catálogo.
5. Conclua as configurações nas páginas a seguir.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Finish**.
7. Acesse o nó **Catálogos de computadores** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de computadores

Para criar um catálogo de máquinas do MCS a partir do nó **Catálogos de computadores**, faça o seguinte:

1. Clique em **Catálogos de computadores** no painel de navegação esquerdo.
2. Clique em **Criar catálogo de máquinas**. A página **Configuração do catálogo de máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de máquina** e **Gerenciamento de máquinas**.
3. Na página **Imagem**:

    a) Selecione **Imagem preparada**.
    b) Em **Imagem preparada**, selecione uma versão da imagem de uma definição de imagem.
    c) Clique no nome da versão da imagem. Para exibir mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
    d) Se a versão da imagem selecionada estiver configurada com um perfil de máquina, selecione um perfil de máquina. Se a versão da imagem selecionada não estiver configurada com um perfil de máquina, você não poderá optar por usar um perfil de máquina.

4. Defina as configurações nas páginas a seguir.
5. Na página **Configurações do disco**, se a imagem preparada selecionada usar um conjunto de criptografia de disco, você não poderá remover o conjunto de criptografia, mas poderá alterar a chave para outra chave de criptografia.
6. (Para Azure) Na página **Grupo de recursos**, você pode escolher criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos desse catálogo.
7. Conclua as configurações nas páginas a seguir.
8. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Finish**.

Atualizar um catálogo de máquinas com uma imagem preparada diferente

Para atualizar um catálogo de máquinas do MCS existente com uma imagem preparada diferente, faça o seguinte:

1. Clique em **Catálogos de computadores** no painel de navegação esquerdo e selecione um catálogo de máquinas que você deseja atualizar. Clique com o botão direito do mouse e selecione **Alterar imagem preparada**.
2. Na página **Imagem**, selecione uma imagem preparada.
3. Na página **Estratégia de implantação**, selecione quando você deseja atualizar esse catálogo com a imagem preparada selecionada.
4. Na página **Resumo**, verifique os detalhes. Clique em **Finish**.

Você pode ver o histórico das alterações de imagem feitas em um catálogo. Para ver o histórico, faça o seguinte:

1. Selecione um catálogo de máquinas.
2. Na guia **Propriedades do modelo**, no campo **Imagem preparada**, clique em **Exibir histórico da imagem**.

Gerenciar as definições e versões da imagem

Você pode editar e excluir as definições e versões de imagem para gerenciar o uso de várias versões e definições de imagem criadas.

Editar uma definição de imagem Você pode editar o nome e a descrição de uma definição de imagem.

Para editar uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Editar definição de imagem**.

Editar versão da imagem Você pode editar a descrição de uma versão da imagem para especificar a finalidade dessa versão da imagem.

Para editar uma versão da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão da imagem e selecione **Editar descrição**.

Excluir uma versão da imagem Para excluir uma versão da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão da imagem e selecione **Excluir versão da imagem**.

> **Nota:**
>
> Você não poderá excluir uma versão da imagem se ela for usada por um catálogo de máquinas.

Excluir uma definição de imagem Para excluir uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Excluir definição de imagem**.

> **Nota:**
>
> Você não poderá excluir uma definição de imagem se ela contiver uma versão da imagem.

Gerenciamento do ciclo de vida de imagens usando o PowerShell Se você quiser usar os comandos do PowerShell para criar um esquema de provisionamento, deverá criar uma especificação de versão da imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para seu ambiente.

Especificação de versão da imagem mestre: uma especificação de versão da imagem mestre é uma imagem específica adicionada ou criada sob uma versão da imagem. Você pode adicionar uma imagem existente no hipervisor como especificação de versão da imagem mestre ou criar uma especificação de versão da imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para seu ambiente. A especificação da versão da imagem preparada pode ser usada para vários esquemas de provisionamento.

O ciclo de vida de uma imagem durante o uso dos comandos do PowerShell é:

1. Crie uma imagem:
    a) Crie uma definição de imagem.
    b) Crie uma versão da imagem.
    c) Adicione uma especificação de versão da imagem mestre.
    d) Crie uma especificação de versão da imagem preparada.
2. Crie um catálogo de máquinas do MCS usando uma especificação de versão de imagem preparada:
    a) Crie um catálogo de agentes.
    b) Crie um pool de identidades.
    c) Crie um esquema de provisionamento com o parâmetro da especificação de versão da imagem preparada Uid usando o comando `New-ProvScheme`.

d) Vincule o catálogo de agentes ao esquema de provisionamento.

3. Crie VMs no catálogo de máquinas do MCS.
4. Altere a especificação da versão da imagem preparada de um esquema de provisionamento usando o comando `Set-ProvScheme`.
5. Gerencie as definições e versões de imagem: edite as versões e definições de imagem.
6. Exclua um catálogo de máquinas do MCS: a ordem de exclusão é: especificação da versão da imagem preparada > especificação da versão da imagem mestre > versão da imagem > definição de imagem. Antes de excluir a especificação da versão da imagem, certifique-se de que a especificação da versão da imagem preparada não esteja associada a nenhum catálogo de máquinas do MCS.

Usar o PowerShell

Você pode fazer o seguinte usando os comandos do PowerShell:

- Criar uma imagem preparada
- Criar um catálogo usando a especificação de versão da imagem preparada
- Atualizar um catálogo usando uma especificação de versão da imagem preparada
- Excluir a definição da imagem, a versão da imagem e a especificação da versão da imagem preparada
- Gerenciar a definição e a versão de imagem
- Obter a definição de imagem, a versão da imagem, a especificação da versão da imagem preparada e os detalhes do esquema de provisionamento

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão da imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando o `Test-ProvImageDefinitionNameAv command`. Por exemplo,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,


```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
```

3. Crie uma versão da imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
```

4. Adicione uma especificação de versão da imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
Add-ProvImageVersionSpec -ImageDefinitionName image1 -
    ImageVersionNumber 1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
```

> **Nota:**
>
> Você pode adicionar somente uma especificação de versão da imagem mestre a uma versão da imagem para uma unidade de hospedagem.

5. Crie uma especificação de versão da imagem preparada a partir da especificação de versão da imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
```

> **Nota:**
>
> Uma unidade de hospedagem e um tipo de preparação podem ter somente uma instância preparada.

Exemplo do conjunto completo de comandos do Powershell para criar a definição de imagem, a versão da imagem e a especificação de versão da imagem preparada no Azure:

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
```



```
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
    virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
     Standard_B2ms.serviceoffering" -CustomProperties "<
     CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
     machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
     instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

Exemplo do conjunto completo de comandos do Powershell para criar a definição de imagem, a versão da imagem e a especificação de versão da imagem preparada na VMware:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

Nota:

- Todas as especificações da versão da imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão da imagem pode ter somente uma especificação de versão da imagem mestre e uma especificação de versão da imagem preparada.
- Todas as especificações da versão da imagem devem ter um perfil de máquina ou nenhuma das especificações da versão da imagem deve ter um perfil de máquina.
- Você não pode especificar um grupo de recursos ao criar uma especificação de versão da imagem.

Criar um catálogo usando uma especificação de versão da imagem preparada

Crie um catálogo de máquinas do MCS a partir da especificação da versão da imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
    int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
    Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
    >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
    TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
    <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
    VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
    NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
    Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
    string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
    CustomProperties <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

Exemplo do conjunto completo de comandos do Powershell para criar um catálogo no Azure:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.
    local" -IdentityPoolName "azurecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric
    " -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\
    azure\serviceoffering.folder\Standard_B2s.serviceoffering" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.
     com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
```



```
        XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
        StorageAccountType`" Value=`"StandardSSD_LRS`" /></
        CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
```

Exemplo do conjunto completo de comandos do Powershell para criar um catálogo na VMware:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.
    local" -IdentityPoolName "vmwarecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "
    Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
    -Scope @() -SecurityGroup @() -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
```

Atualizar um catálogo usando uma especificação de versão da imagem preparada

Você pode atualizar um catálogo usando o comando `Set-ProvSchemeImage`. Por exemplo,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
    <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
    PurgeJobOnSuccess]
```

Ou,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -
    ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
    ] [-PurgeJobOnSuccess]
```

Exemplo do conjunto completo de comandos do Powershell para atualizar um catálogo:


```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
    PreparationType -eq 'Mcs'"
Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

Excluir a definição da imagem, a versão da imagem e a especificação da versão da imagem preparada

Considere o seguinte antes de excluir uma definição de imagem, versão da imagem e especificação de versão da imagem preparada:

- Uma definição de imagem não poderá ser excluída se ela contiver qualquer versão da imagem.
- Uma versão da imagem não poderá ser excluída se ela contiver qualquer especificação de versão da imagem.
- Uma especificação de versão da imagem mestre não poderá ser excluída se for usada por qualquer outra especificação de versão da imagem preparada.
- Uma especificação de versão da imagem preparada não poderá ser excluída se for usada por qualquer esquema de provisionamento.

As etapas detalhadas são as seguintes:

1. Remova uma especificação de versão da imagem preparada. Por exemplo,

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
       ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
       PreparationType -eq 'Mcs'"
   Remove-ProvImageVersionSpec -ImageVersionSpecUid
       $PreparedImageVersionSpec.ImageVersionSpecUid -
       RunAsynchronously
   ```

   > **Nota:**
   >
   > A especificação da versão da imagem principal só poderá ser excluída quando não há nenhuma especificação de versão da imagem preparada associada.

2. Remova a especificação da versão da imagem mestre. Por exemplo,

   ```
   $MasterImageVersionSpec = Get-ProvImageVersionSpec -
       ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
       PreparationType -eq 'None'"
   Remove-ProvImageVersionSpec -ImageVersionSpecUid
       $PreparedImageVersionSpec.ImageVersionSpecUid -
       RunAsynchronously
   ```

3. Remova uma versão da imagem. Por exemplo,


```
Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
```

4. Remova uma definição de imagem. Por exemplo,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos do PowerShell:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
    image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
    1
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Gerenciar a definição e a versão de imagem

Você pode renomear e editar uma definição de imagem e editar uma versão da imagem.

- Renomeie uma definição de imagem usando o comando `Rename-ProvImageDefinition`. Por exemplo:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
      NewImageDefinitionName <string>
  ```

  Ou,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string> -
      NewImageDefinitionName <string>
  ```

- Edite uma definição de imagem usando o comando `Set-ProvImageDefinition`. Por exemplo:

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
      <string>]
  ```

  Ou,

  ```
  Set-ProvImageDefinition -ImageDefinitionName <string> [-
      Description <string>]
  ```

- Edite uma versão da imagem usando o comando `Set-ProvImageVersion`. Por exemplo:


```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
    string>]
```

Ou,

```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
```

Obter a definição de imagem, a versão da imagem, a especificação da versão da imagem preparada e os detalhes do esquema de provisionamento

- Obtenha detalhes da definição de imagem usando o comando `Get-ProvImageDefinition`. Por exemplo:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
```

- Obtenha detalhes da versão da imagem usando o comando `Get-ProvImageVersion`. Por exemplo:
  - Para listar versões da imagem em uma definição de imagem,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Para obter detalhes da versão da imagem,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    ```

- Prepare a especificação da versão da imagem usando o comando `Get-ProvImageVersionSpec`. Por exemplo:
  - Para listar todas as especificações da versão da imagem preparada em uma versão da imagem,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```


- Para listar as especificações da versão da imagem mestre em uma especificação de versão da imagem preparada,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "None"'
```

- Para listar as especificações da versão da imagem preparada em uma versão da imagem, que está associada a uma imagem mestre,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

- Para obter especificações de versão da imagem preparada com sucesso em uma versão da imagem,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
```

- Para obter um detalhe de especificação da versão da imagem preparada,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Obtenha detalhes do esquema de provisionamento usando o comando `Get-ProvScheme`. Por exemplo:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
```

- Prepare o histórico de especificações da versão da imagem de um esquema de provisionamento usando o comando `Get-ProvSchemeImageVersionSpecHistory`. Por exemplo:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
```

Criar um catálogo do Microsoft Azure

August 23, 2024

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

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de criar um catálogo do Microsoft Azure, você precisa concluir a criação de uma conexão com o Microsoft Azure. Consulte Conexão com o Microsoft Azure.

Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio
- Criar um catálogo de máquinas usando o PowerShell

Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

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

> **Nota:**
>
> O suporte ao uso de uma imagem mestre de uma região diferente daquela configurada na conexão do host está obsoleto. Use a Galeria de Computação do Azure para replicar a imagem mestre na região desejada.

Durante a preparação da imagem, uma máquina virtual de preparação é criada com base na VM original. Essa VM de preparação está desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. O grupo de segurança de rede é criado automaticamente uma vez por catálogo. O nome do grupo de segurança de rede é `Citrix-Deny-All-a3pgu-GUID`, sendo o GUID gerado aleatoriamente. Por exemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

No assistente de criação de catálogo de máquinas:

- As páginas **Create machine catalogs** e **Machine Management** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Imagem**, escolha uma imagem que você deseja usar como modelo para criar máquinas nesse catálogo.

  Se você selecionar **Imagem mestre** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e siga estas etapas para selecionar uma imagem mestre conforme necessário:

  1. (Aplicável somente às conexões configuradas com imagens compartilhadas com ou entre locatários) Selecione a assinatura em que a imagem reside.
  2. Selecione um grupo de recursos.
  3. Navegue até o Azure VHD, a Galeria de Computação do Azure ou a versão de imagem do Azure. Adicione uma nota para a imagem selecionada, se necessário.

  Ao selecionar uma imagem, considere o seguinte:

  - Verifique se um Citrix VDA está instalado na imagem.
  - Se você selecionar um VHD conectado a uma VM, deverá desligá-la antes de prosseguir para a próxima etapa.

  > **Nota:**
  >
  > - A assinatura correspondente à conexão (host) que criou as máquinas no catálogo é indicada com um ponto verde. As outras assinaturas são aquelas que têm a Galeria de Computação do Azure compartilhada com essa assinatura. Nessas assinaturas, somente galerias compartilhadas são exibidas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens com um locatário (entre assinaturas) e Compartilhar imagens entre locatários.
> - O uso de um perfil de máquina com início confiável como **Security Type** é obrigatório quando você seleciona uma imagem ou instantâneo com início confiável habilitado. Em seguida, você pode ativar ou desativar o SecureBoot e o vTPM especificando seus valores no perfil de máquina. O Trusted Launch não é compatível com a Galeria de Imagens Compartilhadas. Para obter informações sobre o início confiável do Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
> - Você pode criar um esquema de provisionamento usando o disco de SO efêmero no Windows com início confiável. Ao selecionar uma imagem com início confiável, você deve selecionar um perfil de máquina com início confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando o disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
> - Quando a replicação de imagem está em andamento, você pode prosseguir e sele-

> cionar a imagem como a imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode demorar mais para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída dentro de uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo não se completará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.
> - Quando você seleciona uma imagem mestre para catálogos de máquinas no Azure, o MCS identifica o tipo de SO com base na imagem mestre e no perfil de máquina selecionados. Se o MCS não conseguir identificá-lo, selecione o tipo de SO que corresponde à imagem mestre.
> - Você pode provisionar um catálogo de VM Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem antiga que não tenha informações de geração é uma imagem Gen1.

Se você selecionar **Imagem preparada** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e selecione uma imagem preparada conforme necessário.

Para garantir a criação bem-sucedida da VM, verifique se a imagem tem o Citrix VDA 2311 ou posterior instalado e se o MCSIO está presente no VDA.

Depois de selecionar uma imagem, a caixa de seleção **Usar um perfil de máquina (obrigatório para o Azure Active Directory)** é marcada automaticamente. Clique em **Select a machine profile** para navegar até a especificação de uma VM ou modelo ARM a partir de uma lista de grupos de recursos. As VMs no catálogo podem herdar configurações do perfil de máquina selecionado.

Valide a especificação do modelo ARM para garantir que possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Há duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Next**. Mensagens de erro são exibidas se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Exemplos de configurações que as máquinas virtuais podem herdar de um perfil de máquina incluem:

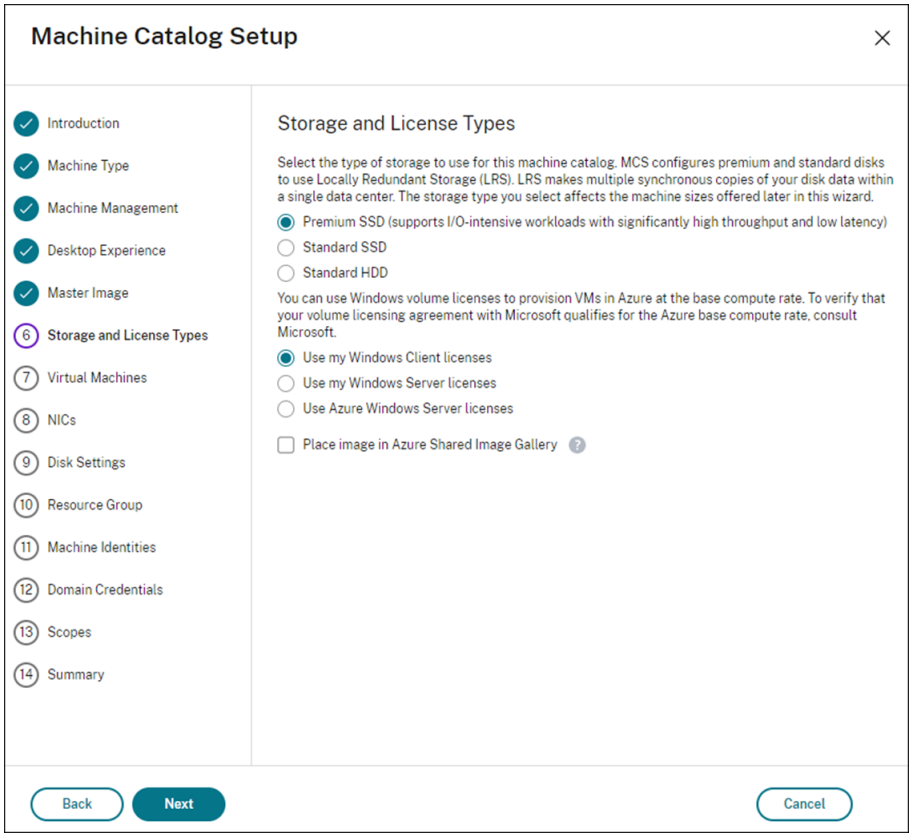
  - Rede acelerada
  - Diagnóstico de inicialização
  - Cache de disco do host (relacionado aos discos OS e MCSIO)
  - Tamanho da máquina (salvo indicação em contrário)
  - Tags colocadas na VM

  Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Machine Catalogs**, selecione o catálogo para exibir seus detalhes no painel inferior. Em seguida, clique na guia **Template Properties** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **View all**.

  Se desejar que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts dedicados** e selecione um grupo de hosts na lista. Um grupo de hosts é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço que fornece servidores físicos que hospedam uma ou mais máquinas virtuais. Seu servidor é dedicado à sua assinatura do Azure, não compartilhado com outros assinantes. Quando você usa um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em execução nesse host. Esse recurso é adequado para cenários em que você precisa atender aos requisitos regulamentares ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

  > **Importante:**
  >
  > - Somente são exibidos os grupos de hosts que têm o posicionamento automático do Azure habilitado.
  > - O uso de um grupo de hosts altera a página **Virtual Machines** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são mostrados nessa página. Além disso, as zonas de disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Storage and License Types** só aparece quando você usa uma imagem do Azure Resource Manager.



Os seguintes tipos de armazenamento podem ser usados no catálogo de máquinas:

- **Premium SSD**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência adequada para VMs com cargas de trabalho intensivas de E/S.
- **Standard SSD**. Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
- **Standard HDD**. Oferece uma opção de armazenamento em disco confiável e de baixo custo adequada para VMs que executam cargas de trabalho insensíveis à latência.
- **Azure ephemeral OS disk**. Oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Como alternativa, você pode usar o PowerShell para criar máquinas que usam discos de SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Leve em consideração os seguintes aspectos ao usar um disco de SO efêmero:
  - O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.
  - Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
  - Não é possível usar a opção **Retain VM and system disk during power cycless** oferecida posteriormente no assistente.

> **Nota:**
>
> O disco de identidade é sempre criado usando SSD Standard, independentemente do tipo de armazenamento que você escolher.

O tipo de armazenamento determina quais tamanhos de máquina são oferecidos na página **Máquinas Virtuais** do assistente. O MCS configura discos premium e padrão para usar o Armazenamento com Redundância Local (LRS). O LRS faz várias cópias síncronas dos dados do disco em um único data center. Os discos de SO efêmeros do Azure usam o disco local das VMs para armazenar o sistema operacional. Para obter detalhes sobre os tipos de armazenamento do Azure e a replicação de armazenamento, consulte o seguinte:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selecione se deseja usar as licenças existentes do Windows ou do Linux.

- Licenças do Windows: o uso de licenças do Windows junto com imagens do Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs do Windows no Azure a um custo reduzido. Existem dois tipos de licenças:
  - **Windows Server license**. Possibilita que você use suas licenças do Windows Server ou do Azure Windows Server, permitindo que você use os Benefícios Híbridos do Azure. Para obter detalhes, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. O Azure Hybrid Benefit reduz o custo de execução de VMs no Azure para a taxa de computação básica, dispensando o custo de licenças extras do Windows Server da galeria do Azure.
  - **Windows Client license**. Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e do Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de acesso para cliente e licenças de gerenciamento.

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando do PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows_Server**. Mais instruções estão disponíveis em https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.

- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows_Client**. Mais instruções estão disponíveis em https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Como alternativa, você pode usar o SDK PowerShell `Get-Provscheme` para fazer a verificação. Por exemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre esse cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenças do Linux: com as licenças BYOS (traga sua própria assinatura) do Linux, você não precisa pagar pelo software. A cobrança da BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:

  * **RHEL_BYOS**: para usar o tipo RHEL_BYOS com sucesso, habilite o Red Hat Cloud Access na sua assinatura do Azure.
  * **SLES_BYOS**: as versões BYOS do SLES incluem suporte da SUSE.

  Você pode definir o valor de LicenseType para as opções do Linux em `New-ProvScheme` e `Set-ProvScheme`.

  Exemplo de configuração de LicenseType como RHEL_BYOS em `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -CustomProperties '<CustomProperties xmlns="http://
    schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
    ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
```

  Exemplo de configuração de LicenseType como SLES_BYOS em `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
```


> **Nota:**
>
> Se o valor `LicenseType` estiver vazio, os valores padrão serão Azure Windows Server License ou Azure Linux License, dependendo do valor de OsType.

Exemplo de configuração de LicenseType como vazio:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
```

Consulte os seguintes documentos para entender os tipos de licença e seus benefícios:

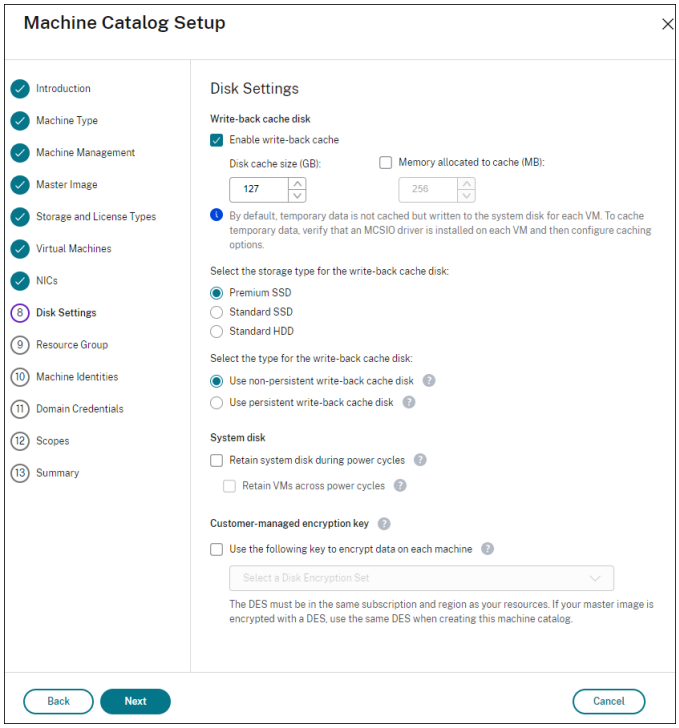
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

A Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas do Azure) é um repositório para gerenciar e compartilhar imagens. Ele permite que você disponibilize suas imagens em toda a organização. Recomendamos que você armazene uma imagem na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos de SO VDA. Depois que você selecionar **Place prepared image in Azure Compute Gallery**, aparece a seção **Azure Compute Gallery settings**, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

- **Ratio of virtual machines to image replicas**. Permite especificar a proporção de máquinas virtuais para réplicas de imagem que você deseja que o Azure mantenha. Por padrão, o Azure mantém uma única réplica de imagem para cada 40 máquinas não persistentes. Em máquinas persistentes, o número assume o valor padrão 1.000.
- **Maximum replica count**. Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 10.

> **Nota:**
>
> Uma galeria é criada no ACG para armazenar a imagem. Essa galeria é acessível somente ao MCS para criação de VMs e não aparece na página **Selecionar uma imagem**.

- Na página **Virtual Machines**, indique quantas VMs você deseja criar. Você deve especificar pelo menos um e selecionar um tamanho de máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.
- A página **NICs** não contém informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Disk Settings**, escolha se deseja ativar o cache write-back. Com o recurso de otimização de armazenamento do MCS ativado, você pode definir as seguintes configurações ao criar um catálogo: Essas configurações se aplicam aos ambientes Azure e GCP.



Depois de ativar o cache de write-back, você pode fazer o seguinte:

  - Configurar o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
  - Selecionar o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:
    - Premium SSD
    - Standard SSD
    - Standard HDD
  - Escolha se deseja que o disco de cache write-back persista para as VMs provisionadas. Selecione **Enable write-back cache** para disponibilizar as opções. Por padrão, a opção **Use non-persistent write-back cache disk** está selecionada.
  - Selecione o tipo para o disco de cache de write-back.

  - **Use non-persistent write-back cache disk**. Se selecionado, o disco de cache write-back é excluído durante os ciclos de alimentação de energia. Todos os dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Template Properties**. Se o disco temporário for usado, você verá **Non-persistent Write-back Cache Disk** e seu valor será **Yes (using VM's temporary disk)**. Caso contrário, você verá **Non-persistent Write-back Cache Disk** e seu valor será **No (not using VM's temporary disk)**.
  - **Use persistent write-back cache disk**. Se selecionado, o disco de cache de write-back persistirá para as VMs provisionadas. Habilitar a opção aumenta os custos de armazenamento.

- Escolha se deseja reter VMs e discos do sistema para VDAs durante os ciclos de alimentação de energia.

  Reter VM e disco do sistema durante ciclos de energia. Disponível quando você seleciona **Ativar cache de write-back**. Por padrão, VMs e discos de sistema são excluídos no desligamento e recriados na inicialização. Se você quiser reduzir o tempo de reinicialização da VM, selecione essa opção. Lembre-se de que ativar essa opção também aumenta os custos de armazenamento.

- Escolha se deseja ativar a **Economia de custos de armazenamento**. Se ativada, economize nos custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Standard quando a VM for desligada. A VM muda para suas configurações originais na reinicialização. A opção se aplica aos discos de armazenamento e cache de write-back. Como alternativa, você também pode usar o PowerShell. Consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

  > **Nota:**
  >
  > A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie as mudanças no tipo de armazenamento no futuro. Para obter mais informações, consulte este artigo da Microsoft.

- Escolha se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia no lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas no catálogo. Para obter mais informações, consulte Criptografia do servidor do Azure.

- Na página **Resource Group**, escolha se deseja criar grupos de recursos ou usar grupos existentes.
  - Se você optar por criar grupos de recursos, selecione **Next**.
  - Se você optar por usar grupos de recursos existentes, selecione grupos na lista **Available Provisioning Resource Groups**. **Lembre-se**: selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Será exibida uma mensagem se você escolher muito poucos. Talvez você queira selecionar mais do que o mínimo necessário se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que o catálogo é criado.

  Para obter mais informações, consulte Azure resource groups.
- Na página **Machine Identities**, escolha um tipo de identidade e configure identidades para máquinas nesse catálogo. Se você selecionar as VMs como **Azure Active Directory joined**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:
  1. No campo **Identity type**, selecione **Azure Active Directory joined**. A opção **Azure AD security group (optional)** é exibida.
  2. Clique em **Azure AD security group: Create new**.
  3. Insira o nome do grupo e clique em **Create**.
  4. Siga as instruções na tela para fazer logon no Azure.
     Se o nome do grupo não existir no Azure, um ícone verde é exibido. Caso contrário, uma mensagem de erro é exibida solicitando que você insira um novo nome.
  5. Insira o esquema de nomenclatura da conta da máquina para as VMs.

  Após a criação do catálogo, o Citrix Virtual Apps and Desktops acessa o Azure em seu nome e cria o grupo de segurança e uma regra de associação dinâmica para o grupo. Com base na regra, as VMs com o esquema de nomenclatura especificado no catálogo são adicionadas automaticamente ao grupo de segurança.

  Adicionar VMs com um esquema de nomenclatura diferente a esse catálogo exige que você entre no Azure. O Citrix Virtual Apps and Desktops pode então acessar o Azure e criar uma regra de associação dinâmica com base no novo esquema de nomenclatura.

  Ao excluir esse catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.
- As páginas **Domain Credentials** e **Summary** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.

Conclua o assistente.

Condições para que o disco temporário do Azure seja elegível para disco de cache write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem atendidas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.
- O tamanho escolhido da VM do Azure deve incluir um disco temporário.
- Não é necessário ativar o disco de SO efêmero
- Aceite colocar o arquivo de cache de write-back no disco temporário do Azure.
- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco do cache de write-back + espaço reservado para o arquivo de paginação + 1 GB de espaço no buffer).

Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back durante a criação do catálogo de máquinas.

Cenário	Resultado
Todas as condições para usar o disco temporário para cache write-back estão satisfeitas.	O arquivo WBC `mcsdif.vhdx` é colocado no disco temporário.
O disco temporário não tem espaço suficiente para o uso do cache write-back.	É criado um disco VHD `MCSWCDisk` e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.
O disco temporário tem espaço suficiente para o uso do cache write-back, mas `UseTempDiskForWBC` está definido como **false**.	É criado um disco VHD `MCSWCDisk` e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la no Web Studio e nos comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Acesse o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a interface de rede e a VM. No menu **...**, na parte superior, clique em **Exportar modelo**.

2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para o provisionamento de catálogos.
3. Clique em **Adicionar à biblioteca** para modificar a especificação do modelo posteriormente.
4. Na página **Importando modelos**, insira as informações necessárias, como **Nome**, **Assinatura**, **Grupo de recursos**, **Local** e **Versão**. Clique em **Próximo: Editar modelo**.
5. Você também precisa de uma interface de rede como um recurso independente se quiser provisionar catálogos. Portanto, você deve remover todos os `dependsOn` especificados na especificação do modelo. Por exemplo:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
```

6. Crie **Revisar+Criar** e crie a especificação do modelo.
7. Na página **Especificações do modelo**, verifique a especificação do modelo que você acabou de criar. Clique na especificação do modelo. No painel esquerdo, clique em **Versões**.
8. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação do modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação do modelo.

Você pode obter informações sobre a especificação e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação do modelo, execute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
```

- Para obter informações sobre a versão da especificação do modelo, execute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
```

Usar a especificação do modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou os comandos do PowerShell.

- Para o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

- Para o PowerShell, consulte Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell

Criptografia do servidor do Azure

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

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco está criptografado, 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 Início rápido: criar um cofre de chaves usando o portal do Azure para obter informações sobre como configurar a criptografia do servidor do Azure.

Chave de criptografia gerenciada pelo cliente do Azure

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

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

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

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

Consulte Criar um catálogo de máquinas usando a chave gerenciada pelo cliente.

Criptografia de disco do Azure no host

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

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

dor 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>
```

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

3. Crie uma especificação de modelo ou uma VM como entrada para o perfil da máquina no portal do Azure com a criptografia no host ativada.
   - Se você quiser criar uma VM, selecione um tamanho de VM que suporte criptografia no host. Depois de criar a VM, a propriedade da VM **Encryption at host** é ativada.
   - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `securityProfile`.
4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina selecionando uma especificação de modelo ou VM.
   - Disco de SO/Disco de dados: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma
   - Disco de SO efêmero: é criptografado somente pela chave gerenciada pela plataforma
   - Disco de cache: é criptografado através da chave gerenciada pelo cliente e da chave gerenciada pela plataforma

   Você pode criar o catálogo de máquinas usando o Web Studio ou executando comandos do PowerShell.

Recuperar informações de criptografia no host de um perfil de máquina

Você pode recuperar a criptografia nas informações do host de um perfil de máquina executando o comando PowerShell com o parâmetro `AdditionalData`. Se o parâmetro `EncryptionAtHost` for **True**, isso indica que a criptografia no host está habilitada para o perfil da máquina.

Por exemplo: quando a entrada do perfil da máquina for uma VM, execute o seguinte comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
```

Por exemplo: quando a entrada do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
```

Criptografia dupla no disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Todos os catálogos criados com esse recurso têm todos os discos do lado do servidor criptografados com chaves gerenciadas pela plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a chave de criptografia e os conjuntos de criptografia de disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

> **Nota:**
>
> - Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e os comandos do PowerShell. Consulte Criar um catálogo de máquinas com criptografia dupla para comandos do PowerShell.
> - Você pode usar um fluxo de trabalho não baseado em perfil de máquina ou um fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
> - Se você usar um fluxo de trabalho não baseado em perfil de máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetId` armazenado.
> - Se você usa um perfil de máquina, pode usar uma especificação de VM ou modelo como uma entrada de perfil de máquina.

Limitações:

- A criptografia dupla não é suportada em Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desabilitar uma chave DiskEncryptionSet associada a um catálogo, as VMs do catálogo serão desativadas.
- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você só pode criar até 50 conjuntos de criptografia de disco por região por assinatura.
- Você não pode atualizar um catálogo de máquinas que já tenha um `DiskEncryptionSetId` com um `DiskEncryptionSetId` diferente.

Grupos de recursos do Azure

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

Uso do grupo de recursos do Azure

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

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

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte Criar um catálogo com discos efêmeros do Azure.

> **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.

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.

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.

Galeria de Computação do Azure

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

- *Galeria*: as imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de imagem na galeria*: esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- *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 a Visão geral da Galeria de Computação do Azure.

Para obter informações sobre como criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure usando o PowerShell, consulte Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida durante o uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho do perfil da máquina para criar esse catálogo. Você pode usar as especificações do modelo VM e ARM como uma entrada de perfil de máquina.

Considerações importantes sobre VMs confidenciais

As considerações importantes sobre os tamanhos de VM compatíveis e a criação de um catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM compatíveis: as VMs confidenciais aceitam os seguintes tamanhos de VM:

  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series

- Crie catálogos de máquinas com VMs confidenciais.

  - Você pode criar um catálogo de máquinas com VMs confidenciais do Azure usando os comandos do Web Studio e do PowerShell.

  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquina com VMs Confidenciais do Azure. Você pode usar uma especificação de modelo ou VM como a entrada do perfil de máquina.

  - A imagem mestre e a entrada do perfil da máquina devem estar ativadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:

    * **VMGuestStateOnly**: VM confidencial com apenas o estado de convidado da VM criptografado
    * **DiskWithVMGuestState**: VM confidencial com disco do sistema operacional e estado de convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco operacional normal quanto o efêmero podem ser criptografados.

  - Você pode obter informações da VM confidencial de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM usando o parâmetro AdditionalData. Por exemplo:

    ```
    PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
       \image.folder\username-dev-testing-rg.resourcegroup\
       username-dev-tsvda.vm).AdditionalData
    ```

    Os campos de dados adicionais são:

    * DiskSecurityType
    * ConfidentialVMDiskEncryptionSetId
    * DiskSecurityProfiles

    Para obter a propriedade de computação confidencial de um tamanho de máquina, execute o seguinte comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

    O campo de dados adicional é `ConfidentialComputingType`.

  - Você não pode alterar a imagem mestre ou o perfil da máquina do tipo de segurança confidencial para não confidencial ou do tipo de segurança não confidencial para confidencial.

- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

Preparar imagens mestras e perfis de máquina

Antes de criar um conjunto de VMs confidenciais, siga estas etapas para preparar uma imagem mestre e um perfil de máquina para elas:

1. No portal do Azure, crie uma VM confidencial com configurações específicas, como:
   - **Tipo de segurança**: máquinas virtuais confidenciais
   - **Criptografia de disco do sistema operacional confidencial**: ativada.
   - **Gerenciamento de chaves**: criptografia confidencial de disco com uma chave gerenciada pela plataforma
     Para obter mais informações sobre a criação de VMs confidenciais, consulte este artigo da Microsoft.
2. Prepare a imagem mestre na VM criada. Instale os aplicativos e o VDA necessários na VM criada.

   > **Nota:**
   >
   > Não há suporte para a criação de VMs confidenciais usando VHD. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil de máquina usando uma das seguintes formas:
   - Use a VM existente criada na etapa 1 se ela tiver as propriedades de máquina necessárias.
   - Se você optar por uma especificação de modelo do ARM como perfil de máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos confidenciais de VM, como *SecurityEncryptionType* e *DiskEncryptionSet* (para chave gerenciada pelo cliente). Para obter mais informações, consulte Criar uma especificação de modelo do Azure.

     > **Nota:**
     >
     > - Certifique-se de que a imagem mestre e o perfil de máquina tenham o mesmo tipo de chave de segurança.
     > - Para criar VMs confidenciais que exijam criptografia confidencial de disco do sistema operacional com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil de máquina sejam idênticos.

Criar VMs confidenciais usando comandos do Web Studio ou PowerShell

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Web Studio, siga as etapas descritas em Criar catálogos de máquinas. Lembre-se das seguintes considerações:

- Na página **Imagem**, selecione uma imagem mestre e um perfil de máquina que você preparou para a criação da VM confidencial. A seleção do perfil de máquina é obrigatória e somente os perfis que correspondam ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.
- Na página **Máquinas virtuais**, somente os tamanhos de máquina que permitem VMs confidenciais aparecem para seleção.
- Na página **Configurações do disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

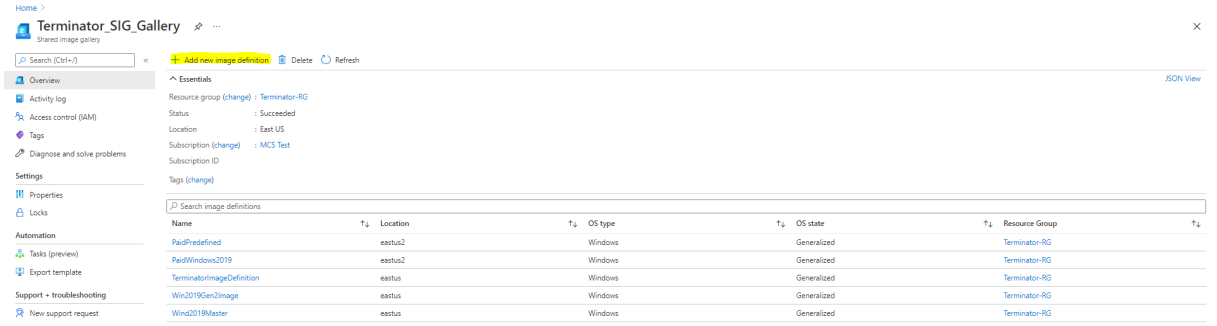
Azure Marketplace

O Citrix Virtual Apps and Desktops oferece suporte ao uso de uma imagem mestre no Azure que contém informações do plano para criar um catálogo de máquina. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**
>
> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não acrescentam informações do plano. O recurso Citrix Virtual Apps and Desktops é para imagens pagas.

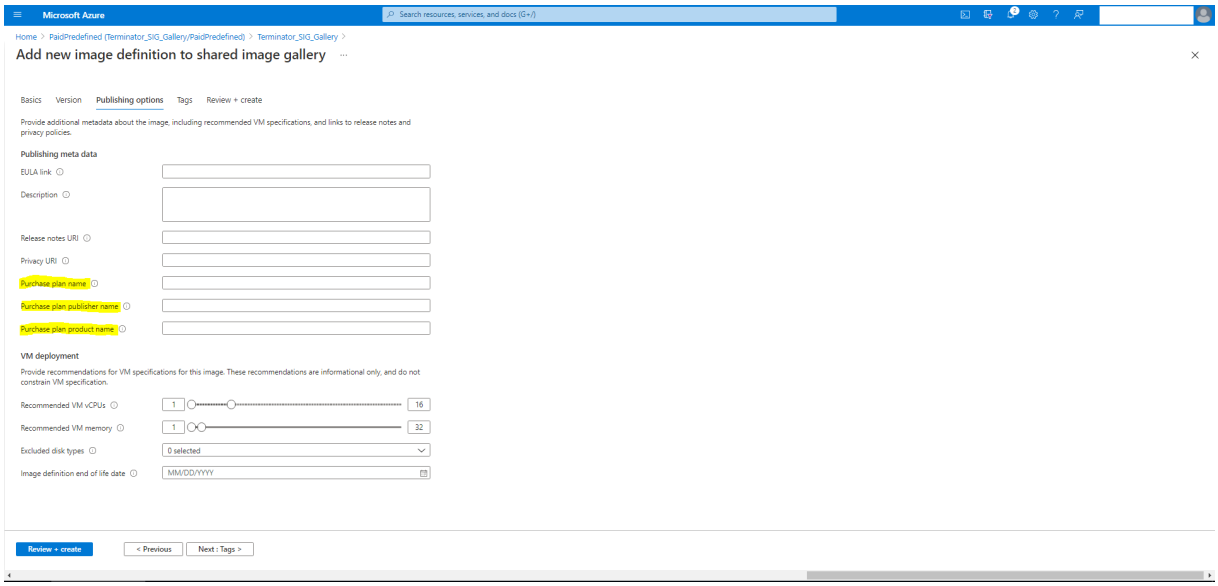
Verifique se a imagem criada na Galeria de Imagens Compartilhadas contém informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Opcionalmente, essas imagens podem ser usadas para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.

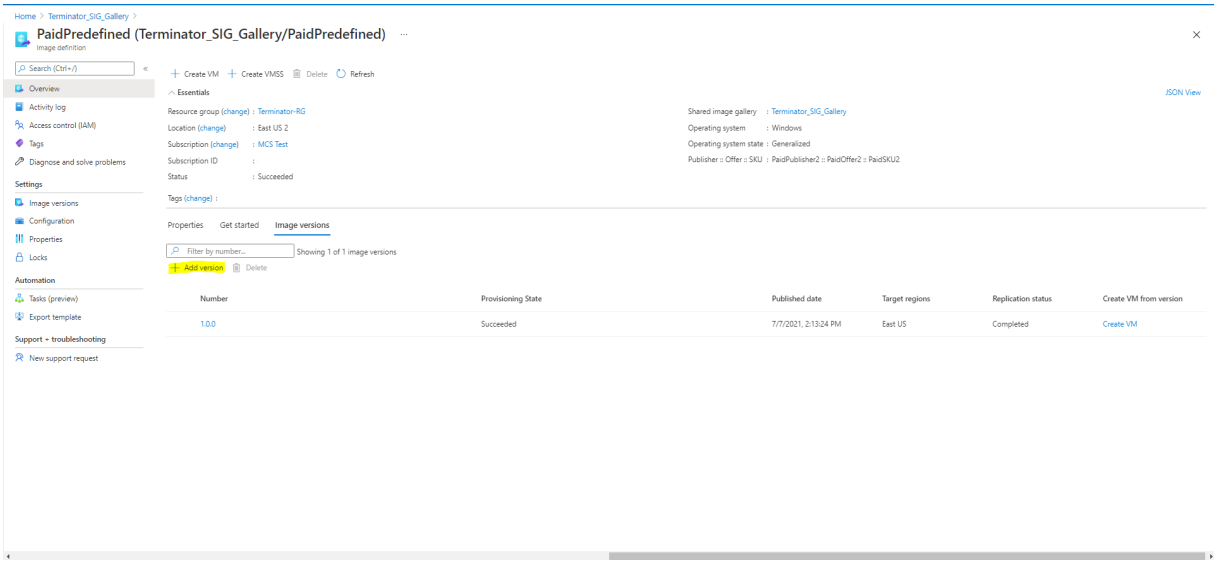


Na página **Publishing options**, verifique as informações do plano de compra.

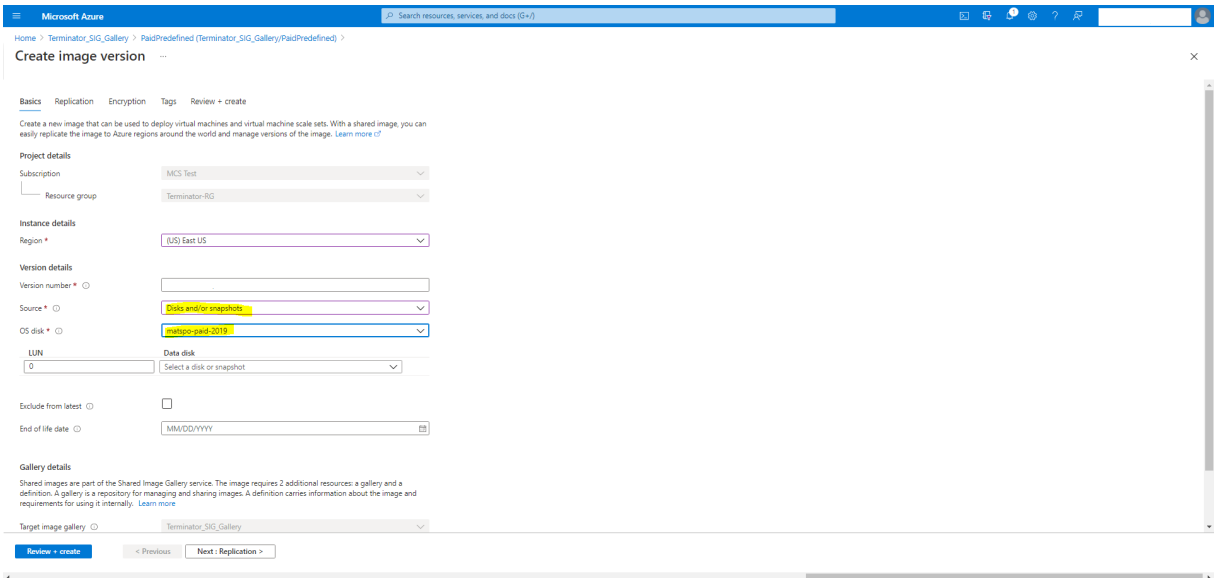
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. Se você deixar de preencher as informações do plano de compra, isso pode causar falha no processo do catálogo de máquinas.



Depois de verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Isso é usado como a imagem mestre. Clique em **Add version**:



Na seção **Version details**, selecione o instantâneo da imagem ou o disco gerenciado como origem:



Criar um catálogo de máquinas usando o PowerShell

Esta seção detalha como você pode criar catálogos usando o PowerShell:

- Criar um catálogo com disco de cache de write-back não persistente
- Criar um catálogo com disco de cache de write-back não persistente
- Melhorar o desempenho de inicialização com o MCSIO
- Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell
- Catálogos de máquinas com início confiável
- Usar valores de propriedades do perfil da máquina
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

- Criar um catálogo de máquinas com criptografia dupla
- Criar um catálogo com discos efêmeros do Azure
- Hosts dedicados do Azure
- Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure
- Configurar a Galeria de Imagens Compartilhadas
- Provisionar máquinas em zonas de disponibilidade especificadas
- Tipos de armazenamento
- Localização do arquivo de paginação
- Atualizar configuração do arquivo de página
- Criar um catálogo usando VMs do Azure Spot
- Configurar tamanhos de VM de backup
- Copiar marcas em todos os recursos
- Provisionar VMs do catálogo com o Azure Monitor Agent instalado

Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back não persistente, use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. A propriedade personalizada `UseTempDiskForWBC` indica se você está aceitando usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como true durante a execução `New-ProvScheme` se você quiser usar o disco temporário como disco de cache write-back. Se essa propriedade não for especificada, o parâmetro será definido como **False** por padrão.

Por exemplo, uso do parâmetro `CustomProperties` para definir `UseTempDiskForWBC` como **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
    true"/> `
</CustomProperties>'
```


> **Nota:**
>
> Depois de confirmar o catálogo da máquina para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar o VHD posteriormente.

Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro do PowerShell `New-ProvScheme CustomProperties`. Esse parâmetro 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>
```

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>
```

> **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
```


Melhorar o desempenho de inicialização com o MCSIO

Você pode melhorar o desempenho de inicialização dos discos gerenciados do Azure e do GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` são:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
</CustomProperties>
```

Para ativar esse recurso, defina a propriedade personalizada `PersistOSDisk` como **`true`**. Por exemplo:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\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
```


```

### Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou os comandos do PowerShell.

Para o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

Usando comandos do PowerShell:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie ou atualize um catálogo.

    - Para criar um catálogo:

        a) Use o comando `New-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

        ```
        New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
            image.folder/fgthj.resourcegroup/nab-ws-
            vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
        MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
            folder/fgthj.resourcegroup/test.templatespec/V1.
            templatespecversion"
        -ProvisioningSchemeName <String>
        -HostingUnitName <String>
        -IdentityPoolName <String>
        [-ServiceOffering <String>][-CustomProperties <String>
        [-LoggingId <Guid>]
        [-BearerToken <String>][-AdminAddress <String>]
        [<CommonParameters>]
        ```

        b) Conclua a criação do catálogo.

    - Para atualizar um catálogo, use o comando `Set-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

    ```
    Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
        Us.region/vm.folder/MasterDisk.vm'
    MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/testing.templatespec/V1.
        templatespecversion'
    [-ProvisioningSchemeName] <String>
    [-CustomProperties <String>][-ServiceOffering <String>] [-
        PassThru]
    [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
        String>] [<CommonParameters>]
    ```


Catálogos de máquinas com início confiável

Para criar com êxito um catálogo de máquinas com início confiável, use:

- Um perfil de máquina com início confiável
- Um tamanho de VM que ofereça suporte ao início confiável
- Uma versão de VM do Windows que ofereça suporte ao início confiável. Atualmente, o Windows 10, o Windows 11 e o Windows Server 2016, 2019 e 2022 oferecem suporte ao início confiável.

> **Importante:**
>
> O MCS oferece suporte à criação de um novo catálogo com VMs habilitadas para o início confiável. No entanto, para atualizar um catálogo persistente existente e as VMs existentes, você precisa usar o portal do Azure. Você não pode atualizar o início confiável de um catálogo não persistente. Para obter mais informações, consulte o documento da Microsoft Habilitar o Início confiável em VMs existentes do Azure.

Para exibir os itens de inventário da oferta do Citrix Virtual Apps and Desktops e determinar se o tamanho da VM oferece suporte ao início confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **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)
```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.
    - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM oferecerá suporte ao início confiável.
    - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não oferecerá suporte ao início confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que oferecem suporte ao início confiável:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
```

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 será 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 será 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.

Criar um catálogo de máquinas com início confiável

1. Crie uma imagem mestre habilitada com o início confiável. Consulte a documentação da Microsoft Imagens da VM de início confiável.
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de início confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft Implantar uma VM de início confiável.
3. Crie um catálogo de máquinas usando os comandos do Web Studio ou do PowerShell.
   - Se você quiser usar o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio.
   - Se você quiser usar os comandos do PowerShell, use o comando `New-ProvScheme` com a VM ou especificação de modelo como uma entrada de perfil de máquina. Para obter a lista completa de comandos para criar um catálogo, consulte Criação de um catálogo.

     Exemplo de `New-ProvScheme` com a VM como entrada de perfil de máquina:

     ```
     1  New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
           IdentityPoolName "name" -InitialBatchSizeHint 1
     2  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
           resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     3  -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
           folder<def.resourcegroup><machine profile vm.vm>"
     4  -ProvisioningSchemeName <String>
     5  -HostingUnitName <String>
     6  -IdentityPoolName <String>
     7  [-ServiceOffering <String>][-CustomProperties <String>]
     8  [<CommonParameters>]
     ```

     Exemplo de `New-ProvScheme` com a especificação de modelo como entrada de perfil de máquina:


```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
```

Erros ao criar catálogos de máquinas com 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

Usar valores de propriedades do perfil da máquina

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

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

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

> **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>"/>
    ```



```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId
    " Value="<mpA-value>"/>
<Property xsi:type="StringProperty" Name="
    DedicatedHostGroupId" Value="<mpA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>
</CustomProperties>
```

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

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

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

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

  As propriedades personalizadas têm prioridade. Os 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>
  ```


- 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>
  ```

- 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"
  ```

  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>
  ```


- 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.

```
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="
      Linux"/>
4  </CustomProperties>
```

- 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>
```


- 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:

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

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



```
8   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mpB-value>"/>
9   </CustomProperties>
```

Provisionar VMs do catálogo com o Azure Monitor Agent instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e atuar nos dados de telemetria de seus ambientes do Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos computacionais, como máquinas virtuais, e entrega os dados para o Azure Monitor. Atualmente, ele oferece suporte à coleção de métricas de Logs de eventos, Syslog e Desempenho e a envia para fontes de dados do Azure Monitor Metrics e do Azure Monitor Logs.

Para habilitar o monitoramento identificando de forma exclusiva as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

Requisitos

- Permissões: verifique se você tem as permissões mínimas do Azure, conforme especificado em Permissões necessárias do Azure, e as seguintes permissões para usar o Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regra de coleta de dados: configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar um DCR, consulte Criar uma regra de coleta de dados. Um DCR é específico da plataforma (Windows ou Linux). Certifique-se de criar um DCR de acordo com a plataforma necessária.
  A AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e fontes de dados, como Azure Monitor Metrics e Azure Monitor Logs.
- Espaço de trabalho padrão: crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um espaço de trabalho, consulte Criar um espaço de trabalho do Log Analytics. Quando você coleta logs e dados, as informações são armazenadas em um espaço de trabalho. Um espaço de trabalho tem um ID de espaço de trabalho e um ID de recurso exclusivos. O nome do espaço de trabalho deve ser exclusivo para um determinado grupo de recursos. Depois de criar um espaço de trabalho, configure fontes de dados e soluções para armazenar seus dados no espaço de trabalho.

- Incluiu a extensão do monitor na lista branca: as extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões definidas na lista branca da Citrix. Para ver a lista de extensões na lista branca, use o comando PoSH `Get-ProvMetadataConfiguration`.
- Imagem mestre: a Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso poderá levar a arquivos remanescentes e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para provisionar VMs de catálogo com o AMA ativado:

1. Configure um modelo de perfil de máquina.
   - Se você quiser usar uma máquina virtual como modelo de perfil de máquina:
     a) Crie uma VM no portal do Azure.
     b) Ligue a VM.
     c) Adicione a VM à regra de coleta de dados em **Resources**. Isso invoca a instalação do agente na VM modelo.

     > **Nota:**
     >
     > Se você precisar criar um catálogo Linux, configure uma máquina Linux.

   - Se você quiser usar a especificação do modelo como modelo de um perfil de máquina:
     a) Configure uma especificação de modelo.
     b) Adicione a seguinte associação de extensão e regra de coleta de dados à especificação do modelo gerado:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
```



```
{

   "type": "Microsoft.Insights/
      dataCollectionRuleAssociations",
   "apiVersion": "2021-11-01",
   "name": "<associatio-name>",
   "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
   "dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>",
   "Microsoft.Compute/virtualMachines/<vm-name>/extensions
      /AzureMonitorWindowsAgent"
   ],
   "properties": {

      "description": "Association of data collection rule.
          Deleting this association will break the data
         collection for this Arc server.",
    "dataCollectionRuleId": "/subscriptions/<azure-
       subscription>/resourcegroups/<azure-resource-group
       >/providers/microsoft.insights/datacollectionrules
       /<azure-data-collection-rule>"
     }

    }
```

2. Crie ou atualize um catálogo de máquinas MCS existente.
   - Para criar um novo catálogo MCS:
     a) Selecione essa de VM ou especificação modelo como um perfil de máquina no Web Studio.
     b) Continue com as próximas etapas para criar o catálogo.
   - Para atualizar um catálogo MCS existente, use os seguintes comandos PoSH:
     - Para que as novas VMs obtenham o modelo de perfil de máquina atualizado, execute o seguinte comando:

       ```
       Set-ProvScheme -ProvisioningSchemeName "name"
       -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
          folder\abc.resourcegroup\ab-machine-profile.vm"
       ```

     - Para atualizar as VMs existentes com o modelo de perfil de máquina atualizado:

       ```
       Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
          catalog -StartsNow -DurationInMinutes -1
       ```

3. Ligue as máquinas virtuais do catálogo.
4. Acesse o portal do Azure e verifique se a extensão do monitor está instalada na VM e se a VM aparece nos recursos do DCR. Depois de alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

Solução de problemas

Para obter informações para orientar a solução de problemas do agente do Azure Monitor, consulte o seguinte:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

As etapas detalhadas sobre como criar um catálogo de máquinas com a chave de criptografia gerenciada pelo cliente são:

1. Abra uma janela do PowerShell.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Digite `cd xdhyp:/`.
4. Digite `cd .\HostingUnits\(your hosting unit)`.
5. Digite `cd diskencryptionset.folder`.
6. Digite `dir` para obter a lista de Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma cadeia de caracteres de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

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


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

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
```

10. Execute o comando New-ProvScheme. Por exemplo:

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

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

11. Conclua a criação do catálogo de máquinas.

Criar um catálogo de máquinas com criptografia dupla

Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e os comandos do PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e um DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Usar o portal do Azure para habilitar a criptografia dupla inativa para discos gerenciados.
2. Para procurar os DiskEncryptionSets disponíveis em sua conexão de hospedagem:
   a) Abra uma janela do **PowerShell**.
   b) Execute os seguintes comandos do PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (ex.: azure-east)
      v. `cd diskencryptionset.folder`
      vi. `dir`

Você pode usar um ID do `DiskEncryptionSet` para criar ou atualizar um catálogo usando propriedades personalizadas.

3. Se você quiser usar o fluxo de trabalho do perfil da máquina, crie uma especificação de VM ou modelo como entrada do perfil da máquina.

   - Se você quiser usar uma VM como entrada de perfil de máquina:
     a) Crie uma VM no Portal do Azure.
     b) Navegue até **Disks>Key management** para criptografar a VM diretamente com um `DiskEncryptionSetID`.
   - Se você quiser usar uma especificação de modelo como entrada de perfil de máquina:
     a) No modelo, em `properties>storageProfile>osDisk>managedDisk`, adicione o parâmetro `diskEncryptionSet` e adicione o ID do DES de criptografia dupla.

4. Crie o catálogo de máquinas.

   - Se estiver usando o Web Studio, siga um dos procedimentos a seguir, além das etapas em Criar catálogos de máquinas.
     - Se você não usar o fluxo de trabalho baseado em perfil de máquina, na página **Configurações do disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue a criar o catálogo.
     - Se estiver usando o fluxo de trabalho do perfil da máquina, na página **Imagem**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID do conjunto de criptografia de disco em suas propriedades.

     Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.
   - Se estiver usando comandos do PowerShell, faça o seguinte:
     - Se não estiver usando o fluxo de trabalho baseado no perfil da máquina, adicione a propriedade personalizada `DiskEncryptionSetId` no `New-ProvScheme` comando. Por exemplo:

```
1  New-ProvScheme -CleanOnBoot -CustomProperties '<
       CustomProperties xmlns="http://schemas.citrix.com/2014/
       xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks"
        Value="true" />
3  <Property xsi:type="StringProperty" Name="
       StorageAccountType" Value="Premium_LRS" />
```



```
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
```

- Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
```

5. Conclua a criação do catálogo usando o SDK remoto 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/. Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina) somente se o catálogo não tiver sido criptografado anteriormente.

- Se não estiver usando o fluxo de trabalho baseado no perfil da máquina, adicione a propriedade personalizada DiskEncryptionSetId no comando `Set-ProvScheme`. Por exemplo:


```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
```

- Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
```

Depois de bem-sucedidas, todas as novas VMs que você adiciona ao seu catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

Verificar se o catálogo está criptografado duas vezes

- No Web Studio:
  1. Navegue até **Machine Catalogs**.
  2. Selecione o catálogo que você deseja verificar. Clique na guia **Template Properties** localizada na parte inferior da tela.
  3. Em **Azure Details**, verifique o ID do conjunto de criptografia de disco em **Disk Encryption Set**. Se o ID do DES do catálogo estiver em branco, o catálogo não está criptografado.
  4. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.
- Usando o comando do PowerShell:
  1. Abra a janela do **PowerShell**.
  2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
  3. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     ```

  4. Recupere a propriedade personalizada DES Id do catálogo da máquina. Por exemplo:


```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
```

5. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.

Criar um catálogo com discos efêmeros do Azure

Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **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"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {
```



```
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          ],
```

Configurar um disco efêmero para um catálogo

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

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

Por exemplo:

```
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">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
     "true" />
4 <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
     true" />
5 </CustomProperties>'
```

Considerações importantes para discos efêmeros

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

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

Considere também esses problemas nas seguintes situações:

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

Hosts dedicados do Azure

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

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

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

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

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

- Um *host dedicado* é uma propriedade de catálogo e não pode ser alterado depois que o catálogo é criado. Atualmente, a locação dedicada não é suportada no Azure.
- 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.

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

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

Para que essas imagens apareçam, você deve:

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

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

1. Abra uma janela do PowerShell.
2. Execute 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")
```

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")
```

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")
```

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 répli-

> cas. 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:

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

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

Para 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>'
```

> **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:

```
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="False"/></CustomProperties>'
```

> **Dica:**
>
> Ao contrário da atualização de um instantâneo para um catálogo da Galeria de Imagens Compartilhadas, os dados personalizados de cada máquina ainda não foram atualizados para refletir as novas propriedades personalizadas. Execute o 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.

Configurar 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`:

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
```

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

```
$serviceOffering.AdditionalData
```

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

Para configurar zonas de disponibilidade 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.

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.

Configurar tipos de armazenamento

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

Habilitar o armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica de forma síncrona seu disco gerenciado do Azure em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser definido usando propriedades personalizadas existentes ou por meio do modelo **MachineProfile**. O armazenamento ZRS também é compatível com o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`, e você pode alterar a máquina existente do armazenamento LRS para o ZRS.

Limitações:

- Compatível somente com discos gerenciados
- Compatível apenas com unidades de estado sólido (SSD) premium e standard
- Não compatível com `StorageTypeAtShutdown`
- Disponível somente em determinadas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em grande escala. Portanto, para a primeira ativação, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

Defina o armazenamento com redundância de zona como o tipo de armazenamento em disco
Você pode selecionar armazenamento com redundância de zona durante a criação do catálogo inicial ou atualizar seu tipo de armazenamento em um catálogo existente.

Selecionar armazenamento com redundância de zona usando comandos do PowerShell Ao criar um novo catálogo no Azure usando o comando `New-ProvScheme` do PowerShell, use `Standard_ZRS` como o valor em `StorageAccountType`.
Por exemplo:


```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se ele pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso do ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: a propriedade personalizada StorageTypeAtShutdown não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: essa exceção ocorre se você tentar usar o Armazenamento ZRS em uma região do Azure que não oferece suporte a ZRS
- **ZrsRequiresManagedDisks**: você pode usar armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento em disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante a criação do catálogo, o disco do sistema operacional do perfil da máquina `StorageType` é usado se as propriedades personalizadas não estiverem definidas.

Capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina enquanto cria um catálogo de máquinas, atualiza um catálogo de máquinas existente e atualiza as VMs existentes.

Você pode criar uma VM ou especificação de modelo como fonte de perfil de máquina.

Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação de modelo.
    - Storage account
    - Espaço de trabalho de análise de logs
    - Namespace do hub de eventos com preços de nível padrão
2. Crie uma fonte de perfil de máquina.

3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize as VMs existentes.

Configurar os IDs necessários no Azure

Configure uma das seguintes opções no Azure:

- Storage account
- Espaço de trabalho de análise de logs
- Namespace do hub de eventos com preços de nível padrão

Configurar uma conta de armazenamento Crie uma conta de armazenamento padrão no Azure. Na especificação de modelo, forneça o resourceId completo da conta de armazenamento como o `storageAccountId`.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, os dados podem ser encontrados no contêiner `insights-metrics-pt1m`.

Configurar um espaço de trabalho de análise de logs Crie um espaço de trabalho de análise de logs. Na especificação de modelo, forneça o resourceId completo para o espaço de trabalho de análise de logs como workspaceId.

Depois que as VMs são configuradas para registrar dados no espaço de trabalho, os dados podem ser consultados em Logs no Azure. Você pode executar o seguinte comando no Azure em Logs para mostrar uma contagem de todas as métricas registradas por um recurso:

‘AzureMetrics
| summarize Count=count() by ResourceId# Criar um catálogo do Microsoft Azure

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

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de criar um catálogo do Microsoft Azure, você precisa concluir a criação de uma conexão com o Microsoft Azure. Consulte Conexão com o Microsoft Azure.

Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio
- Criar um catálogo de máquinas usando o PowerShell

Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

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

> **Nota:**
>
> O suporte ao uso de uma imagem mestre de uma região diferente daquela configurada na conexão do host está obsoleto. Use a Galeria de Computação do Azure para replicar a imagem mestre na região desejada.

Durante a preparação da imagem, uma máquina virtual de preparação é criada com base na VM original. Essa VM de preparação está desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. O grupo de segurança de rede é criado automaticamente uma vez por catálogo. O nome do grupo de segurança de rede é <!JEKYLL@6100@0>, sendo o GUID gerado aleatoriamente. Por exemplo, <!JEKYLL@6100@1>.

No assistente de criação de catálogo de máquinas:

- As páginas **Create machine catalogs** e **Machine Management** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Imagem**, escolha uma imagem que você deseja usar como modelo para criar máquinas nesse catálogo.

  Se você selecionar **Imagem mestre** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e siga estas etapas para selecionar uma imagem mestre conforme necessário:

  1. (Aplicável somente às conexões configuradas com imagens compartilhadas com ou entre locatários) Selecione a assinatura em que a imagem reside.
  2. Selecione um grupo de recursos.

3. Navegue até o Azure VHD, a Galeria de Computação do Azure ou a versão de imagem do Azure. Adicione uma nota para a imagem selecionada, se necessário.

Ao selecionar uma imagem, considere o seguinte:

- Verifique se um Citrix VDA está instalado na imagem.
- Se você selecionar um VHD conectado a uma VM, deverá desligá-la antes de prosseguir para a próxima etapa.

> **Nota:**
>
> - A assinatura correspondente à conexão (host) que criou as máquinas no catálogo é indicada com um ponto verde. As outras assinaturas são aquelas que têm a Galeria de Computação do Azure compartilhada com essa assinatura. Nessas assinaturas, somente galerias compartilhadas são exibidas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens com um locatário (entre assinaturas) e Compartilhar imagens entre locatários.
> - O uso de um perfil de máquina com início confiável como **Security Type** é obrigatório quando você seleciona uma imagem ou instantâneo com início confiável habilitado. Em seguida, você pode ativar ou desativar o SecureBoot e o vTPM especificando seus valores no perfil de máquina. O Trusted Launch não é compatível com a Galeria de Imagens Compartilhadas. Para obter informações sobre o início confiável do Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
> - Você pode criar um esquema de provisionamento usando o disco de SO efêmero no Windows com início confiável. Ao selecionar uma imagem com início confiável, você deve selecionar um perfil de máquina com início confiável que esteja habilitado com vTPM. Para criar catálogos de máquinas usando o disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
> - Quando a replicação de imagem está em andamento, você pode prosseguir e selecionar a imagem como a imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode demorar mais para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída dentro de uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo não se completará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.
> - Quando você seleciona uma imagem mestre para catálogos de máquinas no Azure, o MCS identifica o tipo de SO com base na imagem mestre e no perfil de máquina selecionados. Se o MCS não conseguir identificá-lo, selecione o tipo de SO que corresponde à imagem mestre.
> - Você pode provisionar um catálogo de VM Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo

> de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem antiga que não tenha informações de geração é uma imagem Gen1.

Se você selecionar **Imagem preparada** como o tipo de imagem a ser usado, clique em **Selecionar uma imagem** e selecione uma imagem preparada conforme necessário.

Para garantir a criação bem-sucedida da VM, verifique se a imagem tem o Citrix VDA 2311 ou posterior instalado e se o MCSIO está presente no VDA.

Depois de selecionar uma imagem, a caixa de seleção **Usar um perfil de máquina (obrigatório para o Azure Active Directory)** é marcada automaticamente. Clique em **Select a machine profile** para navegar até a especificação de uma VM ou modelo ARM a partir de uma lista de grupos de recursos. As VMs no catálogo podem herdar configurações do perfil de máquina selecionado.

Valide a especificação do modelo ARM para garantir que possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Há duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Next**. Mensagens de erro são exibidas se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  - <!JEKYLL@6100@2>
  - <!JEKYLL@6100@3>

Exemplos de configurações que as máquinas virtuais podem herdar de um perfil de máquina incluem:

- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado aos discos OS e MCSIO)
- Tamanho da máquina (salvo indicação em contrário)
- Tags colocadas na VM

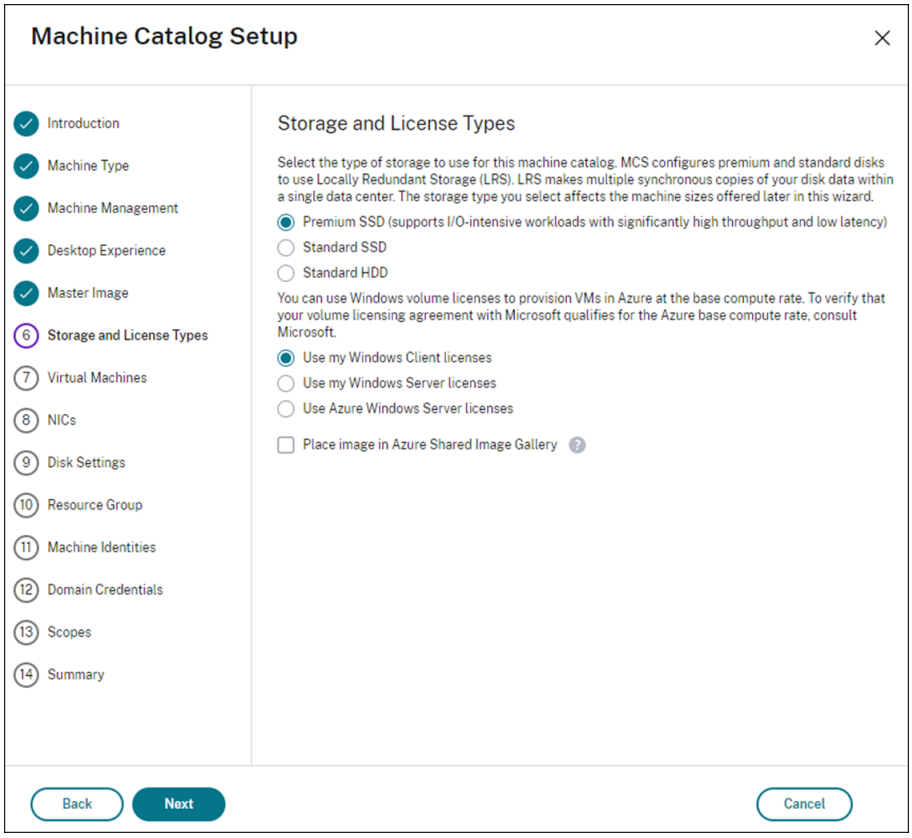
Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Machine Catalogs**, selecione o catálogo para exibir seus detalhes no painel inferior. Em seguida, clique na guia **Template Properties** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **View all**.

Se desejar que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts dedicados** e selecione um grupo de hosts na lista. Um grupo de hosts é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço

que fornece servidores físicos que hospedam uma ou mais máquinas virtuais. Seu servidor é dedicado à sua assinatura do Azure, não compartilhado com outros assinantes. Quando você usa um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em execução nesse host. Esse recurso é adequado para cenários em que você precisa atender aos requisitos regulamentares ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Hosts dedicados do Azure.

> **Importante:**
>
> - Somente são exibidos os grupos de hosts que têm o posicionamento automático do Azure habilitado.
> - O uso de um grupo de hosts altera a página **Virtual Machines** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são mostrados nessa página. Além disso, as zonas de disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

- A página **Storage and License Types** só aparece quando você usa uma imagem do Azure Resource Manager.



Os seguintes tipos de armazenamento podem ser usados no catálogo de máquinas:

- **Premium SSD**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência adequada para VMs com cargas de trabalho intensivas de E/S.

- **Standard SSD**. Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
- **Standard HDD**. Oferece uma opção de armazenamento em disco confiável e de baixo custo adequada para VMs que executam cargas de trabalho insensíveis à latência.
- **Azure ephemeral OS disk**. Oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Como alternativa, você pode usar o PowerShell para criar máquinas que usam discos de SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Leve em consideração os seguintes aspectos ao usar um disco de SO efêmero:
  * O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.
  * Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
  * Não é possível usar a opção **Retain VM and system disk during power cycless** oferecida posteriormente no assistente.

> **Nota:**
>
> O disco de identidade é sempre criado usando SSD Standard, independentemente do tipo de armazenamento que você escolher.

O tipo de armazenamento determina quais tamanhos de máquina são oferecidos na página **Máquinas Virtuais** do assistente. O MCS configura discos premium e padrão para usar o Armazenamento com Redundância Local (LRS). O LRS faz várias cópias síncronas dos dados do disco em um único data center. Os discos de SO efêmeros do Azure usam o disco local das VMs para armazenar o sistema operacional. Para obter detalhes sobre os tipos de armazenamento do Azure e a replicação de armazenamento, consulte o seguinte:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Selecione se deseja usar as licenças existentes do Windows ou do Linux.

- Licenças do Windows: o uso de licenças do Windows junto com imagens do Windows (imagens de suporte da plataforma Azure ou imagens personalizadas) permite executar VMs do Windows no Azure a um custo reduzido. Existem dois tipos de licenças:
  * **Windows Server license**. Possibilita que você use suas licenças do Windows Server ou do Azure Windows Server, permitindo que você use os Benefícios Híbridos do Azure. Para obter detalhes, consulte https://azure.microsoft.com/en-

us/pricing/hybrid-benefit/. O Azure Hybrid Benefit reduz o custo de execução de VMs no Azure para a taxa de computação básica, dispensando o custo de licenças extras do Windows Server da galeria do Azure.

* **Windows Client license**. Permite que você traga suas licenças do Windows 10 e Windows 11 para o Azure, permitindo que você execute VMs do Windows 10 e do Windows 11 no Azure sem a necessidade de licenças extras. Para obter detalhes, consulte Licenças de acesso para cliente e licenças de gerenciamento.

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando do PowerShell: <!JEKYLL@6100@4>.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows_Server**. Mais instruções estão disponíveis em https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows_Client**. Mais instruções estão disponíveis em https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Como alternativa, você pode usar o SDK PowerShell <!JEKYLL@6100@5> para fazer a verificação. Por exemplo: <!JEKYLL@6100@6>. Para obter mais informações sobre esse cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licenças do Linux: com as licenças BYOS (traga sua própria assinatura) do Linux, você não precisa pagar pelo software. A cobrança da BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:

  * **RHEL_BYOS**: para usar o tipo RHEL_BYOS com sucesso, habilite o Red Hat Cloud Access na sua assinatura do Azure.
  * **SLES_BYOS**: as versões BYOS do SLES incluem suporte da SUSE.

  Você pode definir o valor de LicenseType para as opções do Linux em <!JEKYLL@6100@7> e <!JEKYLL@6100@8>.

  Exemplo de configuração de LicenseType como RHEL_BYOS em <!JEKYLL@6100@9>:

  <!JEKYLL@6100@10>

  Exemplo de configuração de LicenseType como SLES_BYOS em <!JEKYLL@6100@11>:

  <!JEKYLL@6100@12>

  > **Nota:**

> Se o valor <!JEKYLL@6100@13> estiver vazio, os valores padrão serão Azure Windows Server License ou Azure Linux License, dependendo do valor de OsType.

Exemplo de configuração de LicenseType como vazio:

<!JEKYLL@6100@14>

Consulte os seguintes documentos para entender os tipos de licença e seus benefícios:

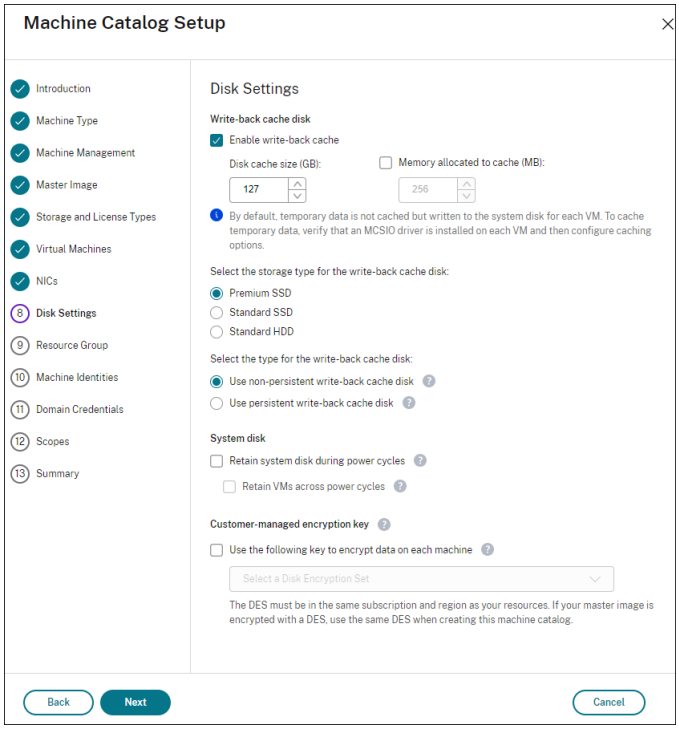
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

A Galeria de Computação do Azure (antiga Galeria de Imagens Compartilhadas do Azure) é um repositório para gerenciar e compartilhar imagens. Ele permite que você disponibilize suas imagens em toda a organização. Recomendamos que você armazene uma imagem na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite redefinições mais rápidas dos discos de SO VDA. Depois que você selecionar **Place prepared image in Azure Compute Gallery**, aparece a seção **Azure Compute Gallery settings**, permitindo que você especifique mais configurações da Galeria de Computação do Azure:

- **Ratio of virtual machines to image replicas**. Permite especificar a proporção de máquinas virtuais para réplicas de imagem que você deseja que o Azure mantenha. Por padrão, o Azure mantém uma única réplica de imagem para cada 40 máquinas não persistentes. Em máquinas persistentes, o número assume o valor padrão 1.000.
- **Maximum replica count**. Permite especificar o número máximo de réplicas de imagem que você deseja que o Azure mantenha. O padrão é 10.

> **Nota:**
>
> Uma galeria é criada no ACG para armazenar a imagem. Essa galeria é acessível somente ao MCS para criação de VMs e não aparece na página **Selecionar uma imagem**.

- Na página **Virtual Machines**, indique quantas VMs você deseja criar. Você deve especificar pelo menos um e selecionar um tamanho de máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.
- A página **NICs** não contém informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.
- Na página **Disk Settings**, escolha se deseja ativar o cache write-back. Com o recurso de otimização de armazenamento do MCS ativado, você pode definir as seguintes configurações ao criar um catálogo: Essas configurações se aplicam aos ambientes Azure e GCP.



Depois de ativar o cache de write-back, você pode fazer o seguinte:

- Configurar o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
- Selecionar o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:
  * Premium SSD
  * Standard SSD
  * Standard HDD
- Escolha se deseja que o disco de cache write-back persista para as VMs provisionadas. Selecione **Enable write-back cache** para disponibilizar as opções. Por padrão, a opção **Use non-persistent write-back cache disk** está selecionada.
- Selecione o tipo para o disco de cache de write-back.
  * **Use non-persistent write-back cache disk**. Se selecionado, o disco de cache write-back é excluído durante os ciclos de alimentação de energia. Todos os dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Template Properties**. Se o disco temporário for usado, você verá **Non-persistent Write-back Cache Disk** e seu valor será **Yes (using VM's temporary**

disk). Caso contrário, você verá **Non-persistent Write-back Cache Disk** e seu valor será **No (not using VM's temporary disk)**.

* **Use persistent write-back cache disk**. Se selecionado, o disco de cache de write-back persistirá para as VMs provisionadas. Habilitar a opção aumenta os custos de armazenamento.

- Escolha se deseja reter VMs e discos do sistema para VDAs durante os ciclos de alimentação de energia.

  Reter VM e disco do sistema durante ciclos de energia. Disponível quando você seleciona **Ativar cache de write-back**. Por padrão, VMs e discos de sistema são excluídos no desligamento e recriados na inicialização. Se você quiser reduzir o tempo de reinicialização da VM, selecione essa opção. Lembre-se de que ativar essa opção também aumenta os custos de armazenamento.

- Escolha se deseja ativar a **Economia de custos de armazenamento**. Se ativada, economize nos custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Standard quando a VM for desligada. A VM muda para suas configurações originais na reinicialização. A opção se aplica aos discos de armazenamento e cache de write-back. Como alternativa, você também pode usar o PowerShell. Consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

  > **Nota:**
  >
  > A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie as mudanças no tipo de armazenamento no futuro. Para obter mais informações, consulte este artigo da Microsoft.

- Escolha se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia no lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas no catálogo. Para obter mais informações, consulte Criptografia do servidor do Azure.

• Na página **Resource Group**, escolha se deseja criar grupos de recursos ou usar grupos existentes.

- Se você optar por criar grupos de recursos, selecione **Next**.
- Se você optar por usar grupos de recursos existentes, selecione grupos na lista **Available Provisioning Resource Groups**. **Lembre-se**: selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Será exibida uma mensagem se você escolher muito poucos. Talvez você queira selecionar mais do que o mínimo necessário se

planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que o catálogo é criado.

Para obter mais informações, consulte Azure resource groups.

- Na página **Machine Identities**, escolha um tipo de identidade e configure identidades para máquinas nesse catálogo. Se você selecionar as VMs como **Azure Active Directory joined**, poderá adicioná-las a um grupo de segurança do Azure AD. As etapas detalhadas são as seguintes:

  1. No campo **Identity type**, selecione **Azure Active Directory joined**. A opção **Azure AD security group (optional)** é exibida.
  2. Clique em **Azure AD security group: Create new**.
  3. Insira o nome do grupo e clique em **Create**.
  4. Siga as instruções na tela para fazer logon no Azure.
     Se o nome do grupo não existir no Azure, um ícone verde é exibido. Caso contrário, uma mensagem de erro é exibida solicitando que você insira um novo nome.
  5. Insira o esquema de nomenclatura da conta da máquina para as VMs.

  Após a criação do catálogo, o Citrix Virtual Apps and Desktops acessa o Azure em seu nome e cria o grupo de segurança e uma regra de associação dinâmica para o grupo. Com base na regra, as VMs com o esquema de nomenclatura especificado no catálogo são adicionadas automaticamente ao grupo de segurança.

  Adicionar VMs com um esquema de nomenclatura diferente a esse catálogo exige que você entre no Azure. O Citrix Virtual Apps and Desktops pode então acessar o Azure e criar uma regra de associação dinâmica com base no novo esquema de nomenclatura.

  Ao excluir esse catálogo, a exclusão do grupo de segurança do Azure também exige o login no Azure.

- As páginas **Domain Credentials** e **Summary** não contêm informações específicas do Azure. Siga as instruções no artigo Criar catálogos de máquinas.

Conclua o assistente.

Condições para que o disco temporário do Azure seja elegível para disco de cache write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem atendidas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.

- O tamanho escolhido da VM do Azure deve incluir um disco temporário.
- Não é necessário ativar o disco de SO efêmero
- Aceite colocar o arquivo de cache de write-back no disco temporário do Azure.
- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco do cache de write-back + espaço reservado para o arquivo de paginação + 1 GB de espaço no buffer).

Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que o disco temporário é usado para cache de write-back durante a criação do catálogo de máquinas.

Cenário	Resultado
Todas as condições para usar o disco temporário para cache write-back estão satisfeitas.	O arquivo WBC <!JEKYLL@6100@15> é colocado no disco temporário.
O disco temporário não tem espaço suficiente para o uso do cache write-back.	É criado um disco VHD <!JEKYLL@6100@16> e o arquivo WBC <!JEKYLL@6100@17> é colocado neste disco.
O disco temporário tem espaço suficiente para o uso do cache write-back, mas <!JEKYLL@6100@18> está definido como **false**.	É criado um disco VHD <!JEKYLL@6100@19> e o arquivo WBC <!JEKYLL@6100@20> é colocado neste disco.

Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la no Web Studio e nos comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Acesse o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a interface de rede e a VM. No menu **...**, na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para o provisionamento de catálogos.
3. Clique em **Adicionar à biblioteca** para modificar a especificação do modelo posteriormente.
4. Na página **Importando modelos**, insira as informações necessárias, como **Nome**, **Assinatura**, **Grupo de recursos**, **Local** e **Versão**. Clique em **Próximo: Editar modelo**.

5. Você também precisa de uma interface de rede como um recurso independente se quiser provisionar catálogos. Portanto, você deve remover todos os <!JEKYLL@6100@21> especificados na especificação do modelo. Por exemplo:

   <!JEKYLL@6100@22>

6. Crie **Revisar+Criar** e crie a especificação do modelo.
7. Na página **Especificações do modelo**, verifique a especificação do modelo que você acabou de criar. Clique na especificação do modelo. No painel esquerdo, clique em **Versões**.
8. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação do modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação do modelo.

Você pode obter informações sobre a especificação e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação do modelo, execute:

  <!JEKYLL@6100@23>

- Para obter informações sobre a versão da especificação do modelo, execute:

  <!JEKYLL@6100@24>

Usar a especificação do modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou os comandos do PowerShell.

- Para o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio
- Para o PowerShell, consulte Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell

Criptografia do servidor do Azure

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

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco está criptografado, altere a chave atual no <!JEKYLL@6100@25>. Todos os recursos associados a essa alteração de <!JEKYLL@6100@26> 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 Início rápido: criar um cofre de chaves usando o portal do Azure para obter informações sobre como configurar a criptografia do servidor do Azure.

Chave de criptografia gerenciada pelo cliente do Azure

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

- <!JEKYLL@6100@27>

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

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

Consulte Criar um catálogo de máquinas usando a chave gerenciada pelo cliente.

Criptografia de disco do Azure no host

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

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

Restrições:

A criptografia de disco do Azure no host é:

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

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

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

2. Verifique se um determinado tamanho de VM do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute uma destas opções:

   <!JEKYLL@6100@28>

   <!JEKYLL@6100@29>

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 <!JEKYLL@6100@30> como **true** dentro de <!JEKYLL@6100@31>.

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

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

   Você pode criar o catálogo de máquinas usando o Web Studio ou executando comandos do PowerShell.

Recuperar informações de criptografia no host de um perfil de máquina

Você pode recuperar a criptografia nas informações do host de um perfil de máquina executando o comando PowerShell com o parâmetro <!JEKYLL@6100@32>. Se o parâmetro <!JEKYLL@6100@33> for **True**, isso indica que a criptografia no host está habilitada para o perfil da máquina.

Por exemplo: quando a entrada do perfil da máquina for uma VM, execute o seguinte comando:

<!JEKYLL@6100@34>

Por exemplo: quando a entrada do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

<!JEKYLL@6100@35>

Criptografia dupla no disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Todos os catálogos criados com esse recurso têm todos os discos do lado do servidor criptografados com chaves gerenciadas pela

plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a chave de criptografia e os conjuntos de criptografia de disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a algoritmos de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. O sistema operacional persistente e os discos de dados, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

> **Nota:**
>
> - Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e os comandos do PowerShell. Consulte Criar um catálogo de máquinas com criptografia dupla para comandos do PowerShell.
> - Você pode usar um fluxo de trabalho não baseado em perfil de máquina ou um fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
> - Se você usar um fluxo de trabalho não baseado em perfil de máquina para criar um catálogo de máquinas, poderá reutilizar o <!JEKYLL@6100@36> armazenado.
> - Se você usa um perfil de máquina, pode usar uma especificação de VM ou modelo como uma entrada de perfil de máquina.

Limitações:

- A criptografia dupla não é suportada em Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.
- Se você desabilitar uma chave DiskEncryptionSet associada a um catálogo, as VMs do catálogo serão desativadas.
- Todos os recursos relacionados às chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você só pode criar até 50 conjuntos de criptografia de disco por região por assinatura.
- Você não pode atualizar um catálogo de máquinas que já tenha um <!JEKYLL@6100@37> com um <!JEKYLL@6100@38> diferente.

Grupos de recursos do Azure

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

Uso do grupo de recursos do Azure

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

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

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você redefina o objetivo do disco de cache para armazenar o disco de SO para uma máquina virtual habilitada para o Azure. Essa funcionalidade é útil para ambientes do Azure que exigem um disco SSD de maior desempenho em relação a um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte Criar um catálogo com discos efêmeros do Azure.

> **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.

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 <!JEKYLL@6100@39>.

Considere o seguinte:

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

Otimização de armazenamento de disco efêmero do Azure e do MCS (Machine Creation Services) (MCS I/O)

O disco de SO efêmero do Azure e o MCS I/O não podem estar ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Não é possível criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- Os parâmetros do PowerShell (<!JEKYLL@6100@40> e <!JEKYLL@6100@41>) falham com uma mensagem de erro apropriada se você os definir como **true** em <!JEKYLL@6100@42> ou <!JEKYLL@6100@43>.
- Para catálogos de máquinas existentes criados com os dois recursos ativados, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

Galeria de Computação do Azure

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

- *Galeria*: as imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- *Definição de imagem na galeria*: esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- *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 a Visão geral da Galeria de Computação do Azure.

Para obter informações sobre como criar ou atualizar um catálogo de máquinas usando uma imagem da Galeria de Computação do Azure usando o PowerShell, consulte Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida durante o uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho do perfil da máquina para criar esse catálogo. Você pode usar as especificações do modelo VM e ARM como uma entrada de perfil de máquina.

Considerações importantes sobre VMs confidenciais

As considerações importantes sobre os tamanhos de VM compatíveis e a criação de um catálogo de máquinas com VMs confidenciais são as seguintes:

- Tamanhos de VM compatíveis: as VMs confidenciais aceitam os seguintes tamanhos de VM:
  - DCasv5-series
  - DCadsv5-series
  - ECasv5-series
  - ECadsv5-series
- Crie catálogos de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com VMs confidenciais do Azure usando os comandos do Web Studio e do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquina com VMs Confidenciais do Azure. Você pode usar uma especificação de modelo ou VM como a entrada do perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar ativadas com o mesmo tipo de segurança confidencial. Os tipos de segurança são:
    * **VMGuestStateOnly**: VM confidencial com apenas o estado de convidado da VM criptografado
    * **DiskWithVMGuestState**: VM confidencial com disco do sistema operacional e estado de convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco operacional normal quanto o efêmero podem ser criptografados.

- Você pode obter informações da VM confidencial de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM usando o parâmetro AdditionalData. Por exemplo:

  <!JEKYLL@6100@44>

  Os campos de dados adicionais são:

  * DiskSecurityType
  * ConfidentialVMDiskEncryptionSetId
  * DiskSecurityProfiles

  Para obter a propriedade de computação confidencial de um tamanho de máquina, execute o seguinte comando: <!JEKYLL@6100@45>

  O campo de dados adicional é <!JEKYLL@6100@46>.

- Você não pode alterar a imagem mestre ou o perfil da máquina do tipo de segurança confidencial para não confidencial ou do tipo de segurança não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

Preparar imagens mestras e perfis de máquina

Antes de criar um conjunto de VMs confidenciais, siga estas etapas para preparar uma imagem mestre e um perfil de máquina para elas:

1. No portal do Azure, crie uma VM confidencial com configurações específicas, como:

   - **Tipo de segurança**: máquinas virtuais confidenciais
   - **Criptografia de disco do sistema operacional confidencial**: ativada.
   - **Gerenciamento de chaves**: criptografia confidencial de disco com uma chave gerenciada pela plataforma
     Para obter mais informações sobre a criação de VMs confidenciais, consulte este artigo da Microsoft.

2. Prepare a imagem mestre na VM criada. Instale os aplicativos e o VDA necessários na VM criada.

   > **Nota:**
   >
   > Não há suporte para a criação de VMs confidenciais usando VHD. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil de máquina usando uma das seguintes formas:

   - Use a VM existente criada na etapa 1 se ela tiver as propriedades de máquina necessárias.

- Se você optar por uma especificação de modelo do ARM como perfil de máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos confidenciais de VM, como *SecurityEncryptionType* e *DiskEncryptionSet* (para chave gerenciada pelo cliente). Para obter mais informações, consulte Criar uma especificação de modelo do Azure.

  > **Nota:**
  >
  > – Certifique-se de que a imagem mestre e o perfil de máquina tenham o mesmo tipo de chave de segurança.
  > – Para criar VMs confidenciais que exijam criptografia confidencial de disco do sistema operacional com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil de máquina sejam idênticos.

Criar VMs confidenciais usando comandos do Web Studio ou PowerShell

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Web Studio, siga as etapas descritas em Criar catálogos de máquinas. Lembre-se das seguintes considerações:

- Na página **Imagem**, selecione uma imagem mestre e um perfil de máquina que você preparou para a criação da VM confidencial. A seleção do perfil de máquina é obrigatória e somente os perfis que correspondam ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.
- Na página **Máquinas virtuais**, somente os tamanhos de máquina que permitem VMs confidenciais aparecem para seleção.
- Na página **Configurações do disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

Azure Marketplace

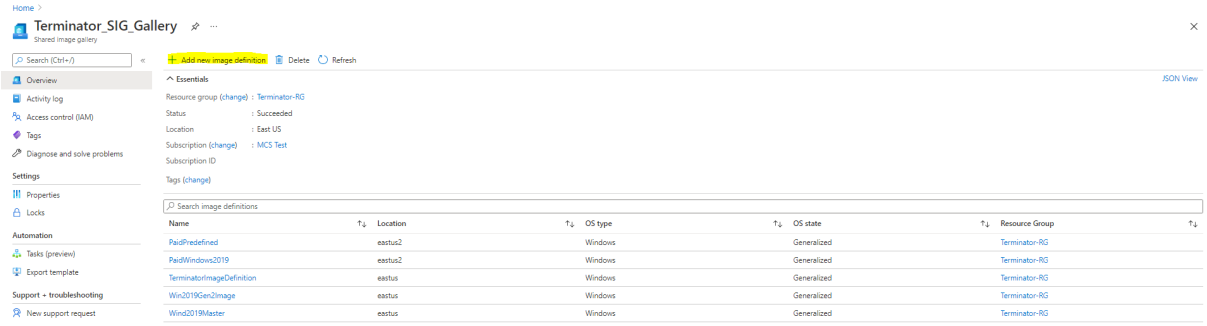
O Citrix Virtual Apps and Desktops oferece suporte ao uso de uma imagem mestre no Azure que contém informações do plano para criar um catálogo de máquina. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**
>
> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não acrescentam informações do plano. O recurso Citrix Virtual Apps and Desktops é

> para imagens pagas.

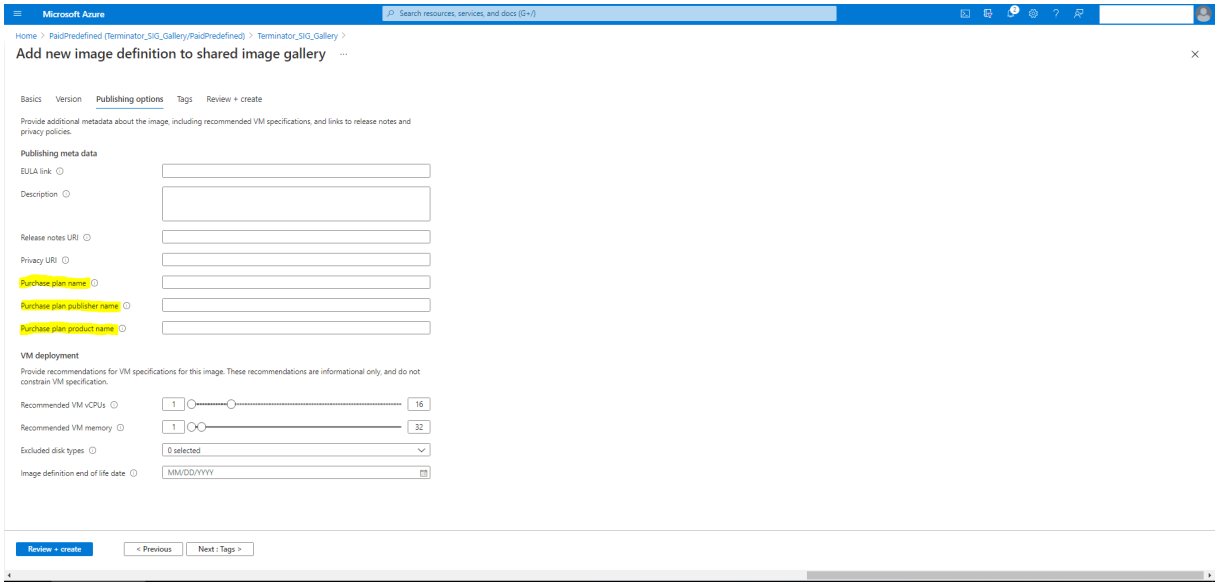
Verifique se a imagem criada na Galeria de Imagens Compartilhadas contém informações do plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Imagens Compartilhadas no Web Studio. Opcionalmente, essas imagens podem ser usadas para uma imagem mestre. Para colocar a imagem em uma Galeria de Imagens Compartilhadas, crie uma definição de imagem em uma galeria.

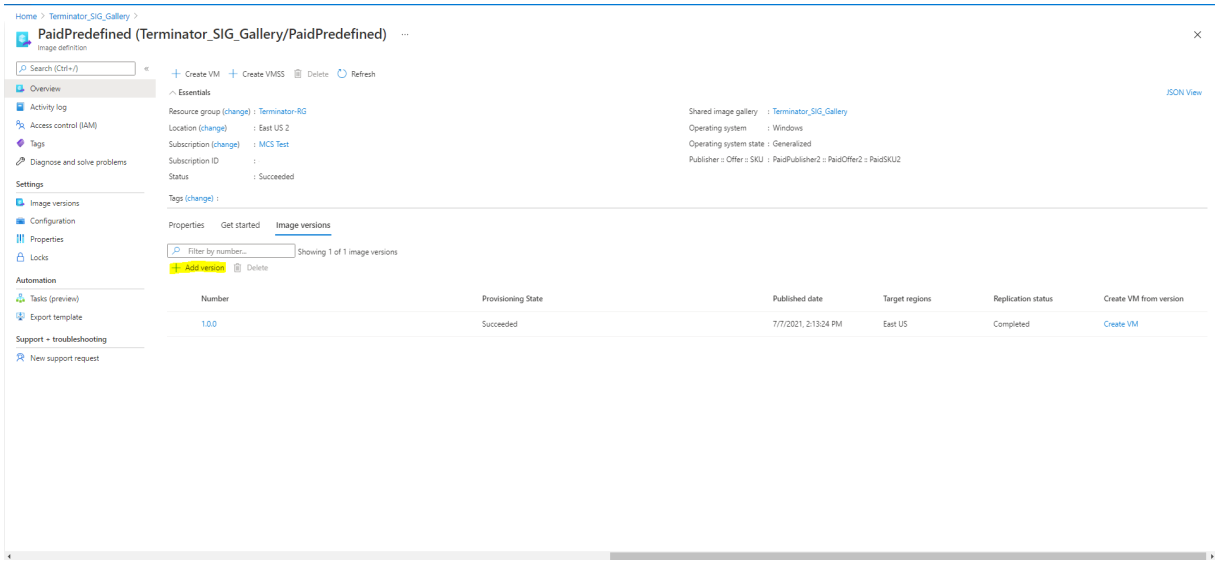


Na página **Publishing options**, verifique as informações do plano de compra.

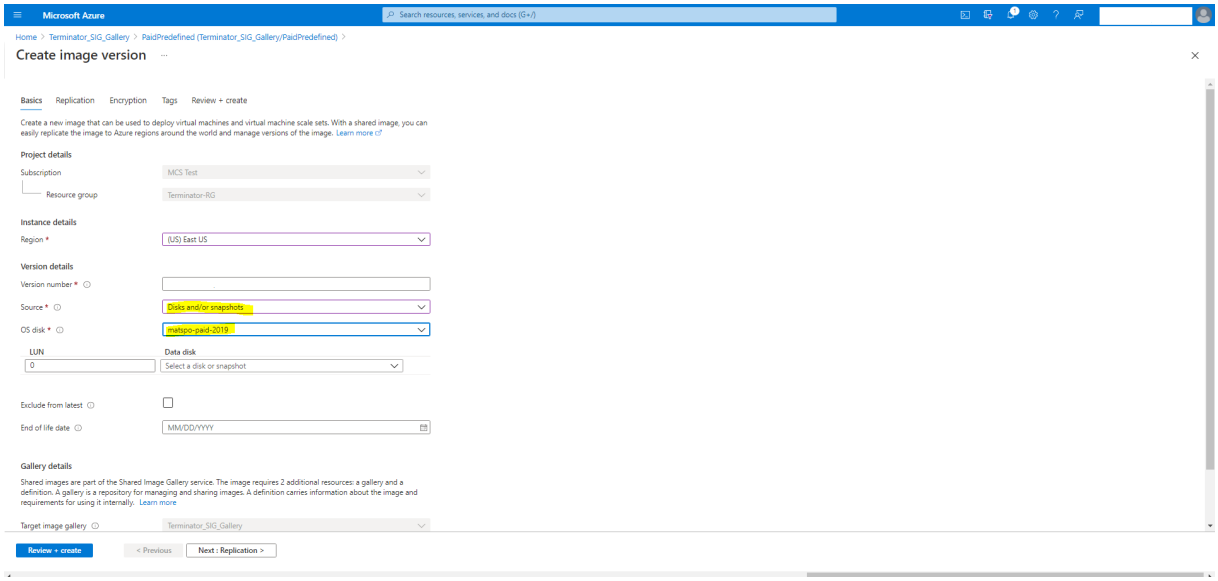
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. Se você deixar de preencher as informações do plano de compra, isso pode causar falha no processo do catálogo de máquinas.



Depois de verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Isso é usado como a imagem mestre. Clique em **Add version**:



Na seção **Version details**, selecione o instantâneo da imagem ou o disco gerenciado como origem:



Criar um catálogo de máquinas usando o PowerShell

Esta seção detalha como você pode criar catálogos usando o PowerShell:

- Criar um catálogo com disco de cache de write-back não persistente
- Criar um catálogo com disco de cache de write-back não persistente
- Melhorar o desempenho de inicialização com o MCSIO
- Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell
- Catálogos de máquinas com início confiável
- Usar valores de propriedades do perfil da máquina
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente
- Criar um catálogo de máquinas com criptografia dupla
- Criar um catálogo com discos efêmeros do Azure
- Hosts dedicados do Azure
- Criar ou atualizar um catálogo de máquinas usando a imagem da Galeria de Computação do Azure
- Configurar a Galeria de Imagens Compartilhadas
- Provisionar máquinas em zonas de disponibilidade especificadas
- Tipos de armazenamento
- Localização do arquivo de paginação
- Atualizar configuração do arquivo de página
- Criar um catálogo usando VMs do Azure Spot
- Configurar tamanhos de VM de backup
- Copiar marcas em todos os recursos
- Provisionar VMs do catálogo com o Azure Monitor Agent instalado

Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back não persistente, use o parâmetro do PowerShell <!JEKYLL@6100@47>. A propriedade personalizada <!JEKYLL@6100@48> indica se você está aceitando usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como true durante a execução <!JEKYLL@6100@49> se você quiser usar o disco temporário como disco de cache write-back. Se essa propriedade não for especificada, o parâmetro será definido como **False** por padrão.

Por exemplo, uso do parâmetro <!JEKYLL@6100@50> para definir <!JEKYLL@6100@51> como **true**:

<!JEKYLL@6100@52>

> **Nota:**
>
> Depois de confirmar o catálogo da máquina para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar o VHD posteriormente.

Criar um catálogo com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro do PowerShell <!JEKYLL@6100@53>. Esse parâmetro suporta uma propriedade extra, <!JEKYLL@6100@54>, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas MCS. A propriedade <!JEKYLL@6100@55> só é usada quando o parâmetro <!JEKYLL@6100@56> é especificado, e quando o parâmetro <!JEKYLL@6100@57> é definido para indicar que um disco foi criado.

Exemplos de propriedades encontradas no parâmetro <!JEKYLL@6100@58> antes do suporte a <!JEKYLL@6100@59> incluem:

<!JEKYLL@6100@60>

Ao usar essas propriedades, considere que elas contêm valores padrão se as propriedades forem omitidas do parâmetro <!JEKYLL@6100@61>. A propriedade <!JEKYLL@6100@62> tem dois valores possíveis: **true** ou **false**.

Definir a propriedade <!JEKYLL@6100@63> 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 <!JEKYLL@6100@64> 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 <!JEKYLL@6100@65> 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 <!JEKYLL@6100@66> para definir <!JEKYLL@6100@67> como true:

<!JEKYLL@6100@68>

> **Importante:**
>
> A propriedade <!JEKYLL@6100@69> só pode ser definida usando o cmdlet <!JEKYLL@6100@70> do PowerShell. Tentar alterar <!JEKYLL@6100@71> 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 <!JEKYLL@6100@72> para usar o cache de write-back ao definir a propriedade <!JEKYLL@6100@73> como true:

<!JEKYLL@6100@74>

Melhorar o desempenho de inicialização com o MCSIO

Você pode melhorar o desempenho de inicialização dos discos gerenciados do Azure e do GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada do PowerShell <!JEKYLL@6100@75> no comando <!JEKYLL@6100@76> para configurar esse recurso. As opções associadas a <!JEKYLL@6100@77> são:

<!JEKYLL@6100@78><!JEKYLL@6100@79><!JEKYLL@6100@80>

Para ativar esse recurso, defina a propriedade personalizada <!JEKYLL@6100@81> como <!JEKYLL@6100@82>. Por exemplo:

<!JEKYLL@6100@83>

Usar a especificação do modelo na criação ou atualização de um catálogo usando o PowerShell

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Web Studio ou os comandos do PowerShell.

Para o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio

Usando comandos do PowerShell:

1. Abra a janela do **PowerShell**.
2. Execute <!JEKYLL@6100@84>.
3. Crie ou atualize um catálogo.

    - Para criar um catálogo:
        a) Use o comando <!JEKYLL@6100@85> com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

        <!JEKYLL@6100@86>

        b) Conclua a criação do catálogo.
    - Para atualizar um catálogo, use o comando <!JEKYLL@6100@87> com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

    <!JEKYLL@6100@88>

Catálogos de máquinas com início confiável

Para criar com êxito um catálogo de máquinas com início confiável, use:

- Um perfil de máquina com início confiável
- Um tamanho de VM que ofereça suporte ao início confiável
- Uma versão de VM do Windows que ofereça suporte ao início confiável. Atualmente, o Windows 10, o Windows 11 e o Windows Server 2016, 2019 e 2022 oferecem suporte ao início confiável.

> **Importante:**
>
> O MCS oferece suporte à criação de um novo catálogo com VMs habilitadas para o início confiável. No entanto, para atualizar um catálogo persistente existente e as VMs existentes, você precisa usar o portal do Azure. Você não pode atualizar o início confiável de um catálogo não persistente. Para obter mais informações, consulte o documento da Microsoft Habilitar o Início confiável em VMs existentes do Azure.

Para exibir os itens de inventário da oferta do Citrix Virtual Apps and Desktops e determinar se o tamanho da VM oferece suporte ao início confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos do PowerShell específicos à Citrix.
3. Execute o seguinte comando:

    <!JEKYLL@6100@89>

4. Execute <!JEKYLL@6100@90>
5. Verifique o valor do atributo <!JEKYLL@6100@91>.

- Se <!JEKYLL@6100@92> for **True**, o tamanho da VM oferecerá suporte ao início confiável.
- Se <!JEKYLL@6100@93> for **False**, o tamanho da VM não oferecerá suporte ao início confiável.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que oferecem suporte ao início confiável:

<!JEKYLL@6100@94>

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 <!JEKYLL@6100@95> 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 <!JEKYLL@6100@96> for **True**, o tamanho da VM de Geração 2 não será compatível com o início confiável.
- *Exemplo 3*: se a VM do Azure oferecer suporte somente à Geração 2 e o recurso <!JEKYLL@6100@97> não for exibido após a execução do comando PowerShell, o tamanho da VM de Geração 2 não será 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.

Criar um catálogo de máquinas com início confiável

1. Crie uma imagem mestre habilitada com o início confiável. Consulte a documentação da Microsoft Imagens da VM de início confiável.
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de início confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft Implantar uma VM de início confiável.
3. Crie um catálogo de máquinas usando os comandos do Web Studio ou do PowerShell.
   - Se você quiser usar o Web Studio, consulte Criar um catálogo de máquinas por meio de uma imagem do Azure Resource Manager no Web Studio.
   - Se você quiser usar os comandos do PowerShell, use o comando <!JEKYLL@6100@98> com a VM ou especificação de modelo como uma entrada de perfil de máquina. Para obter a lista completa de comandos para criar um catálogo, consulte Criação de um catálogo.

     Exemplo de <!JEKYLL@6100@99> com a VM como entrada de perfil de máquina:

     <!JEKYLL@6100@100>

Exemplo de <!JEKYLL@6100@101> com a especificação de modelo como entrada de perfil de máquina:

<!JEKYLL@6100@102>

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	<!JEKYLL@6100@103>
Se você selecionar um perfil de máquina compatível com início confiável ao criar um catálogo com disco não gerenciado como imagem mestre	<!JEKYLL@6100@104>
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	<!JEKYLL@6100@105>
Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre	<!JEKYLL@6100@106>
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	<!JEKYLL@6100@107>

Usar valores de propriedades do perfil da máquina

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

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

- Tipo de armazenamento

Se essas propriedades personalizadas não forem definidas explicitamente, os valores da propriedade serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como o perfil da máquina. Além disso, se <!JEKYLL@6100@108> 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 <!JEKYLL@6100@109> e <!JEKYLL@6100@110> quando <!JEKYLL@6100@111> 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:

    <!JEKYLL@6100@112>

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

    <!JEKYLL@6100@113>
  - MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem somente LicenseType e OsType.

    <!JEKYLL@6100@114>

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

    <!JEKYLL@6100@115>
  - Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

    <!JEKYLL@6100@116>

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

    <!JEKYLL@6100@117>
  - 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

<!JEKYLL@6100@118>

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

<!JEKYLL@6100@119>

- 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

<!JEKYLL@6100@120>

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

<!JEKYLL@6100@121>

- 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:

<!JEKYLL@6100@122>

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

<!JEKYLL@6100@123>

- Cenários Set-ProvScheme
  - Um catálogo existente com:
    - CustomProperties para <!JEKYLL@6100@124> e OsType
    - MachineProfile <!JEKYLL@6100@125> que define Zones
  - Atualizações:
    - MachineProfile mpB.vm que define StorageAccountType
    - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define LicenseType e OsType

<!JEKYLL@6100@126>

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

<!JEKYLL@6100@127>

- Um catálogo existente com:
  - CustomProperties para S<!JEKYLL@6100@128> e OsType
  - MachineProfile <!JEKYLL@6100@129> que define StorageAccountType e LicenseType

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

<!JEKYLL@6100@130>

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

<!JEKYLL@6100@131>

- Um catálogo existente com:
  - CustomProperties para <!JEKYLL@6100@132> e OsType
  - MachineProfile <!JEKYLL@6100@133> que define Zones
- Atualizações:
  - Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  - <!JEKYLL@6100@134> não está especificado

<!JEKYLL@6100@135>

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

<!JEKYLL@6100@136>

Provisionar VMs do catálogo com o Azure Monitor Agent instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e atuar nos dados de telemetria de seus ambientes do Azure e locais.

O Azure Monitor Agent (AMA) coleta dados de monitoramento de recursos computacionais, como máquinas virtuais, e entrega os dados para o Azure Monitor. Atualmente, ele oferece suporte à coleção de métricas de Logs de eventos, Syslog e Desempenho e a envia para fontes de dados do Azure Monitor Metrics e do Azure Monitor Logs.

Para habilitar o monitoramento identificando de forma exclusiva as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

Requisitos

- Permissões: verifique se você tem as permissões mínimas do Azure, conforme especificado em Permissões necessárias do Azure, e as seguintes permissões para usar o Azure Monitor:
  - <!JEKYLL@6100@137>
  - <!JEKYLL@6100@138>

  - <!JEKYLL@6100@139>
  - <!JEKYLL@6100@140>
  - <!JEKYLL@6100@141>

- Regra de coleta de dados: configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar um DCR, consulte Criar uma regra de coleta de dados. Um DCR é específico da plataforma (Windows ou Linux). Certifique-se de criar um DCR de acordo com a plataforma necessária.
  A AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e fontes de dados, como Azure Monitor Metrics e Azure Monitor Logs.
- Espaço de trabalho padrão: crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um espaço de trabalho, consulte Criar um espaço de trabalho do Log Analytics. Quando você coleta logs e dados, as informações são armazenadas em um espaço de trabalho. Um espaço de trabalho tem um ID de espaço de trabalho e um ID de recurso exclusivos. O nome do espaço de trabalho deve ser exclusivo para um determinado grupo de recursos. Depois de criar um espaço de trabalho, configure fontes de dados e soluções para armazenar seus dados no espaço de trabalho.
- Incluiu a extensão do monitor na lista branca: as extensões <!JEKYLL@6100@142> e <!JEKYLL@6100@143> são extensões definidas na lista branca da Citrix. Para ver a lista de extensões na lista branca, use o comando PoSH <!JEKYLL@6100@144>.
- Imagem mestre: a Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso poderá levar a arquivos remanescentes e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para provisionar VMs de catálogo com o AMA ativado:

1. Configure um modelo de perfil de máquina.
   - Se você quiser usar uma máquina virtual como modelo de perfil de máquina:
     a) Crie uma VM no portal do Azure.
     b) Ligue a VM.
     c) Adicione a VM à regra de coleta de dados em **Resources**. Isso invoca a instalação do agente na VM modelo.

     > **Nota:**
     >
     > Se você precisar criar um catálogo Linux, configure uma máquina Linux.

   - Se você quiser usar a especificação do modelo como modelo de um perfil de máquina:
     a) Configure uma especificação de modelo.

b) Adicione a seguinte associação de extensão e regra de coleta de dados à especificação do modelo gerado:

<!JEKYLL@6100@145>

2. Crie ou atualize um catálogo de máquinas MCS existente.

   - Para criar um novo catálogo MCS:

     a) Selecione essa de VM ou especificação modelo como um perfil de máquina no Web Studio.
     b) Continue com as próximas etapas para criar o catálogo.

   - Para atualizar um catálogo MCS existente, use os seguintes comandos PoSH:

     – Para que as novas VMs obtenham o modelo de perfil de máquina atualizado, execute o seguinte comando:

       <!JEKYLL@6100@146>

     – Para atualizar as VMs existentes com o modelo de perfil de máquina atualizado:

       <!JEKYLL@6100@147>

3. Ligue as máquinas virtuais do catálogo.
4. Acesse o portal do Azure e verifique se a extensão do monitor está instalada na VM e se a VM aparece nos recursos do DCR. Depois de alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

Solução de problemas

Para obter informações para orientar a solução de problemas do agente do Azure Monitor, consulte o seguinte:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

As etapas detalhadas sobre como criar um catálogo de máquinas com a chave de criptografia gerenciada pelo cliente são:

1. Abra uma janela do PowerShell.

2. Execute o comando <!JEKYLL@6100@148> para carregar os módulos do PowerShell específicos da Citrix.
3. Digite <!JEKYLL@6100@149>.
4. Digite <!JEKYLL@6100@150>.
5. Digite <!JEKYLL@6100@151>.
6. Digite <!JEKYLL@6100@152> para obter a lista de Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma cadeia de caracteres de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

   <!JEKYLL@6100@153>
9. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

   <!JEKYLL@6100@154>
10. Execute o comando New-ProvScheme. Por exemplo:

    <!JEKYLL@6100@155>
11. Conclua a criação do catálogo de máquinas.

Criar um catálogo de máquinas com criptografia dupla

Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Web Studio e os comandos do PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e um DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Usar o portal do Azure para habilitar a criptografia dupla inativa para discos gerenciados.
2. Para procurar os DiskEncryptionSets disponíveis em sua conexão de hospedagem:
   a) Abra uma janela do **PowerShell**.
   b) Execute os seguintes comandos do PowerShell:
      i. <!JEKYLL@6100@156>
      ii. <!JEKYLL@6100@157>
      iii. <!JEKYLL@6100@158>
      iv. <!JEKYLL@6100@159> (ex.: azure-east)
      v. <!JEKYLL@6100@160>
      vi. <!JEKYLL@6100@161>

Você pode usar um ID do <!JEKYLL@6100@162> para criar ou atualizar um catálogo usando propriedades personalizadas.

3. Se você quiser usar o fluxo de trabalho do perfil da máquina, crie uma especificação de VM ou modelo como entrada do perfil da máquina.

   - Se você quiser usar uma VM como entrada de perfil de máquina:
     a) Crie uma VM no Portal do Azure.
     b) Navegue até **Disks>Key management** para criptografar a VM diretamente com um <!JEKYLL@6100@163>.
   - Se você quiser usar uma especificação de modelo como entrada de perfil de máquina:
     a) No modelo, em <!JEKYLL@6100@164>, adicione o parâmetro <!JEKYLL@6100@165> e adicione o ID do DES de criptografia dupla.

4. Crie o catálogo de máquinas.

   - Se estiver usando o Web Studio, siga um dos procedimentos a seguir, além das etapas em Criar catálogos de máquinas.
     - Se você não usar o fluxo de trabalho baseado em perfil de máquina, na página **Configurações do disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla no menu suspenso. Continue a criar o catálogo.
     - Se estiver usando o fluxo de trabalho do perfil da máquina, na página **Imagem**, selecione uma imagem mestre e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID do conjunto de criptografia de disco em suas propriedades.

     Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.
   - Se estiver usando comandos do PowerShell, faça o seguinte:
     - Se não estiver usando o fluxo de trabalho baseado no perfil da máquina, adicione a propriedade personalizada <!JEKYLL@6100@166> no <!JEKYLL@6100@167> comando. Por exemplo:

       <!JEKYLL@6100@168>

     - Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando <!JEKYLL@6100@169>. Por exemplo:

       <!JEKYLL@6100@170>

5. Conclua a criação do catálogo usando o SDK remoto 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/.

Todas as máquinas criadas no catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina) somente se o catálogo não tiver sido criptografado anteriormente.

- Se não estiver usando o fluxo de trabalho baseado no perfil da máquina, adicione a propriedade personalizada DiskEncryptionSetId no comando <!JEKYLL@6100@171>. Por exemplo:

  <!JEKYLL@6100@172>

- Se estiver usando um fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando <!JEKYLL@6100@173>. Por exemplo:

  <!JEKYLL@6100@174>

Depois de bem-sucedidas, todas as novas VMs que você adiciona ao seu catálogo são criptografadas duas vezes pela chave associada ao DES selecionado.

Verificar se o catálogo está criptografado duas vezes

- No Web Studio:

  1. Navegue até **Machine Catalogs**.
  2. Selecione o catálogo que você deseja verificar. Clique na guia **Template Properties** localizada na parte inferior da tela.
  3. Em **Azure Details**, verifique o ID do conjunto de criptografia de disco em **Disk Encryption Set**. Se o ID do DES do catálogo estiver em branco, o catálogo não está criptografado.
  4. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.

- Usando o comando do PowerShell:

  1. Abra a janela do **PowerShell**.
  2. Execute o comando <!JEKYLL@6100@175> para carregar os módulos do PowerShell específicos da Citrix.
  3. Use <!JEKYLL@6100@176> para obter as informações do seu catálogo de máquinas. Por exemplo:

     <!JEKYLL@6100@177>

4. Recupere a propriedade personalizada DES Id do catálogo da máquina. Por exemplo:

   <!JEKYLL@6100@178>

5. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES são chaves gerenciadas pela plataforma e pelo cliente.

Criar um catálogo com discos efêmeros do Azure

Para usar discos efêmeros, você deve definir a propriedade personalizada <!JEKYLL@6100@179> como **true** ao executar <!JEKYLL@6100@180>.

> **Nota:**
>
> Se a propriedade personalizada <!JEKYLL@6100@181> 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:

<!JEKYLL@6100@182>

Configurar um disco efêmero para um catálogo

Para configurar um disco de SO efêmero do Azure para um catálogo, use o parâmetro <!JEKYLL@6100@183> em <!JEKYLL@6100@184>. Defina o valor do parâmetro <!JEKYLL@6100@185> como **true**.

> **Nota:**
>
> Para usar esse recurso, você também deve habilitar os parâmetros <!JEKYLL@6100@186> e <!JEKYLL@6100@187>.

Por exemplo:

<!JEKYLL@6100@188>

Considerações importantes para discos efêmeros

Para provisionar discos de sistema operacional efêmeros usando <!JEKYLL@6100@189>, considere as seguintes restrições:

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

- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também esses problemas nas seguintes situações:

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

Hosts dedicados do Azure

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

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

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

<!JEKYLL@6100@190>

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 <!JEKYLL@6100@191>.
- 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.

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

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

Para que essas imagens apareçam, você deve:

1. Configurar um site do Citrix Virtual Apps and Desktops.
2. Conectar-se ao Azure Resource Manager.

3. No portal do Azure, criar um grupo de recursos. Para obter detalhes, consulte Criar uma Galeria de Computação do Azure usando o portal.
4. No grupo de recursos, crie uma Galeria de Computação do Azure.
5. Na Galeria de Computação do Azure, crie uma definição de imagem.
6. Na definição da imagem, crie uma versão da imagem.

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

1. Abra uma janela do PowerShell.
2. Execute o comando <!JEKYLL@6100@192> para carregar os módulos do PowerShell específicos da Citrix.
3. Selecione um grupo de recursos e liste todas as galerias do grupo de recursos.

   <!JEKYLL@6100@193>
4. Selecione uma galeria e liste todas as definições de imagem da galeria.

   <!JEKYLL@6100@194>
5. Selecione uma definição de imagem e liste todas as versões da definição de imagem.

   <!JEKYLL@6100@195>
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 <!JEKYLL@6100@196> para criar um esquema de provisionamento com suporte à Galeria de Imagens Compartilhadas. Use o comando <!JEKYLL@6100@197> 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:

<!JEKYLL@6100@198>

- 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**.

<!JEKYLL@6100@199>

- 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.

<!JEKYLL@6100@200>

- 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 <!JEKYLL@6100@201> para atualizar as propriedades personalizadas para todas as máquinas existentes no catálogo e quaisquer máquinas futuras:

<!JEKYLL@6100@202>

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

Para esse caso de uso:

1. Execute <!JEKYLL@6100@203> com o sinalizador <!JEKYLL@6100@204> definido como **True**. Opcionalmente, inclua as propriedades <!JEKYLL@6100@205> e <!JEKYLL@6100@206>.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

<!JEKYLL@6100@207>

> **Dica:**
>
> Os parâmetros <!JEKYLL@6100@208> e <!JEKYLL@6100@209> não são necessários. Após a conclusão do comando <!JEKYLL@6100@210>, 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 <!JEKYLL@6100@211> com o sinalizador <!JEKYLL@6100@212> definido como **False** ou não definido.
2. Atualizar o catálogo.
3. Aplique um ciclo de energia nas máquinas para forçar uma atualização.

Por exemplo:

<!JEKYLL@6100@213>

> **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: <!JEKYLL@6100@214>. Depois que o comando <!JEKYLL@6100@215> 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 <!JEKYLL@6100@216> 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.

Configurar zonas de disponibilidade por meio do PowerShell

Com o PowerShell, você pode visualizar os itens de inventário oferecidos usando <!JEKYLL@6100@217>. Por exemplo, para visualizar a oferta de serviços da *Eastern US region* <!JEKYLL@6100@218>:

<!JEKYLL@6100@219>

Para visualizar as zonas, use o parâmetro <!JEKYLL@6100@220> para o item:

<!JEKYLL@6100@221>

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 <!JEKYLL@6100@222>. 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, <!JEKYLL@6100@223> para as zonas 1 e 3.

Use o comando <!JEKYLL@6100@224> 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.

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:**
>
> <!JEKYLL@6100@225> está configurado para um tipo de sistema operacional e uma conta de armazenamento. <!JEKYLL@6100@226> está configurado para o tipo de armazenamento em cache de write-back. Para um catálogo normal, é necessário <!JEKYLL@6100@227>. Se <!JEKYLL@6100@228> não estiver configurado, <!JEKYLL@6100@229> será usado como padrão para <!JEKYLL@6100@230>.

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

Configurar tipos de armazenamento

Para configurar os tipos de armazenamento para a VM, use o parâmetro <!JEKYLL@6100@231> em <!JEKYLL@6100@232>. Defina o valor do parâmetro <!JEKYLL@6100@233> como um dos tipos de armazenamento compatíveis.

Veja a seguir um exemplo de conjunto do parâmetro <!JEKYLL@6100@234> em um esquema de provisionamento:

<!JEKYLL@6100@235>

Habilitar o armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica de forma síncrona seu disco gerenciado do Azure em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser definido usando propriedades personalizadas existentes ou por meio do modelo **MachineProfile**. O armazenamento ZRS também é compatível com o comando <!JEKYLL@6100@236> com os parâmetros <!JEKYLL@6100@237> e <!JEKYLL@6100@238>, e você pode alterar a máquina existente do armazenamento LRS para o ZRS.

Limitações:

- Compatível somente com discos gerenciados
- Compatível apenas com unidades de estado sólido (SSD) premium e standard
- Não compatível com <!JEKYLL@6100@239>
- Disponível somente em determinadas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em grande escala. Portanto, para a primeira ativação, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

Defina o armazenamento com redundância de zona como o tipo de armazenamento em disco
Você pode selecionar armazenamento com redundância de zona durante a criação do catálogo inicial ou atualizar seu tipo de armazenamento em um catálogo existente.

Selecionar armazenamento com redundância de zona usando comandos do PowerShell Ao criar um novo catálogo no Azure usando o comando <!JEKYLL@6100@240> do PowerShell, use <!JEKYLL@6100@241> como o valor em <!JEKYLL@6100@242>.
Por exemplo:

<!JEKYLL@6100@243>

Ao definir esse valor, ele é validado por uma API dinâmica que determina se ele pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso do ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: a propriedade personalizada StorageTypeAtShutdown não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: essa exceção ocorre se você tentar usar o Armazenamento ZRS em uma região do Azure que não oferece suporte a ZRS
- **ZrsRequiresManagedDisks**: você pode usar armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento em disco usando as seguintes propriedades personalizadas:

- <!JEKYLL@6100@244>
- <!JEKYLL@6100@245>
- <!JEKYLL@6100@246>

> **Nota:**
>
> Durante a criação do catálogo, o disco do sistema operacional do perfil da máquina <!JEKYLL@6100@247> é usado se as propriedades personalizadas não estiverem definidas.

Capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs a partir de um perfil de máquina enquanto cria um catálogo de máquinas, atualiza um catálogo de máquinas existente e atualiza as VMs existentes.

Você pode criar uma VM ou especificação de modelo como fonte de perfil de máquina.

Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação de modelo.
    - Storage account
    - Espaço de trabalho de análise de logs
    - Namespace do hub de eventos com preços de nível padrão
2. Crie uma fonte de perfil de máquina.
3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize as VMs existentes.

Configurar os IDs necessários no Azure

Configure uma das seguintes opções no Azure:

- Storage account
- Espaço de trabalho de análise de logs
- Namespace do hub de eventos com preços de nível padrão

Configurar uma conta de armazenamento Crie uma conta de armazenamento padrão no Azure. Na especificação de modelo, forneça o resourceId completo da conta de armazenamento como o <!JEKYLL@6100@248>.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, os dados podem ser encontrados no contêiner <!JEKYLL@6100@249>.

Configurar um espaço de trabalho de análise de logs Crie um espaço de trabalho de análise de logs. Na especificação de modelo, forneça o resourceId completo para o espaço de trabalho de análise de logs como workspaceId.

Depois que as VMs são configuradas para registrar dados no espaço de trabalho, os dados podem ser consultados em Logs no Azure. Você pode executar o seguinte comando no Azure em Logs para mostrar uma contagem de todas as métricas registradas por um recurso:

‘AzureMetrics

Configurar um hub de eventos Faça o seguinte para configurar um hub de eventos no portal do Azure:

1. Crie um namespace de hub de eventos com o preço de nível padrão.
2. Crie um hub de eventos abaixo do namespace.
3. Navegue até **Capturar** no hub de eventos. ATIVE o seletor para capturar com o tipo de saída Avro.
4. Crie um novo contêiner em uma conta de armazenamento existente para capturar os logs.
5. Na especificação de modelo, especifique o `eventHubAuthorizationRuleId` no seguinte formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique o nome do hub de eventos.

Depois que as VMs são configuradas para registrar dados no hub de eventos, os dados são capturados no contêiner de armazenamento configurado.

Criar uma fonte de perfil de máquina

Você pode criar uma VM ou especificação de modelo como fonte de perfil de máquina.

Criar um perfil de máquina baseado em VM com configurações de diagnóstico Se você quiser criar uma VM como seu perfil de máquina, primeiro defina as configurações de diagnóstico na própria

VM de modelo. Você pode consultar as instruções detalhadas fornecidas na documentação da Microsoft Configurações de diagnóstico no Azure Monitor.

Você pode executar os seguintes comandos para verificar se agora há configurações de diagnóstico associadas à VM ou à NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

Criar um modelo de perfil de máquina baseado em especificações com configurações de diagnóstico Se você quiser usar uma VM que já tenha as configurações de diagnóstico habilitadas e exportá-la para uma especificação de modelo do ARM, essas configurações não serão incluídas automaticamente no modelo. Você deve adicionar ou modificar manualmente as configurações de diagnóstico no modelo do ARM.

No entanto, se você quiser uma VM como perfil de sua máquina, o MCS garante que as configurações críticas de diagnóstico sejam capturadas e aplicadas com precisão aos recursos em seu catálogo do MCS.

1. Crie uma especificação de modelo padrão que defina uma VM e NIC(s).
2. Adicione recursos adicionais para implantar as configurações de diagnóstico de acordo com a especificação: Microsoft.Insights diagnosticSettings. Para obter o escopo, faça referência a uma VM ou NIC que esteja no modelo pelo nome com uma ID parcial. Por exemplo, para criar configurações de diagnóstico anexadas a uma VM chamada test-VM na especificação de modelo, especifique o escopo como:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use a especificação de modelo como uma fonte de perfil de máquina.

Criar ou atualizar um catálogo com configurações de diagnóstico

Depois de criar uma fonte de perfil de máquina, agora você pode criar um catálogo de máquinas usando o comando `New-ProvScheme`, atualizar um catálogo de máquinas existente usando o comando `Set-ProvScheme` e atualizar as VMs existentes usando o comando `Request-ProvVMUpdate`.

Localização do arquivo de paginação

Em ambientes do Azure, o arquivo de paginação é configurado no local apropriado quando a VM é criada. A configuração do arquivo de paginação é definida no formato <page file location >[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 página

Você também pode especificar a configuração do arquivo de paginação, incluindo o local e o tamanho, usando explicitamente o comando do the PowerShell. Isso substitui o valor determinado pelo MCS. Você pode fazer isso executando o comando `New-ProvScheme` e incluindo as seguintes

propriedades personalizadas:

- `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>'
```

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.

Criar um catálogo usando VMs do Azure Spot

As VMs do Azure Spot permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa. No entanto, a capacidade de alocar uma VM do Azure Spot depende da capacidade e do preço atuais. Portanto, o Azure pode expulsar sua VM em execução, falhar ao criar a VM ou não ligar a VM de acordo com a política de despejo. Portanto, as VMs do Azure

Spot são boas para alguns aplicativos e áreas de trabalho não críticos. Para obter mais informações, consulte Usar máquinas virtuais do Azure Spot.

Limitações

- Nem todos os tamanhos de VM são compatíveis com as VMs do Azure Spot. Para obter mais informações, consulte Limitações.

  Você pode executar o seguinte comando do PowerShell para verificar se um tamanho de VM oferece suporte a VMs do Spot ou não. Se um tamanho de VM oferecer suporte à VM do Spot, então `SupportsSpotVM` será **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
     folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  ```

- Atualmente, as VMs do Azure Spot não oferecem suporte à hibernação.

Requisito

Ao criar a fonte do perfil de máquina (VM ou especificação de modelo) para o catálogo de VMs do Azure Spot, você deve selecionar Instância do Azure Spot (se estiver usando a VM) ou definir `priority` como `Spot` (se estiver usando a especificação de modelo).

Etapas para criar um catálogo usando VMs do Azure Spot

1. Criar uma fonte de perfil de máquina (VM ou modelo de inicialização).
   - Para criar uma VM usando o portal do Azure, consulte Implantar máquinas virtuais do Azure Spot usando o portal do Azure.
   - Para criar uma especificação de modelo, adicione as seguintes propriedades em **resources > type: Microsoft.Compute/virtualMachines > properties** na especificação de modelo. Por exemplo:

     ```
     "priority": "Spot",
     "evictionPolicy": "Deallocate",
     "billingProfile": {

     "maxPrice": 0.01
      }
     ```

     > **Nota:**
     >
     > - A política de despejo pode ser **Desalocar** ou **Excluir**.

  - Para VMs não persistentes, o MCS sempre define a política de despejo como **Excluir**. Se a VM for despejada, ela será excluída junto com todos os discos não persistentes (por exemplo, disco do sistema operacional). Nenhum disco permanente (por exemplo, disco de identidade) não é excluído. No entanto, um disco do sistema operacional será persistente se o tipo de catálogo for persistente ou se a propriedade personalizada `PersistOsDisk` estiver definida como True. Da mesma forma, um disco do WBC será persistente se a propriedade personalizada `PersistWbc` estiver definida como **True**.
  - Para VMs persistentes, o MCS sempre define a política de despejo como Desalocar. Se a VM for despejada, ela será desalocada. Nenhuma alteração é feita nos discos.
- O preço máximo é o preço que você está disposto a pagar por hora. Se você estiver usando **Somente capacidade**, isso será **-1**. O preço máximo só pode ser nulo, -1 ou um decimal maior que zero. Para obter mais informações, consulte Preços.

2. Você pode executar o seguinte comando do PowerShell para verificar se um perfil de máquina está habilitado para a VM do Azure Spot ou não. Se o parâmetro `SpotEnabled` for **True** e `SpotEvictionPolicy` estiver definido como **Desalocar** ou **Excluir**, o perfil de máquina estará habilitado para a VM do Azure Spot. Por exemplo,

   - Se a fonte do perfil de máquina for uma VM, execute o seguinte comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   ```

   - Se a fonte do perfil de máquina for uma especificação de modelo, execute o seguinte comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   ```

3. Crie um catálogo de máquinas usando um perfil de máquina com o comando `New-ProvScheme` do PowerShell.

Você pode atualizar um catálogo usando o comando `Set-ProvScheme`. Você também pode atualizar as VMs existentes usando o comando `Set-ProvVmUpdateTimeWindow` do PowerShell. O perfil de máquina é atualizado na próxima inicialização.

Despejos em uma VM do Azure Spot em execução

Se a capacidade de computação não estiver disponível ou o preço por hora for maior do que o preço máximo conforme configurado, o Azure despejará uma VM do Spot em execução. Por padrão, você

não é notificado sobre um despejo. A VM simplesmente congela e é despejada. A Microsoft recomenda o uso de eventos agendados para monitorar despejos. Consulte Monitorar continuamente o despejo. Você também pode executar scripts em uma VM para receber uma notificação antes do despejo. Por exemplo, a Microsoft tem um script de pesquisa em ScheduledEvents.cs do Python.

Solução de problemas

- Você pode ver as propriedades da VM do Spot em customMachineData da VM provisionada usando o comando `Get-ProvVM`. Se o campo de prioridade estiver definido como **Spot**, o Spot estará em uso.
- Você pode verificar se uma VM está usando o Spot no Portal do Azure:
  1. Encontre a VM no Portal do Azure.
  2. Acesse a página **Visão geral**.
  3. Role até a parte inferior e localize a seção **Azure Spot**.
     - Se o Spot não estiver em uso, esse campo estará vazio.
     - Se o Spot estiver em uso, os campos **Azure Spot** e **Política de despejo do Azure Spot** serão definidos.

1. Você pode verificar o perfil de cobrança ou o preço máximo por hora da VM na página Configuração.

Configurar tamanhos de VM de backup

Às vezes, as nuvens públicas podem ficar sem capacidade para um tamanho específico de VM. Além disso, se você usar VMs do Azure Spot, as VMs serão removidas a qualquer momento com base nas necessidades de capacidade do Azure. Nesse caso de capacidade insuficiente no Azure ou de falha na alimentação de uma VM do Spot, o MCS recorre aos tamanhos de VM de backup. Você pode fornecer uma lista de tamanhos de VM de backup usando uma propriedade personalizada `BackupVmConfiguration` ao criar ou atualizar um catálogo de máquinas do MCS. O MCS tenta usar os tamanhos das VMs de backup na ordem fornecida por você na lista.

Quando o MCS usa uma configuração de backup específica para a VM, ele continua usando essa configuração até o próximo desligamento. Na próxima inicialização, o MCS tenta inicializar a configuração primária da VM. Em caso de falha, o MCS tenta inicializar novamente uma configuração de tamanho de VM de backup conforme a lista.

Esse recurso tem suporte para:

- um catálogo que usa um perfil de máquina

- catálogos de máquinas do MCS persistentes e não persistentes
- ambientes do Azure atualmente

Considerações importantes

- Você pode fornecer mais de um tamanho de VM de backup na lista.
- A lista deve ser exclusiva.
- Você pode adicionar a propriedade do tipo de instância para cada uma das VMs na lista. O tipo é **Spot** ou **Regular**. Se o tipo não for especificado, o MCS considerará a VM como **Regular**.
- Você pode alterar a lista de tamanhos de VM de backup de um catálogo existente usando os comandos `Set-ProvScheme` do PowerShell.
- Você pode atualizar as VMs existentes criadas a partir do esquema de provisionamento associado ao catálogo usando o comando `Set-ProvVMUpdateTimeWindow`.
- Você pode configurar a lista de tamanhos de VM de backup para um número selecionado de VMs existentes do MCS usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs que estão usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Se o `Set-ProvVm` comando for usado em uma VM, a VM continuará usando a lista de tamanhos de VM de backup definida nessa VM específica, mesmo que a lista no esquema de provisionamento seja atualizada posteriormente. Você pode usar `Set-ProvVM` com `-RevertToProvSchemeConfiguration` para fazer com que a VM use a lista de backup no esquema de provisionamento.

Criar um catálogo com tamanhos de VM de backup

1. Abra uma janela do **PowerShell**.
2. Execute o comando `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Crie um catálogo de agentes. Esse catálogo é preenchido com máquinas que estão prestes a ser criadas.
4. Crie um pool de identidades. Isso se torna um contêiner para contas do AD criadas para as máquinas que serão criadas.
5. Crie um esquema de provisionamento com o perfil de máquina. Por exemplo:
    - Se você quiser fornecer uma lista somente de tamanhos regulares de VM, execute o seguinte:

```
1  New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
```



```
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`
    " Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"
    StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
    Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
    Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
    Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering':
     'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3',
     'ServiceOffering': 'C']`"/>
</CustomProperties>"
```

- Se você quiser fornecer uma lista de tamanhos mistos de VM (VMs regulares e spot), execute o seguinte:

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
    MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
    folder\helenli.resourcegroup\helenli-master1-mcsio-
    snapshot.snapshot"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`
    " Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"
    StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
    Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
    Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
    Name=`"BackupVmConfiguration`" Value=`"[{
'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
]`"/>
</CustomProperties>"
```

6. Atualize o BrokerCatalog com o ID exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

Atualizar um catálogo existente

Você pode atualizar um esquema de provisionamento usando o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
    true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
    =`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
    Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
    "/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
    Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

Atualizar as VMs existentes

Você pode atualizar as VMs existentes em um catálogo usando o comando `Set-ProvVMUpdateTimeWindow` do PowerShell. O comando atualiza as VMs criadas a partir do esquema de provisionamento associado ao catálogo na próxima inicialização dentro da janela de tempo especificada. Por exemplo:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Nota:**
>
> `StartsNow` indica a hora de início programada. `DurationInMinutes` é a janela de tempo do cronograma.

Você pode configurar a lista de tamanhos de VM de backup para um número selecionado de VMs existentes do MCS usando o comando `Set-ProvVM`. No entanto, para aplicar as atu-

alizações, defina uma janela de tempo de atualização para as VMs que estão usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Por exemplo:

1. Execute o comando `Set-ProvVM` para configurar a lista de tamanhos de VM de backup para uma VM existente do MCS selecionada. Por exemplo:

```
Set-ProvVM -VMName "Vm-001"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
    Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`
    "Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration
    `" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

2. Execute o comando `Set-ProvVMUpdateTimeWindow` para aplicar as atualizações. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
```

Copiar marcas em todos os recursos

Você pode copiar marcações especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do sistema operacional, disco de identidade e disco de cache de write-back) de uma nova VM ou de uma VM existente em um catálogo de máquinas. A origem do perfil da máquina pode ser uma especificação de modelo de ARM ou VM.

> **Nota:**
>
> Você deve adicionar a política nas marcações (consulte Atribuir definições de política para conformidade de marca) ou adicionar as marcações em uma origem de perfil de máquina para reter as marcações nos recursos.

Pré-requisitos

Crie a origem do perfil da máquina (especificação do modelo de ARM ou VM) para ter marcações na VM, nos discos e nas NICs dessa VM.

- Se você quiser ter uma VM como entrada de perfil de máquina, aplique as marcações na VM e em todos os recursos no portal do Azure. Consulte Aplicar marcas com o portal do Azure.
- Se você quiser ter a especificação do modelo ARM como uma entrada de perfil de máquina, adicione o seguinte bloco de marcações sob cada recurso.

```
 "tags": {

"TagC": "Value3"
 }
,
```

> **Nota:**
>
> Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

Copiar marcações para os recursos de uma VM em um novo catálogo de máquinas

1. Crie um catálogo não persistente ou persistente com uma especificação de modelo de ARM ou VM como a entrada do perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

   > **Nota:**
   >
   > Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidas no perfil da máquina e o número de NICs que você deseja que as VMs usem.

Modificar marcações nos recursos de uma VM existente

1. Crie um perfil de máquina com as marcações em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
```

3. Desative a VM na qual você deseja aplicar as atualizações.
4. Solicite uma atualização agendada para a VM. Por exemplo:


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
```

5. Ligue a VM.
6. Você deve ver as marcações especificadas no perfil da máquina copiadas para os recursos correspondentes.

> **Nota:**
>
> Você receberá um erro se houver uma incompatibilidade entre o número de NICs fornecidas no perfil da máquina e o número de NICs fornecidas em `Set-ProvScheme`.

O que fazer a seguir

- Se este for o primeiro catálogo criado, o Web Studio orientará você para criar um grupo de entrega
- Para revisar todo o processo de configuração, consulte Instalar e configurar
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft Azure

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure Resource Manager
- Criar catálogos de máquinas

Remote PC Access

August 22, 2024

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

O Remote PC Access é um recurso do Citrix Virtual Apps and Desktops que as organizações usam para permitir que seus funcionários acessem facilmente os recursos corporativos remotamente e de forma

segura. A plataforma Citrix possibilita esse acesso seguro, dando aos usuários acesso a seus PCs físicos no escritório. Se os usuários puderem acessar seus PCs no escritório, eles podem acessar todos os aplicativos, dados e recursos necessários para fazer o trabalho. O Remote PC Access elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, áreas de trabalho ou aplicativos virtuais e a infraestrutura associada.

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

O recurso consiste em um catálogo de máquinas do tipo **Remote PC Access** que proporciona a essa funcionalidade:

- Capacidade de adicionar máquinas especificando unidades organizacionais. Essa capacidade facilita a adição de PCs em massa.
- Atribuição automática do usuário com base no usuário que faz login no PC Windows do escritório. Oferecemos suporte a atribuições de usuário único e multiusuário. Por padrão, atribuímos automaticamente vários usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, entre no Web Studio, vá para **Settings** e desative a configuração **Enable automatic assignment of multiple users for Remote PC Access**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs físicos Linux
- PCs físicos em pool (isto é, aleatoriamente atribuídos, não dedicados)

> **Notas:**
>
> Para obter detalhes sobre as versões do SO com suporte, consulte os requisitos do sistema para o VDA para SO de sessão única e Linux VDA.
>
> Para implantações locais, o Remote PC Access é válido apenas para licenças do Citrix Virtual Apps and Desktops Advanced ou Premium. As sessões consomem licenças da mesma maneira que outras sessões do Citrix Virtual Desktops. No caso do Citrix Cloud, o Remote PC Access é válido para o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) e Workspace Premium Plus.

Considerações

Embora todos os requisitos e considerações técnicas que se aplicam ao Citrix Virtual Apps and Desktops em geral também se apliquem ao Remote PC Access, alguns podem ser mais relevantes ou exclusivos para casos de uso de PC físico.

> **Importante:**
>
> Os sistemas físicos do Windows 11 (e alguns que executam o Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software do VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:
>
> - Use a opção "/physicalmachine"juntamente com a opção "/remotepc"como parte da instalação da linha de comando do VDA
> - Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada acima não tenha sido usada
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - Nome: ForceEnableRemotePC
>   - Tipo: DWORD
>   - Dados: 1

Considerações sobre implantação

Ao planejar a implantação do Remote PC Access, adote algumas medidas gerais.

- Você pode adicionar o Remote PC Access a uma implantação existente do Citrix Virtual Apps and Desktops. Antes de escolher essa opção, considere o seguinte:
  - Os Delivery Controllers ou os Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os bancos de dados locais do site e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs do Remote PC Access?
  - Os VDAs existentes e os novos VDAs do Remote PC Access ultrapassam o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs no escritório por meio de um processo automatizado. A seguir estão as opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instale VDAs usando SCCM.
  - Scripts de implantação: Instale VDAs usando scripts.

- Veja as Considerações de segurança do Remote PC Access.

> **Nota:**
>
> Ao projetar o acesso ao PC remoto, você deve considerar o número de monitores físicos conectados à GPU no PC remoto e atualmente configurados/operacionais. Mesmo que o monitor não seja usado na sessão Citrix, mas seja detectado pela GPU, a presença do monitor é computada no limite máximo de monitores suportados pela GPU.

Considerações do catálogo de máquinas

O tipo de catálogo de máquinas exigido depende do caso de uso:

- Catálogo de máquinas de Remote PC Access
  - PCs Windows dedicados
  - PCs Windows multiusuário dedicados Esse caso de uso se aplica a PCs físicos de escritório que vários usuários podem acessar remotamente em turnos diferentes.
  - PCs Windows em pool. Esse caso de uso se aplica a PCs físicos que vários usuários aleatórios podem acessar, como laboratórios de informática.
- Catálogo de máquinas com SO de sessão única
  - Estático - PCs Linux dedicados
  - Aleatório - PCs Linux em pool

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.
- Ao escolher as UOs em que as contas da máquina residem, selecione UOs de nível inferior para obter maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de bancos/caixas/guichês, selecione **Tellers** para obter maior granularidade. Caso contrário, você pode selecionar **Officers** ou **Bank** baseado nas exigências.
- Mover ou excluir UOs depois de atribuídas a um catálogo de máquinas de Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Portanto, tenha o cuidado de planejar adequadamente para que as atualizações de atribuição da unidade organizacional a catálogos de máquina sejam contabilizadas no plano de alteração do Active Directory.
- Se não for fácil escolher UOs para adicionar máquinas ao catálogo de máquinas por causa da estrutura de unidade organizacional, você não precisa selecionar nenhuma UO. Você pode usar o PowerShell para adicionar máquinas ao catálogo posteriormente. As atribuições automáticas

de usuário continuam funcionando se a atribuição da área de trabalho estiver configurada corretamente no Grupo de Entrega. Um script de exemplo para adicionar máquinas ao catálogo da máquina juntamente com as atribuições do usuário está disponível em GitHub.

- Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Remote PC Access**.

Considerações do Linux VDA

Estas considerações são específicas para o Linux VDA:

- Use o Linux VDA em máquinas físicas somente no modo não 3D. Devido a limitações do driver do NVIDIA, a tela local do PC não pode ser desligada e exibe as atividades da sessão quando o modo HDX 3D está ativado. Mostrar essa tela é um risco de segurança.
- Use catálogos de máquina do tipo SO de sessão única para máquinas físicas Linux.
- A atribuição automática de usuário não está disponível para máquinas Linux.
- Se os usuários já estiverem conectados em seus PCs localmente, as tentativas de iniciar os PCs a partir do StoreFront falharão.
- Opções de economia de energia não estão disponíveis para máquinas Linux.

Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e as considerações para PCs físicos.

- Não há suporte para:
  - Chaveadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo notebooks e PCs All-in-One e NVIDIA Optimus.
  - Máquinas de inicialização dupla.
- Conecte o teclado e o mouse diretamente ao PC. Esses periféricos poderão se tornar indisponíveis se forem conectados ao monitor ou a outros componentes que podem ser desligados ou desconectados. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desative os componentes.
- Os PCs devem ser ingressados em um domínio do Active Directory Domain Services
- A Inicialização Segura é suportada apenas no Windows 10 e Windows 11.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é recomendada para ter-se maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:

1. Defina as configurações de energia para deixar o adaptador sem fio ligado.
2. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registra até que o usuário faça logon. O PC não está disponível para acesso remoto até que um usuário tenha feito logon.
3. Certifique-se de que os Delivery Controllers ou os Cloud Connectors possam ser acessados da rede Wi-Fi.

- Você pode usar o Remote PC Access em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:

  1. Desative o recurso de hibernação.
  2. Desative o recurso de suspensão.
  3. Defina a ação de fechar a tampa como **Não fazer nada**.
  4. Defina a ação "pressionar o botão de energia"como **Desligar**.
  5. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Remote PC Access é suportado em dispositivos Surface Pro com Windows 10. Siga as mesmas instruções para laptops mencionadas anteriormente.

- Se estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixa o laptop, o VDA se registra novamente nos Delivery Controllers ou Cloud Connectors por Wi-Fi. No entanto, quando você reencaixa o laptop, o VDA não muda para a conexão com fio, a menos que você desconecte o adaptador de conexão sem fio. Alguns dispositivos fornecem funcionalidade interna para desconectar o adaptador de conexão sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador de conexão sem fio. Revise as considerações de Wi-Fi mencionadas anteriormente.

  Faça o seguinte para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

  1. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão**, e defina **Suspender** como **Nunca**.
  2. Em **Gerenciador de dispositivos > Adaptadores de rede > Adaptador Ethernet** vá para **Gerenciamento de energia** e desmarque **O computador pode desligar o dispositivo para economizar energia**. Assegure que **Permitir que este dispositivo acorde o computador** esteja selecionado.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz logon no Citrix Workspace, o recurso aparece como indisponível se já estiver sendo usado por outro usuário.

- Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

Sequência de configuração

Esta seção contém uma visão geral de como configurar o Remote PC Access ao usar o catálogo da máquinas do tipo **Remote PC Access**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquina.

1. Somente site local –Para usar o recurso Wake on LAN integrado, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para o Remote PC Access:

   a) Selecione o tipo de site **Remote PC Access**.
   b) Em **Power Management**, escolha se deseja ativar ou desabilitar o gerenciamento de energia para o catálogo de máquinas Remote PC Access. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.
   c) Forneça as informações nas páginas **Users** e **Machine Accounts**

   Ao concluir essas etapas, é criado um catálogo de máquinas chamado **Remote PC Access Machines** e um grupo de entrega chamado **Remote PC Access Desktops**.
3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

   a) Crie um catálogo de máquinas do tipo **Remote PC Access** (página Operating System do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Tenha o cuidado de atribuir a unidade organizacional correta para que os PCs de destino sejam disponibilizados para uso com o Remote PC Access.
   b) Crie um grupo de entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um grupo de entrega, consulte Criar grupos de entrega. Certifique-se de atribuir o grupo de entrega a um grupo do Active Directory que contém os usuários que exigem acesso a seus PCs.
4. Implantar o VDA nos PCs do escritório.

   - Recomendamos usar o instalador de VDA básico de SO de sessão única (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:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to automatically
               disconnect the remote session.
```

ID do evento 44 Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```

ID do evento 45 Este ID de evento aparece quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user.
3          The user preference is set to local user.
```

Evento de desconexão de sessão remota

Este evento aparece quando a sessão remota é desconectada por diferentes motivos.

Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 46, 47, 48
- Fonte: ICA Service

ID do evento 46 Este ID de evento aparece quando a sessão remota é desconectada e quando o valor do registro SasNotification não existe ou quando o valor do registro SasNotification é 0.

- Mensagem:


```
1          The remote session for <remoteUserName> has been
               disconnected.
```

ID do evento 47 Este ID de evento aparece quando o usuário remoto concorda em desconectar a sessão e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 1 ou o valor do registro RpcaMode é 2 ou o valor do registro RpcaMode não existe.

- Mensagem:

```
1          The remote session for <remoteUserName> has been
               disconnected because the user accepted the request to
               disconnect the session.
```

ID do evento 48 Este ID de evento aparece quando o usuário remoto não recusa a solicitação de desconexão dentro do período de tempo limite específico e quando o valor do registro SasNotification é 1 e o valor do registro RpcaMode é 2.

- Mensagem:

```
1          The remote session for <remoteUserName> has been
               disconnected because the user did not decline the
               disconnection request within the configured timeout
               period (<timeout period>).
```

Evento Ctrl+Alt+Del pressionado duas vezes Este evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

Detalhes do evento

- Nome do log: Application and Services
- ID do evento: 49
- Fonte: ICA Service

ID do evento 49 Este ID de evento aparece quando Ctrl+Alt+Del é pressionado duas vezes em 10 segundos.

- Mensagem:

```
1          The remote session for <remoteUserName> has been forcibly
               disconnected.
```


Wake on LAN

O Remote PC Access suporta Wake on LAN, o que dá aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs no escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina for desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede em que o PC reside quando instruído pelo Delivery Controller. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura extras ou soluções de terceiros para a entrega dos pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN legado baseado em SCCM. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN —SCCM integrado.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 ou posterior
- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes sobre a capacidade de suporte, consulte os Requisitos do sistema para VDA.
  - Wake on LAN habilitado no BIOS/UEFI
  - Wake on LAN habilitado nas propriedades do adaptador de rede dentro da configuração do Windows

Configurar o Wake on LAN

Se você estiver usando o Citrix Virtual Apps and Desktops no local, a configuração do Wake on LAN integrado só será suportada usando o PowerShell.

Para configurar o Wake on LAN:

1. Crie o catálogo de máquinas Remote PC Access se ainda não tiver um.
2. Crie a conexão de host Wake on LAN se ainda não tiver uma.

> **Nota:**
>
> Para usar o recurso Wake on LAN, se você tiver uma conexão de host do tipo "Microsoft Configuration Manager Wake on LAN", crie uma nova conexão de host.

3. Obtenha o identificador exclusivo da conexão de host Wake on LAN.
4. Associe a conexão de host Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host Wake on LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties>" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
 }
```

Quando a conexão 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
```

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
```


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**.

Solucionar problemas

Desligamento do monitor não funciona

Se o monitor local do PC Windows não for desligado enquanto houver uma sessão HDX ativa (o monitor local exibir o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê prioridade maior ao Citrix Indirect Display Driver (IDD) do que ao driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para obter mais detalhes sobre as prioridades do adaptador de exibição e criação de monitor, consulte o artigo CTX237608 do Knowledge Center.

A sessão desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão ativada

A notificação de gerenciamento de sessão controlada pelo valor do registro **SasNotification** funciona somente quando o modo Remote PC Access está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou um recurso de segurança baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Informações de diagnóstico

As informações de diagnóstico sobre o Remote PC Access são gravadas no log de Eventos de Aplicativos do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas, descartando-se as mensagens duplicadas.

- 3300 (informativo): máquina adicionada ao catálogo
- 3301 (informativo): máquina adicionada ao grupo de entrega
- 3302 (informativo): máquina atribuída ao usuário
- 3303 (erro): exceção

Gerenciamento de energia

Se o gerenciamento de energia do Remote PC Access estiver ativado, as transmissões direcionadas por sub-rede não iniciarão máquinas que estejam em uma sub-rede diferente daquela do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando transmissões direcionadas por sub-rede e o suporte AMT não estiver disponível, tente o método Wake-up proxy ou Unicast. Certifique-se de que essas configurações estejam ativadas nas propriedades avançadas para a conexão de gerenciamento de energia.

A sessão remota ativa registra a entrada local da tela sensível ao toque

Quando o VDA habilita o modo Remote PC Access, a máquina ignora a entrada local da tela sensível ao toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou um recurso de segurança

baseado em virtualização ativado, o PC é presumido como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo Remote PC Access. Para ativar o modo Remote PC Access, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Mais recursos

Veja a seguir outros recursos para Remote PC Access:

- Orientação sobre o projeto da solução: Remote PC Access Design Decisions
- Exemplos de arquiteturas do Remote PC Access: Reference Architecture for Citrix Remote PC Access Solution.

Atualizar e migrar

August 22, 2024

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 2402 LTSR a partir de:

- Virtual Apps and Desktops 2203 LTSR com ou sem CUs, até CU4, inclusive
- Virtual Apps and Desktops 1912 LTSR com ou sem CUs, até CU8, inclusive
- Versões CR atualmente suportadas do Citrix Virtual Apps and Desktops

> Nota:
>
> - Antes de iniciar o processo de atualização, a Citrix recomenda que os clientes testem a atualização em um ambiente controlado e verifiquem se ela atende aos requisitos específicos. Além disso, aconselhamos a revisão de toda a documentação relevante do produto, incluindo a lista de descontinuação e os problemas conhecidos, para garantir uma transição perfeita. Essa abordagem ajuda a mitigar possíveis interrupções nos sistemas de produção e aprimora a experiência geral de atualização.
> - O Citrix Virtual Apps and Desktops 1912 LTSR logo atingirá sua fase de fim de vida útil. Para obter mais informações sobre a lista de versões compatíveis, consulte a Matriz de produtos.

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.

- **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.

- **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.

- **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 do **Long Term Service Release (LTSR)** usam atualizações cumulativas (CUs). 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 2203 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 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

Otimização para Microsoft Teams (novo)

August 22, 2024

A Microsoft lançou uma nova versão do Microsoft Teams (Teams 2.x) para ambientes VDI. A Citrix agora oferece suporte à otimização para essa nova versão do Teams. Esta documentação se concentra principalmente na Otimização do Citrix HDX com o novo Teams e oferece informações essenciais para a transição para a Otimização do Microsoft SlimCore.

Terminologia e transição

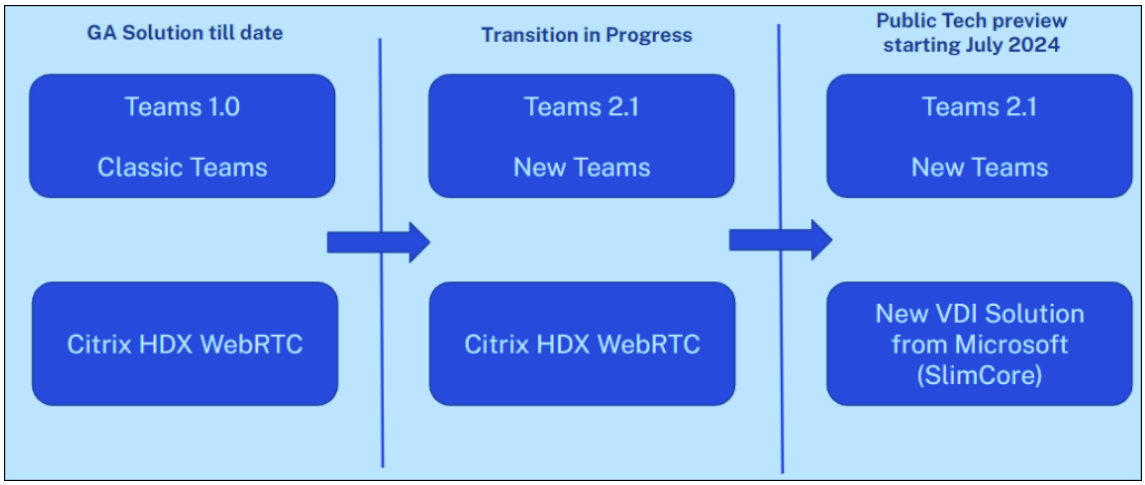
Transição para o Microsoft Teams

Atualmente, existem duas transições no espaço do Microsoft Teams:

- **Transição do Teams Clássico para o Novo Teams**: essa transição é para clientes nativos e de VDI
  - O Teams Clássico chegará ao fim do suporte e ao fim da vida útil. Para obter informações sobre o cronograma dessa transição, consulte Fim da disponibilidade do cliente Teams clássico.
  - A documentação completa para a implantação do Novo Teams está disponível em Novo Teams para VDI.
- **Transição da Otimização do Citrix HDX para a Otimização do Microsoft SlimCore**: essa transição é específica para ambientes VDI.
  - Apresentamos os termos `VDI 1.0` e `VDI 2.0` para diferenciarmos entre a otimização existente com o Citrix HDX e a nova solução VDI da Microsoft.
  - Coloquialmente, VDI 1.0 se refere à Otimização do Citrix HDX e VDI 2.0 se refere à nova solução VDI para Teams (Otimização do Microsoft SlimCore).

Cronogramas

- Para obter mais informações sobre o cronograma de fim da vida útil do Teams Clássico, consulte Fim da disponibilidade do cliente Teams clássico.
- Para participar da prévia pública da otimização do SlimCore, os administradores devem mover os usuários para o canal público de prévia, conforme descrito neste artigo



Principais distinções

Otimização do Citrix HDX	Otimização do Microsoft SlimCore
A otimização é uma solução combinada da Citrix e da Microsoft e usa um canal virtual criado pela Citrix.	A solução de otimização é de propriedade e gerenciada pela Microsoft e usa canais virtuais criados pela Microsoft.
O descarregamento de mídia é feito pelo `HdxRtcEngine` que reside no aplicativo Citrix Workspace.	O descarregamento de mídia é feito pelo mecanismo de mídia Microsoft SlimCore.
Nenhum componente adicional é necessário no endpoint, exceto a instalação do aplicativo Citrix Workspace.	Componente adicional: o **plug-in Teams VDI** precisa ser implantado no endpoint por vários meios. Esse plug-in gerencia o download e as atualizações do mecanismo SlimCore.
Disponível em plataformas de endpoint: Windows, macOS, Linux e ChromeOS.	Disponível em plataformas de endpoint: Windows até a data.
Os novos recursos são gerenciados em conjunto entre a Citrix e a Microsoft.	Os novos recursos são gerenciados pela Microsoft. Os usuários têm acesso a alguns novos recursos não disponíveis com a Otimização do Citrix HDX.

Interoperabilidade e roaming

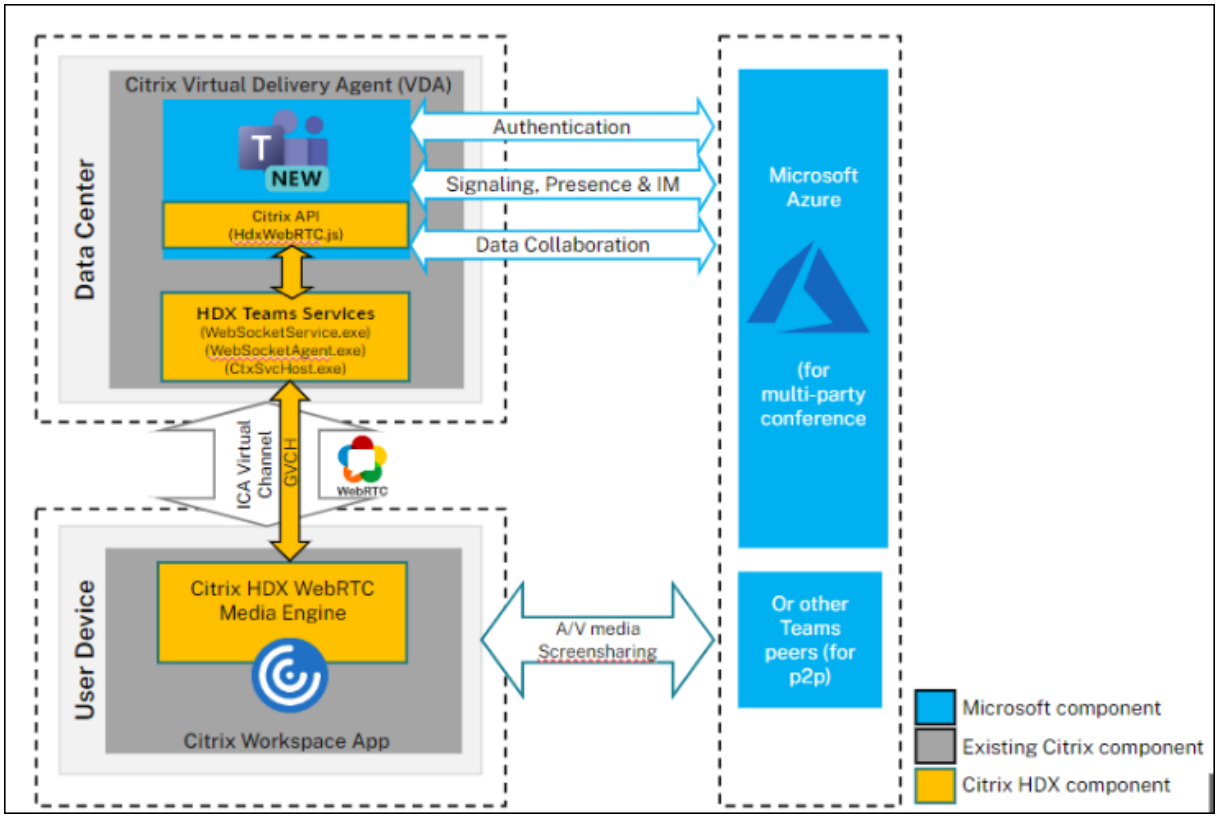
A otimização do Citrix HDX (WebRTC) e a otimização do Microsoft SlimCore podem existir em paralelo, no entanto, o novo cliente Teams pode ser otimizado com apenas uma das formas por vez.

- O Novo Teams carrega o WebRTC ou o SlimCore em tempo de execução. Em tempo de execução, uma decisão é tomada na seguinte ordem: SlimCore > WebRTC > Redirecionamento padrão de áudio/vídeo.
- O processo de seleção não é dinâmico. Por exemplo: caso o Novo Teams comece a otimizar com o SlimCore e ocorra um problema, ele volta ao redirecionamento padrão de áudio/vídeo. É necessário reiniciar o aplicativo Teams para, em seguida, passar pelo processo de tomada de decisão e otimizar com o WebRTC.
- O mesmo cenário se aplica aos cenários de roaming. Por exemplo: se um usuário se conecta a partir de um endpoint com a otimização do SlimCore e faz roaming para um endpoint sem o plug-in (ou) um endpoint Mac/Linux, o Teams opera o redirecionamento padrão de áudio/vídeo. É necessário reiniciar o aplicativo Teams para voltar à otimização do WebRTC.
- Os cenários de roaming entre endpoints que já estão otimizados para o SlimCore estão integrados.

Otimização do Citrix HDX

August 22, 2024

No Citrix HDX (Otimização de WebRTC), o mecanismo de mídia (HdxRtcEngine) no endpoint responsável por lidar com a mídia descarregada é incorporado ao aplicativo Citrix Workspace e a instalação do aplicativo Citrix Workspace também instala automaticamente o mecanismo.



Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para oferecer suporte ao novo cliente Teams. Observe que, nas versões mínimas, algumas correções críticas de erros ou recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as correções e os recursos mais recentes.

Sistemas operacionais VDI

Para obter informações detalhadas, consulte as recomendações fornecidas na documentação da Microsoft.

> **Nota:**
>
> - Não há suporte para o Windows Server 2016. A Citrix recomenda que você planeje suas atualizações adequadamente.
> - Como as versões são atualizadas com frequência, as versões mencionadas aqui podem entrar em fim de vida útil. Portanto, consulte as páginas do ciclo de vida do produto do aplicativo Citrix Workspace e do Citrix Virtual Apps and Desktops para garantir que você esteja usando versões compatíveis de diferentes componentes.
> - Se você usa o Citrix Virtual Apps and Desktops 1912 LTSR, a Citrix recomenda planejar uma atualização, pois sua vida útil será encerrada em dezembro de 2024.

Virtual Delivery Agent (VDA)

Versões mínimas	Versões recomendadas
1912 LTSR CU8+; 2203 LTSR (qualquer CU); 2212 CR	2203 LTSR CU5+ (ou) 2402 LTSR e qualquer versão CR acima

Aplicativo Citrix Workspace

Versões mínimas	Versões recomendadas
Windows 2203 LTSR (CU mais recente); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405

Deployment

1. Instale o novo cliente do Teams na VDI. Para obter informações detalhadas, consulte Implantar novo Teams para VDI.
2. Configure a seguinte chave de registro no VDA para otimizar o novo Teams.
   - **Localização**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **Chave (REG_Multi_SZ)**: `ProcessWhitelist`
   - **Valor**: `msedgewebview2.exe`

     > **Nota:**
     >
     > A partir do Citrix Virtual Apps and Desktops 2402 LTSR (ou) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, você não precisa configurar manualmente a entrada

> do registro do `msedgewebview2.exe`, pois ela está listada como permitida por padrão.

3. Certifique-se de que a política de redirecionamento do Microsoft Teams esteja habilitada. Essa política está ativada por padrão.
4. Nenhuma configuração adicional é necessária no lado do cliente. Siga as instruções do assistente para instalar o aplicativo Citrix Workspace.

App Layering

O novo Microsoft Teams mudou seu método de instalação e agora é instalado em C:\Program Files\WindowsApps. Para oferecer suporte a essa alteração, você deve executar o App Layering versão 2403.2 ou posterior. Você pode baixar um disco de atualização na página de downloads do App Layering que inclui essa correção.

Para obter informações detalhadas, consulte a documentação do App Layering.

Citrix Profile Management

Consulte a documentação do Citrix Profile Management para obter informações sobre como habilitar o roaming para o Novo Microsoft Teams. A orientação atual da versão mínima para o Citrix Profile Management é 2402 LTSR (ou) 2203 LTSR CU5+.

Considerações sobre rede

Os requisitos de rede para o Novo Teams não diferem do Teams Clássico. Portanto, consulte a seção Requisitos de rede na documentação do Teams Clássico.

Matriz de recursos e compatibilidade de versões

Como as versões são atualizadas com frequência, algumas versões mais antigas mencionadas aqui podem chegar ao fim da vida útil. Portanto, consulte as páginas do ciclo de vida do produto do Aplicativo Citrix Workspace e do Citrix Virtual Apps and Desktops para garantir que você esteja usando versões compatíveis de diferentes componentes.

> **Nota:**
>
> - As versões mencionadas aqui são as versões mínimas nas quais há suporte para o recurso específico (ou) a versão mínima na qual há suporte para o Novo Teams, a que for maior.
> - O Citrix Virtual Apps and Desktops 1912 LTSR CU8+ indicado na seção de versões mínimas não está sendo mencionado na tabela abaixo, pois chegará ao fim de sua vida útil em

> dezembro de 2024. No entanto, ainda é uma versão com suporte até então.
> - Os recursos que têm as versões mínimas do Citrix Virtual Apps and Desktops como N/A apenas implicam que o recurso não envolveu nenhuma alteração do lado do VDA.

Recurso	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Áudio/vídeo (P2P e conferência)	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Compartilhamento de tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
i. Borda vermelha do indicador de tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
ii. Limitar captura ao Desktop Viewer	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
iii. Multimonitor	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
DTMF	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Suporte ao servidor proxy	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2305
Compartilhamento de aplicativos	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2209	Não

Recurso	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Legendas ao vivo	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
e911 dinâmico	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Dar o controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
Solicitar o controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Várias janelas	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Transcrições de reuniões	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Desfoque de fundo	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2212	2303
Compartilhamento de tela (com App Protection)	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	Não
Simulcast	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
Toque secundário	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312

Recurso	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Compartilhar áudio do sistema	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	Não

Solução de problemas e outras considerações

Para o Novo Teams, consulte CTX253754, Solução de problemas do Microsoft Teams. Para obter as atualizações mais recentes sobre qualquer coisa relacionada ao Novo Teams, consulte CTX585013.

Limitações conhecidas

Limitações no aplicativo Citrix Workspace

- Suporte a HID - Não há suporte para atender e encerrar chamadas. Aumentar e diminuir volume têm suporte.
- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.
- Limitações de compartilhamento do áudio do sistema
  - O áudio não pode ser compartilhado usando esse recurso ao compartilhar a tela com aplicativos ou guias redirecionados por RAVE e BCR.
  - Esse recurso tem suporte somente em áreas de trabalho publicadas.

Limitações no VDA

- Não há suporte para o Novo Teams como um aplicativo publicado (integrado)
  - Corrigido no CVAD 2402 LTSR, 2203 LTSR CU5 e superior
- Quando você define a configuração de DPI alto do aplicativo Citrix Workspace como Sim, a janela de vídeo redirecionado aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum valor acima de 100%.

Limitação no aplicativo Citrix Workspace e no VDA

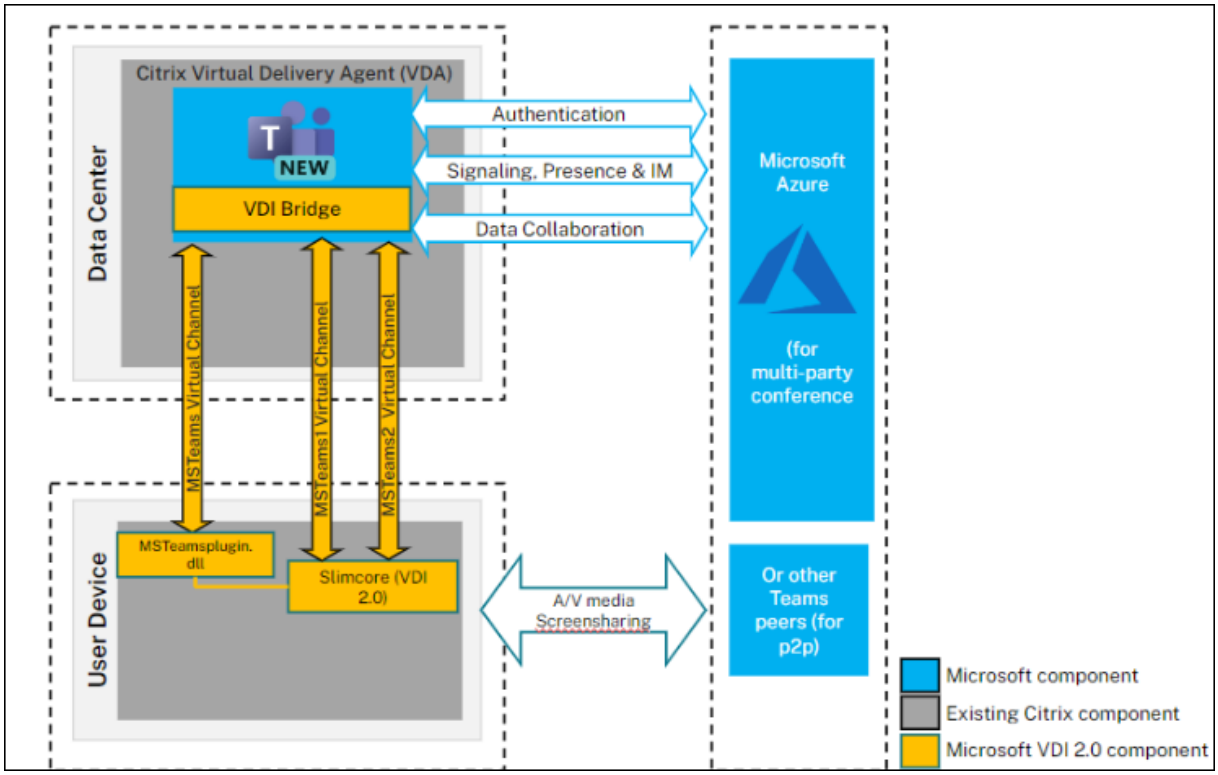
- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume no computador cliente, não no VDA.

Para obter mais detalhes sobre as limitações da Microsoft, consulte Recursos sem suporte na VDI.

Otimização do Microsoft SlimCore

August 22, 2024

Na nova solução de VDI para o Teams, a Microsoft aproveitou o SDK do Canal Virtual da Citrix para criar canais virtuais personalizados e, no lado do endpoint, a Microsoft está usando o SlimCore, o mecanismo de mídia que alimenta o Microsoft Teams (cliente nativo) atualmente. Nessa otimização, o SlimCore seria responsável por gerenciar a mídia descarregada em vez do HdxRtcEngine. Os canais virtuais personalizados que a Microsoft criou serviriam como canal de comunicação entre o Teams na VDI e o mecanismo de mídia SlimCore.
Para obter mais informações, consulte Nova solução de VDI para o Teams e O futuro do Microsoft Teams.



Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para oferecer suporte à Otimização do Microsoft Teams SlimCore. Observe que, nas versões mínimas, algumas correções críticas de erros ou recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as correções e os recursos mais recentes.

Virtual Delivery Agent (VDA)

> **Nota:**
>
> Se você estiver usando a versão 2203 LTSR CU2 ou abaixo (ou) 2303 CR ou abaixo, consulte CTX682593 para entender as limitações dessas versões e planejar sua atualização para as versões mínimas mencionadas abaixo para obter suporte para a Otimização do SlimCore.

Versões mínimas	Versões recomendadas
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+ (ou) 2402 LTSR e qualquer versão CR acima

Aplicativo Citrix Workspace (CWA)

> **Nota:**
>
> Atualmente, a Otimização do SlimCore está disponível apenas para endpoints do Windows.

Versões mínimas	Versões recomendadas
Windows 2203 LTSR (CU mais recente); Windows 2302 CR	Windows 2402 LTSR; Windows 2405 CR

Para obter recomendações sobre as versões mínimas do Teams, os requisitos do sistema operacional do endpoint e os requisitos de hardware, consulte a documentação da Microsoft.

Componentes

- vdiBridge do Novo Teams - Este é o módulo de canal virtual do lado do servidor
- Canal virtual (VC) personalizado - Este é o VC personalizado de propriedade do Microsoft Teams
- Plug-in - dll do VC do lado do cliente. Esse plugin é responsável pelo download e limpeza do SlimCore
- SlimCore - Mecanismo de mídia específico do sistema operacional

Deployment

1. Certifique-se de ter a nova versão do Microsoft Teams, conforme recomendado em Pré-requisitos.
2. Configure a política de lista de permissões de canais virtuais para permitir canais virtuais específicos do Microsoft Teams. Esses canais virtuais são necessários para que o novo cliente Teams possa se conectar ao plug-in do lado do cliente. Para obter mais informações sobre a lista de permissões de canais virtuais, consulte Segurança de canais virtuais.

   Para a Otimização do SlimCore, o Novo Microsoft Teams precisa de três canais virtuais personalizados. Use os curingas para permitir canais virtuais do `ms-teams.exe` executáveis e personalizados:

   ```
   1 MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-
       teams.exe
   2 MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-
       teams.exe
   3 MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-
       teams.exe
   ```

   > **Nota:**
   >
   > - Os curingas da política de lista de permissões de canais virtuais estão disponíveis no CVAD 2203 LTSR CU2 e superior (ou) no Citrix Virtual Apps and Desktops 2206 CR e superior.
   > - As máquinas VDA devem ser reiniciadas para que a política entre em vigor.
   > - O caminho para a instalação do MSTeams muda, pois é um aplicativo MSIX e, portanto, curingas são necessários. Certifique-se de inclui as linhas exatas recomendadas acima na lista de permissões

3. Ative a política do Novo Teams, se necessário, para um grupo de usuários específico (ela é ativada por padrão em nível global)
4. Implante `MSTeamsplugin` em seus endpoints. Consulte a seção Opções para instalar o plugin MSTeams para obter informações detalhadas. Para otimizar com o SlimCore nos endpoints da Citrix, a Citrix oferece várias maneiras para os clientes implantarem o `MSTeamsplugin`.
5. Consulte a documentação da Microsoft para obter mais etapas relacionadas à preparação e ao registro do SlimCore, pois pode haver casos que podem bloquear a instalação do pacote MSIX do novo mecanismo de mídia.

Opções para instalar o plug-in MSTeams

Independentemente do método de instalação, o plug-in MSI detecta automaticamente a pasta de instalação do aplicativo Citrix Workspace e coloca o MsTeamsPluginCitrix.dll nessa localização:

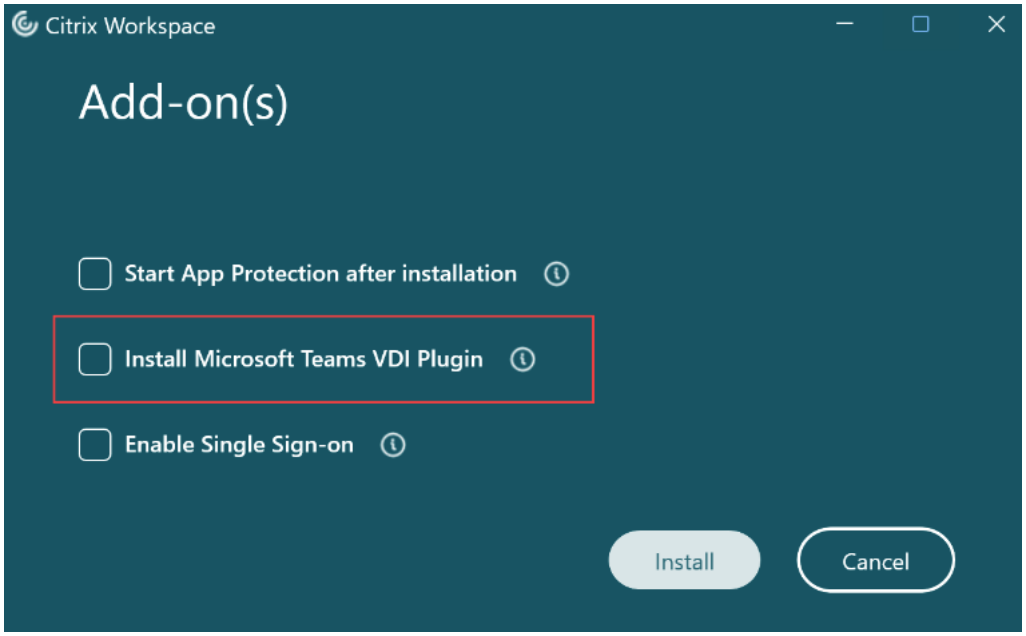
Localizações do plug-in dll quando o plug-in é instalado por meio das opções abaixo com a instalação do administrador do aplicativo Citrix Workspace:

- 64 bits: C:\Program Files (x86)\Citrix\ICA Client
- 32 bits: C:\Program Files\Citrix\ICA Client

> **Nota:**
>
> - Certifique-se de que o aplicativo Citrix Workspace esteja instalado no modo de administrador. Isso garante que os canais virtuais sejam abertos corretamente.
> - A instalação do plug-in será interrompida se nenhum aplicativo Citrix Workspace for encontrado no endpoint
> - Para as experiências de primeira execução, duas reinicializações do aplicativo Teams são necessárias para entrar na Otimização do SlimCore. Para obter mais informações, consulte Verificação da otimização do endpoint.

Opção 1: implantar o plug-in por meio da instalação do aplicativo Citrix Workspace

- O plug-in MSTeams pode ser instalado por meio da interface do usuário durante a nova instalação ou atualização manual.



- Você também pode instalar o plug-in MSTeams por meio da instalação da linha de comando
  - Use a seguinte opção de linha de comando: /InstallMSTeamsPlugin
    Exemplo: CitrixWorkspaceApp.exe /installMSTeamsPlugin

- Para uma nova instalação, o requisito mínimo é: aplicativo Citrix Workspace para Windows 2402 LTSR. Para cenários de atualização em vigor, o requisito mínimo é: aplicativo Citrix Workspace para Windows 2405 CR.

Opção 2: baixe o plug-in MSI diretamente

Se você não estiver usando as versões mais recentes nas quais a instalação do plug-in por meio do CWA é compatível, poderá baixar o plug-in MSI aqui e implantá-lo usando ferramentas como o SCCM, além de qualquer versão existente do aplicativo Citrix Workspace compatível.

Opção 3: implantar o plug-in usando o Global App Configuration Service

O Global App Configuration Service ajuda você a gerenciar as configurações do aplicativo para endpoints gerenciados e não gerenciados e agora você também pode implantar o plug-in Teams em seus endpoints por meio do GACS.

Consulte a documentação de Gerenciamento de plug-ins do Microsoft Teams para obter detalhes sobre como gerenciar o plug-in Teams por meio do GACS.

Considerações sobre rede

Para a Otimização do SlimCore, consulte Considerações sobre rede na documentação da Microsoft para obter os detalhes necessários.

Matriz de recursos e compatibilidade de versões

Com a Otimização do SlimCore, como os recursos e a implementação da solução VDI são de propriedade da Microsoft, consulte a documentação da Microsoft.

Solução de problemas e outras considerações

Para o Novo Teams com a Otimização do Microsoft SlimCore, consulte a documentação da Microsoft.

Limitações conhecidas

Com a Otimização do SlimCore, como os recursos e a implementação da solução VDI são de propriedade da Microsoft, consulte os problemas conhecidos documentados pela Microsoft.

Otimização para Microsoft Teams (clássico)

August 22, 2024

> **Nota:**
>
> O novo Microsoft Teams 2.1 agora está disponível para VDA. Essa versão do Microsoft Teams é compatível com a Otimização do Microsoft Teams da Citrix usando WebRTC. Para obter mais informações sobre a otimização para o Novo Teams, consulte Novo MS Teams
>
> A partir do Citrix Virtual Apps and Desktops 2402, você não precisa configurar manualmente a entrada do registro do `msedgewebview2.exe`, pois ela está listada como permitida por padrão.
>
> Os aplicativos publicados agora são compatíveis com o novo Microsoft Teams.

A Citrix oferece otimização para Microsoft Teams baseados em desktop usando o Citrix Virtual Apps and Desktops e o aplicativo Citrix Workspace. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

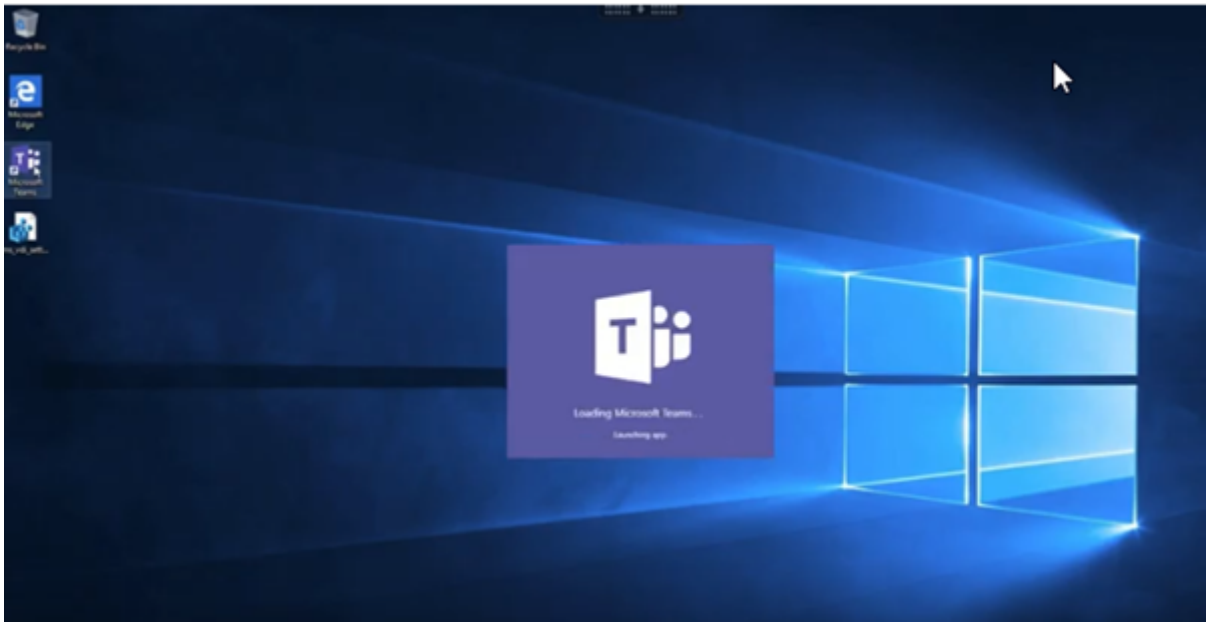
Nossa otimização para o Microsoft Teams inclui serviços HDX do lado do VDA e API para fazer interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O ponto de extremidade decodifica e renderiza a multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem de forma nativa no aplicativo hospedado pelo Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um comando e controle de canal virtual. Isso significa que não há troca de mídia entre o aplicativo Citrix Workspace e o VDA.

Apenas a busca de cliente/renderização do cliente está disponível.

Esta demonstração de vídeo oferece uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam o uso da versão mais recente disponível do Microsoft Teams e que a mantenham atualizada.
As versões do aplicativo de desktop Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas.
Versões não suportadas do aplicativo de desktop Microsoft Teams mostram uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Microsoft Teams (Desktop e Mac).

Recomendamos que você siga as diretrizes de instalação em todo o computador do Microsoft Teams. Evite usar o instalador .exe que instala o Microsoft Teams no `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` da linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Quando você define esse parâmetro, o Instalador de Todo o Computador do Microsoft Teams aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro

`ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` somente em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não é atualizado automaticamente sempre que há uma nova versão. Recomendamos esse modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou áreas de trabalho fora de catálogos aleatórios/agrupados do Windows Server ou Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação da VDI).

Suponha que você tem um ambiente VDI persistente dedicado do Windows 10. Você deseja que o aplicativo Microsoft Teams atualize automaticamente e prefere que o Microsoft Teams instale por usuário em `Appdata/Local`. Nesse caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> Recomendamos instalar o VDA antes de instalar o Microsoft Teams na golden image. Esta ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA foi, desinstale e reinstale o Microsoft Teams.

Para Remote PC Access

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior depois de instalar o VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 ou posterior inclui lógica aumentada executada no momento da inicialização do Microsoft Teams e no momento do login para a detecção do VDA. Essas versões também incluem a identificação do tipo da sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, as versões anteriores do Microsoft Teams podem não detectar e desativar determinados recursos ou elementos da interface do usuário. Por exemplo, salas simultâneas, janelas pop-out de reuniões e chats, ou reações da reunião.

> **Importante:**
>
> Quando você faz roaming de uma sessão local para uma sessão HDX com o Microsoft Teams ainda aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar com o HDX corretamente.
> Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Quando estiver trabalhando no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do Remote PC Access (HDX ou local). Isso porque o Microsoft Teams só pode avaliar o modo VDI no momento da inicialização do aplicativo, não quando ele já está sendo executado em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-out, salas simultâneas ou

> reações à reunião.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações do VDA e do Microsoft Teams em camadas diferentes, você deve criar uma chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em Multimídia.

Recomendações de gerenciamento de perfis

Recomendamos usar o instalador em toda o computador para ambientes Windows Server e VDI em pool no Windows 10.

Quando o sinalizador **ALLUSER =1** é passado para o MSI a partir da linha de comando (o instalador em todo o computador), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~ 300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600—700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**
>
> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em:`HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> Um logon de usuário subsequente aciona a instalação final em **AppData**, em vez disso.

Instalador em toda a máquina

Veja a seguir um exemplo de pastas, atalhos de área de trabalho e registros criados com a instalação de um instalador do Microsoft Teams em todo o computador em uma VM de 64 bits do Windows Server 2016:

Pasta:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<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

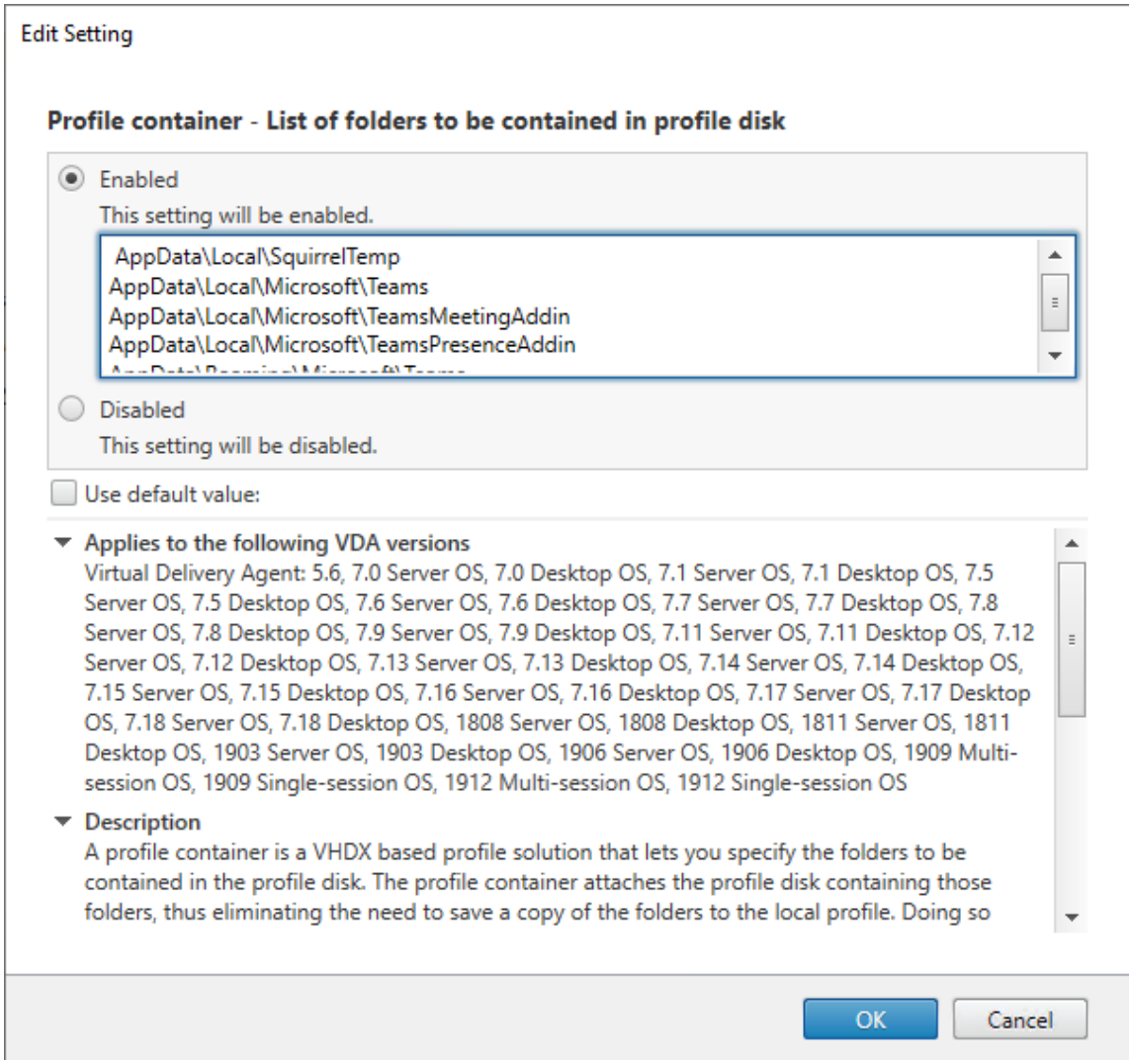
As recomendações de melhor prática baseiam-se nos cenários de caso de uso.
O uso do Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente de dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as 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 nesta configuração. Você também pode configurar essas configurações usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

Requisitos do sistema

Versão mínima recomendada - Delivery Controller (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 está presente no sistema.

Os administradores podem ativar/desativar o Microsoft Teams iniciando no modo otimizado alterando a política de otimização do Microsoft Teams. Os usuários que começam no modo otimizado no aplicativo Citrix Workspace não têm a opção de desativar o Microsoft Teams.

Versão mínima - aplicativo Citrix Workspace 2006 para Linux

Para obter mais informações, consulte Otimização para Microsoft Teams na documentação do aplicativo Citrix Workspace para Linux.

Software:

- `GStreamer` 1.0 ou posterior ou Cairo 2
- `libc++-9.0` ou posterior
- `libgdk` 3.22 ou posterior
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 ou posterior

Aprimoramento da autenticação:

- Biblioteca Libsecret
- Biblioteca libunwind-12. Para obter mais informações, consulte Adding the libunwind-12 library dependency for llvm-12.

Hardware:

- CPU dual-core mínima de 1,8 GHz que possa dar suporte à resolução HD 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com uma velocidade base de 1,8 GHz e uma alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de pontos de extremidade verificados, consulte Clientes finos.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desativar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é VDWEBRTC=On. Depois que a atualização for concluída, reinicie a sessão. (É necessária permissão raiz).

Versão mínima - Aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais compatíveis:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 ou posterior.
- macOS Monterey.

Recursos suportados:

- Áudio

- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Nota:**
>
> O aplicativo Citrix Viewer requer acesso às preferências de segurança e privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência no **menu Apple > Preferências do sistema > Segurança e privacidade > guia Privacidade > Screen recording** e selecionam **Citrix Viewer**.

A otimização do Microsoft Teams funciona por padrão se o usuário tiver o aplicativo Citrix Workspace 2012 ou posterior e o macOS 10.15.

Se você deseja desativar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versão mínima –Versão mais recente do aplicativo Citrix Workspace para ChromeOS em execução na versão mais recente do ChromeOS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core de 2,4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desativada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de um único servidor

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) são suportados em um único host físico. Isso é comumente chamado de Citrix Virtual Apps and Desktops Single Server Scalability (SSS). No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade do usuário. A ideia é descobrir quantos usuários ou máquinas virtuais podem ser executados em um único equipamento de hardware executando um hipervisor principal.

> **Nota:**
>
> Esta seção inclui uma orientação para fazer uma estimativa de SSS. A orientação é de alto nível e pode não ser necessariamente específica para sua situação ou ambiente exclusivo. A única maneira de realmente entender o Citrix Virtual Apps and Desktops SSS é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda seguir essa orientação e essas regras simples para fazer uma estimativa rápida apenas da SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar equipamentos de hardware ou tomar qualquer decisão financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máximo Turbo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- 6 TB de armazenamento SSD RAID 0 local (11 discos)

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando o Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminologia

- Carga de trabalho do Knowledge Worker: inclui Acrobat Reader, Freemind/Java, Photo viewer, Edge e aplicativos MS Office, como Excel, Outlook, PowerPoint e Word.
- Baseline: os testes de escalabilidade do servidor são executados com a carga de trabalho do Knowledge Worker (sem o Microsoft Teams).
- Carga de trabalho do Microsoft Teams: carga de trabalho típica do Knowledge Worker + Microsoft Teams.

Como é realizado o teste de estresse no Microsoft Teams

- O Microsoft Teams é otimizado com o HDX. Portanto, todo o processamento multimídia é descarregado para o ponto de extremidade ou cliente e não faz parte da medição.

- Todos os processos do Microsoft Teams são interrompidos ou eliminados antes do início da carga de trabalho.
- Abra o Microsoft Teams (inicialização a frio).
- Meça o tempo gasto pelo Microsoft Teams para carregar e capturar o foco da janela principal do Microsoft Teams.
- Alterne para a janela de bate-papo usando atalhos de teclado.
- Alterne para a janela do calendário usando atalhos de teclado.
- Envie a mensagem de bate-papo para um usuário específico usando atalhos de teclado.
- Alterne para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- 40% de impacto na escalabilidade com o Microsoft Teams Workload (81 usuários), quando comparado ao Baseline (137 usuários).
- Aumentar a capacidade do servidor em ~40% (na CPU) restaura o número de usuários como com a carga de trabalho Baseline.
- 20% de memória extra necessária com o Microsoft Teams Workload, quando comparado ao Baseline.
- Aumento do tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% em gravações de IOPS, aumento de ~100% em leituras de IOPS. O Microsoft Teams pode ter um impacto significativo em um ambiente com armazenamento mais lento.

Matriz de recursos e compatibilidade de versões

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Áudio/Vídeo (P2P e conferência)	Versão atual menos 90 dias	1906	1907	2009	2004	2105.5

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	2012	2006	2105.5
i. Indicador de tela Borda vermelha	Versão atual menos 90 dias	1906	2002	2012	2006	Não
ii. Limitar captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	2012	2006	Não
iii. Multi-monitor	Versão atual menos 90 dias	1912 CU6+	2106 (1)	2106	2106	Não
DTMF	Versão atual menos 90 dias	N/A	2102	2101	2101	2111.1
Suporte a Proxy Server	Versão atual menos 90 dias	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Compartilhamento de aplicativos	Versão atual menos 90 dias	2109	2109.1	2203.1	2209	Não
Legendas ao vivo	Versão atual menos 90 dias	N/A (4)	2109.1	2109	2109	2303

Recurso	Microsoft Teams (versão mínima)	VDA (versão mínima)	Aplicativo Citrix Workspace para Windows CR (versão mínima)	Aplicativo Citrix Workspace para Mac (versão mínima)	Aplicativo Citrix Workspace para Linux (versão mínima)	Aplicativo Citrix Workspace para ChromeOS (versão mínima)
e911 dinâmico	Versão atual menos 90 dias	N/A	2112.1	2112	2112	2112
Dar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	Não	Não
Solicitar o controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	2203	2303
Várias janelas	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Transcrições de reuniões	Versão atual menos 90 dias	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Desfoque do fundo	Versão atual menos 90 dias	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewer somente no modo de tela cheia. SHIFT+F2 não é suportado.
2. Negociar/Kerberos, NTLM, Basic e Digest. Pac os arquivos também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, a legenda ao vivo só funcionará se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 para Linux ou 2112 para Windows. Isso ocorre porque as legendas ao vivo se comportam de maneira diferente se o Microsoft Teams está no modo de IU de Janela única ou no modo Várias janelas.
5. O modo Várias janelas foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

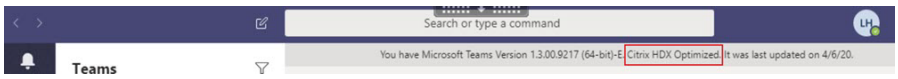
> **Nota:**
>
> - Todos os recursos listados no **aplicativo Citrix Workspace para Windows 1912 CU6 (ou posterior)** são aplicáveis ao aplicativo Citrix Workspace para Windows 2203.1 LTSR CU1.
> - A Microsoft preteriu o suporte ao modo Janela única no Microsoft Teams. Para ajustar-se às normas, você deve atualizar seu VDA para 1912 CU6+ LTSR e o aplicativo Citrix Workspace para 2203 CU2+ ou superior, que oferece suporte ao modo Várias janelas.

Ativar a otimização do Microsoft Teams

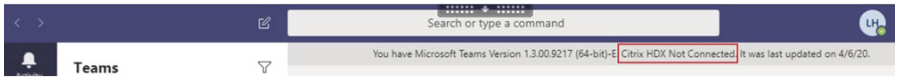
Para habilitar a otimização para o Microsoft Teams, use a política Gerenciar console descrita na política de redirecionamento do Microsoft Teams. Essa política está **ATIVADA** por padrão. Além da ativação dessa política, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima necessária. Se você habilitou a política e a versão do aplicativo Citrix Workspace for suportada, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definida como **1** automaticamente no VDA. O Microsoft Teams lê a chave a ser carregada no modo VDI.

> **Nota:**
>
> Se você estiver usando VDAs da versão 1906.2 ou posterior com versões mais antigas do controlador (por exemplo, versão 7.15) que não têm a política disponível no console Gerenciar (Studio), seu VDA ainda poderá ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

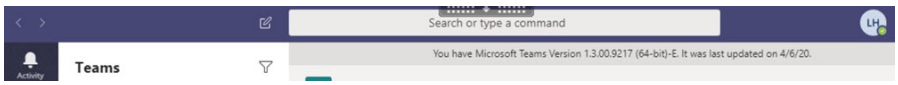
Se você clicar em **About > Version**, a legenda **Citrix HDX Optimized** exibirá:



Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro em partes posteriores da pilha. O erro é mais provável nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, isso indica que o Microsoft Teams não conseguiu carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito no ícone da área de notificação e reinicie. Certifique-se de que a política Gerenciar console não esteja definida como **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 depende do produto VPN e da plataforma de máquina usada, mas a maioria das soluções VPN permite a configuração simples da política para aplicar essa lógica. Para obter mais informações com orientações de túnel dividido específicas à plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o SRTP (Secure Real-Time Transport Protocol) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para esse recurso, são usadas chaves simétricas (negociadas com DTLS) para criptografar mídia e controlar mensagens usando a codificação de criptografia AES.

As seguintes métricas são recomendadas para garantir uma experiência positiva do usuário:

Métrica	Ponto de extremidade para Microsoft 365
Latência (um sentido)	< 50 ms
Latência (RTT)	< 100 ms
Perda de pacote	< 1% durante um intervalo de 15s
Jitter entre chegada de pacotes	<30ms durante um intervalo de 15s

Para obter mais informações, consulte Preparar a rede da sua organização para o Microsoft Teams.

Em termos de requisitos de largura de banda, a otimização para o Microsoft Teams pode usar uma grande variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam estes codecs durante o processo do estabelecimento de chamada usando a oferta/resposta do Session Description Protocol (SDP).
As recomendações mínimas da Citrix são:

Tipo	Largura de banda	Codec
Áudio (em cada sentido)	~ 90 kbps	G.722
Áudio (em cada sentido)	~ 60 kbps	Opus*
Vídeo (em cada sentido)	~ 700 kbps	H264 360p a 30 fps 16:9
Compartilhamento de tela	~ 300 kbps	H264 1080p a 15 fps

* O Opus suporta codificação de taxa de bits constante e variável de 6 kbps até 510 kbps.

Opus e H264 são os codecs preferidos para chamadas ponto a ponto e em conferência.

> **Importante:**
>
> Quanto ao desempenho, a codificação é mais cara do que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix Workspace para Linux e Windows. Consulte Encoder performance estimator e Otimização para Microsoft Teams.

Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

  Se você configurar um servidor proxy explícito no VDA e encaminhar conexões para localhost por meio de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Bypass proxy servers for local address** em **Internet Options > Connections > LAN Settings > Proxy Servers** e ignorar `127.0.0.1:9002`.

  Se você usar um arquivo PAC, o script de configuração do proxy VDA do arquivo PAC deverá retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

  Se a filial estiver configurada para acessar a Internet por meio de um proxy, esses aplicativos suportam servidores proxy:

  - Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos Pac também têm suporte)
  - Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos Pac também têm suporte)

- Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
- Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler configurações de proxy. Esses dispositivos enviam tráfego diretamente para servidores do Microsoft 365 TURN.

> **Importante:**
>
> - Verifique se o dispositivo cliente pode se conectar ao servidor DNS para executar resoluções de DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor Microsoft Teams Relay:
>
>   - `worldaz.relay.teams.microsoft.com`
>   - `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 chamadas de conferência com o estabelecimento de mídia falharão.
>
> - A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não no cliente).

Estabelecimento de chamadas e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão SRTP (Secure Real-Time Transport Protocol) de rede direta via User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia recorre ao TCP/TLS 443.

O mecanismo de mídia HDX dá suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal usando retransmissões em torno de NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Este suporte significa que o ponto de extremidade deve poder executar resoluções DNS.

Considere um cenário em que não há caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está ingressando em uma chamada ou reunião com vários participantes. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP da sub-rede do Microsoft 365 e

quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver bloqueado). Para obter mais informações, consulte o diagrama de arquitetura na Configuração de chamada e URLs do Office 365 e intervalos de endereços IP ID 11.

ID	Categoria	Endereços	Portas de destino
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**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.

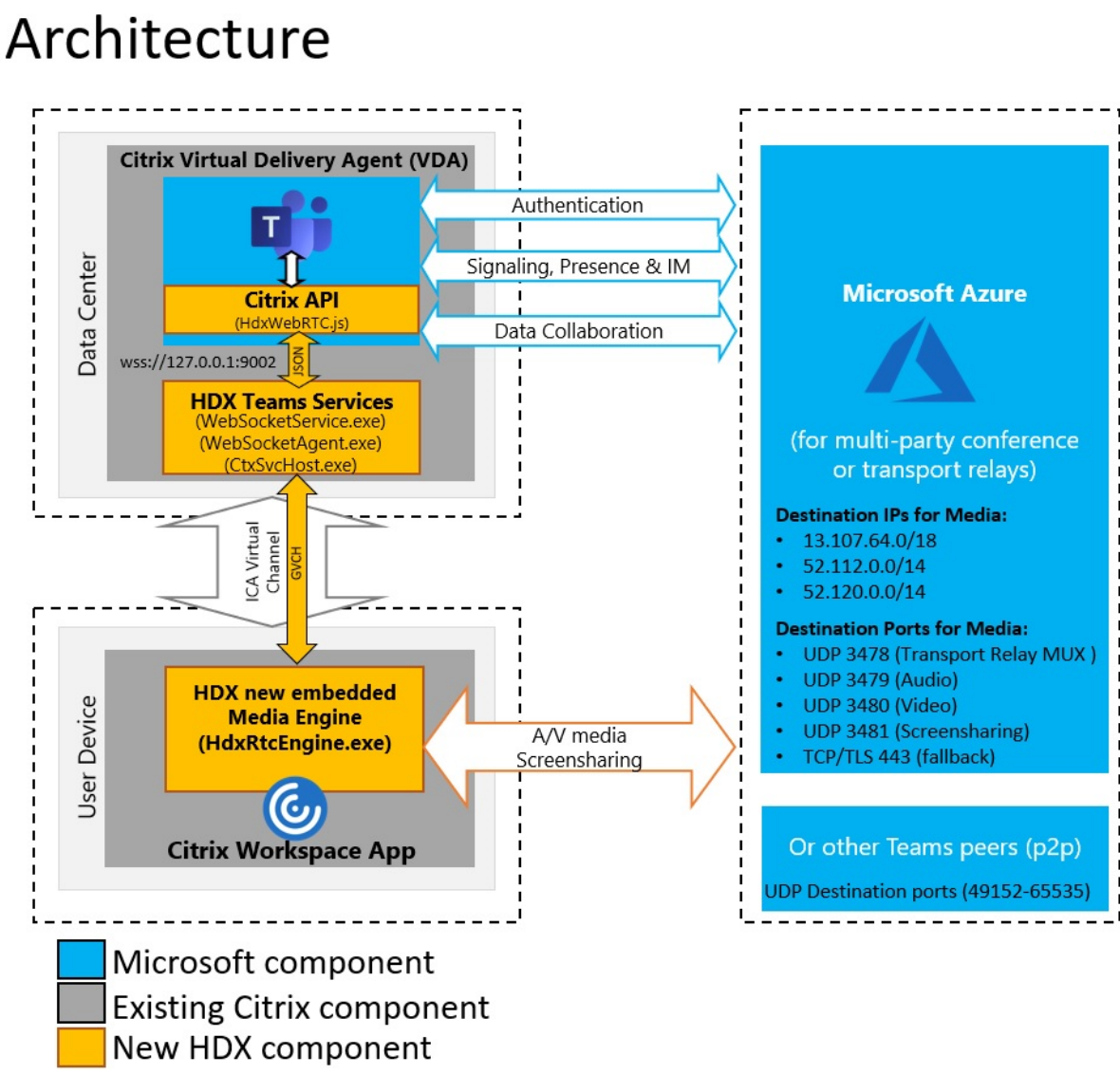
O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com a retransmissão de transporte do Microsoft Teams mais próxima na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e porta 3478—3481 UDP (portas UDP diferentes por carga de trabalho, embora possa haver multiplexação) ou 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 pode conectar seu próprio controlador de borda de sessão suportado ao sistema de telefonia Microsoft diretamente sem nenhum software local adicional.
Há suporte para filas de chamadas, transferência, encaminhamento, espera, silenciar e retomar uma chamada.

DTMF

O recurso de tons duplos de multifrequência (DTMF) são compatíveis com estas versões do aplicativo Citrix Workspace (ou posterior):

- Aplicativo Citrix Workspace para Windows versão 2102

- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101
- Aplicativo Citrix Workspace para ChromeOS versão 2111.1

Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado no Microsoft Calling Plans, Operator Connect e Direct Routing, ele permite a você:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace em execução no ponto de extremidade, em vez do cliente Microsoft Teams em execução no VDA.

A lei de Ray Baum exige que o local despachável do chamador de 911 seja transmitido para o Ponto de Atendimento Público Seguro (PSAP) apropriado. O Microsoft Teams Optimization with HDX está em conformidade com a lei de Ray Baum quando usado com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posteriores
- Aplicativo Citrix Workspace para Linux versão 2112 e posteriores
- Aplicativo Citrix Workspace para Mac versão 2112 e posteriores
- Aplicativo Citrix Workspace para ChromeOS versão 2112 e posteriores

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de localização de rede ou emergência:

- Configurações de rede
- Serviço de Informações de Local (LIS)

Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de local despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

- ID do chassi/ID da porta usando o Link Layer Discovery Protocol (LLDP) para conexões Ethernet/Switch. O Ethernet/Switch (LLDP) é suportado em:
  - Versões 8.1 e 10 do Windows

  - macOS, que requer software de ativação LLDP Para baixar o software de ativação LLDP, acesse `www.microsoft.com` 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.

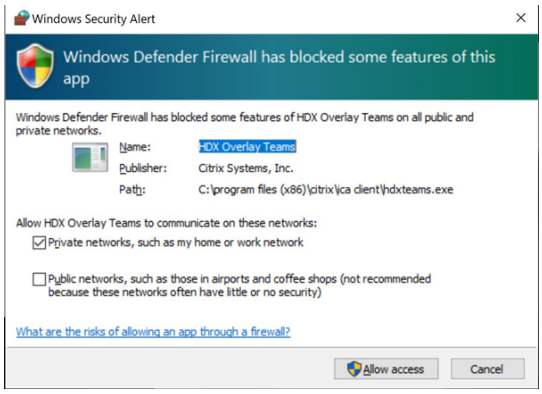
  - Locais baseados em sub-rede e WiFi são compatíveis com o aplicativo Workspace para Windows, Linux e Mac.

- 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)

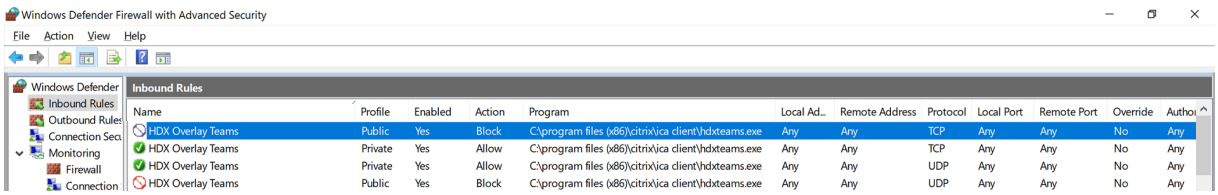
  - Compatível com todas as plataformas de aplicativos do Workspace. No entanto, no caso do Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do SO do cliente fino (>sudo apt-get install libgps23 gpsd lldpd).

Considerações sobre o firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso com as configurações de **firewall do Windows**. O aviso pede aos usuários para permitir a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Firewall do Windows Defender > Segurança Avançada**. Você pode aplicar regras mais restritivas, se desejar.

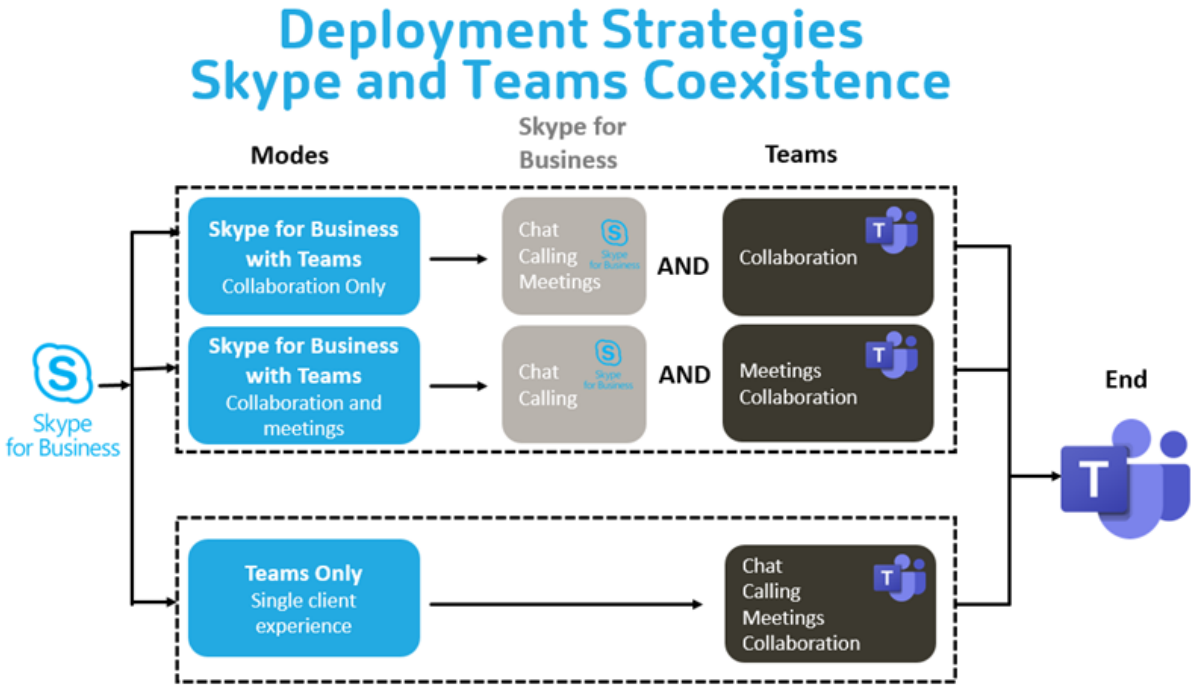


Coexistência do Microsoft Teams e Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado, como duas soluções separadas com recursos sobrepostos.
Para obter mais informações, consulte Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para os mecanismos multimídia do Microsoft Teams, em seguida, honram o conjunto de configurações Alguns exemplos são modos de ilha e colaboração do Skype for Business com o Microsoft Teams. Além disso, colaboração e reuniões do Skype for Business com Microsoft Teams.

O acesso periférico só pode ser concedido a um único aplicativo no momento. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



Citrix SD-WAN: conectividade de rede otimizada para Microsoft Teams

A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio-vídeo do Microsoft Teams dos usuários do aplicativo Citrix Workspace em locais de filiais para um data center antes de ir à Internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço

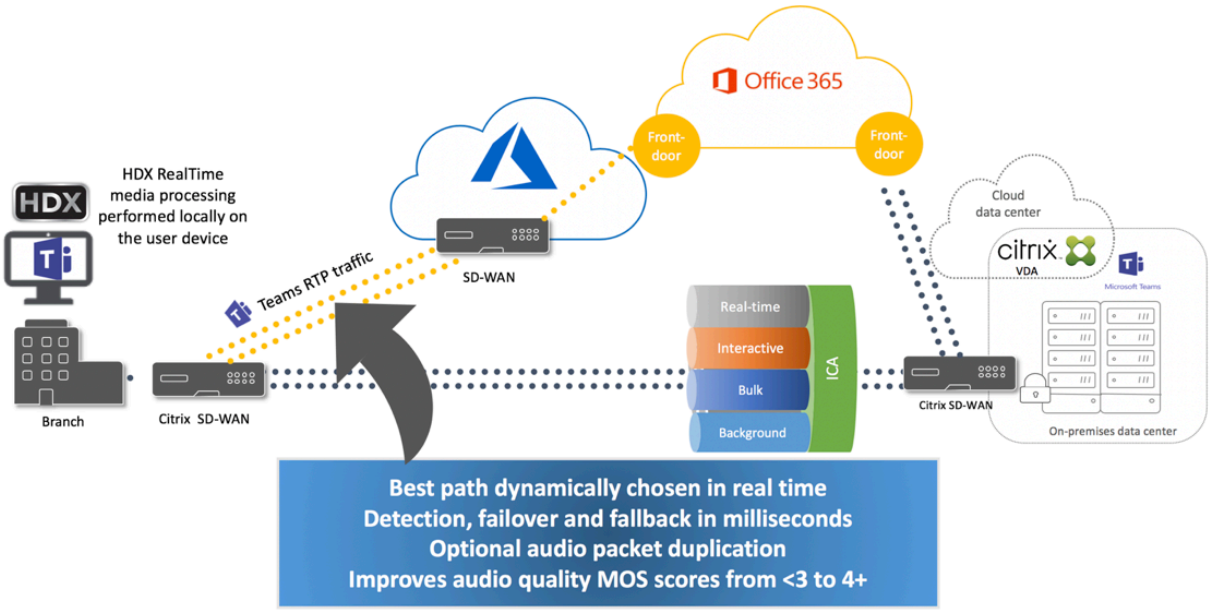
Web do Microsoft 365 baseados em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

As conexões de internet de banda larga de negócios em muitas áreas sofrem de perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio-vídeo do Microsoft Teams quando a integridade da rede é variável ou está degradada.

- Se você usar o Microsoft Azure, um Appliance Virtual (VPX) Citrix SD-WAN implantado no Azure VNET fornece otimizações avançadas de conectividade. Essas otimizações incluem failover de link integrado e corridas de pacotes de áudio.
- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud Direct. Este serviço fornece entrega confiável e segura para todo o tráfego direcionado à Internet.

Se a qualidade da conexão com a Internet da filial não for uma preocupação, pode ser suficiente para minimizar a latência. Desvie o tráfego do Microsoft Teams diretamente do dispositivo de filial Citrix SD-WAN para a porta da frente do Microsoft 365 mais próxima para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo com várias janelas

Você pode usar várias janelas de reuniões ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings no site do Microsoft 365.

> **Nota:**
>
> Esse recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Ele requer VDA 2112 ou superior e foi retroportado para 1912 CU6+ LTSR.

Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 suporta desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas ajudando a conversa a manter o foco na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas em conferência ou P2P.

> **Nota:**
>
> Esse recurso está integrado à interface do usuário/botões do Microsoft Teams. O suporte a 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 2307
- Aplicativo Citrix Workspace para ChromeOS 2303

Limitações:

- O cliente deve estar conectado à Internet durante a substituição da imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição da imagem de fundo definida pelo administrador e pelo usuário não é compatível com a interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser definidas usando parâmetros de configuração no cliente, se a imagem também estiver armazenada no cliente.

Configurar uma imagem de fundo personalizada

As chaves de registro a seguir só são necessárias se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso ou se um administrador quiser substituir os comportamentos padrão. Por exemplo, desativar o desfoque da tela de fundo porque o ponto de extremidade não é poderoso o suficiente.

No Windows Para definir uma imagem de fundo personalizada, os administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou ponto de extremidade:

Localização: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição da imagem de fundo)

Um valor definido como 1 desfoca o fundo. O usuário final ou o administrador podem definir esse valor.

O valor definido como 2 também requer que a chave **VideoBackgroundImage** esteja presente também. Somente o administrador pode definir esse valor. A seguinte chave é necessária somente se você quiser substituir a imagem de fundo, não para desfocar:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: my_image_name.jpeg

A imagem de fundo do vídeo deve estar presente no diretório `C:\Program Files (x86)\Citrix\ICA Client`.

Essa configuração do registro também pode ser usada para habilitar o desfoque em segundo plano ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de interface do usuário do Microsoft Teams. Em outras palavras, se o seu ambiente ou VDA não suportar várias janelas, você ainda poderá aplicar a solução alternativa do registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações da chave do Registro só entram em vigor quando a sessão HDX se conecta.

No Mac Localização da imagem baixada pelo usuário: */Users/username/Downloads/any_image.png*

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

No Linux Localização da imagem baixada pelo usuário: */home/username/Downloads/any_image.jpg*

Crie o arquivo */var/.config/citrix/hdx_rtc_engine/config.json* e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,


```
{


"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
     }

 }
```

3. Salve as alterações.

Considerações sobre o consumo de CPU cliente

Embora o recurso de desfoque seja econômico em termos de uso de CPU, você pode esperar um aumento no consumo. Por exemplo, em um cliente fino com um chip Intel® Pentium® Silver de 4 núcleos e 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

Exibição de galeria e alto-falantes ativos no Microsoft Teams

O Microsoft Teams oferece suporte a layouts de **Gallery**, **Large gallery** e **Together mode**.

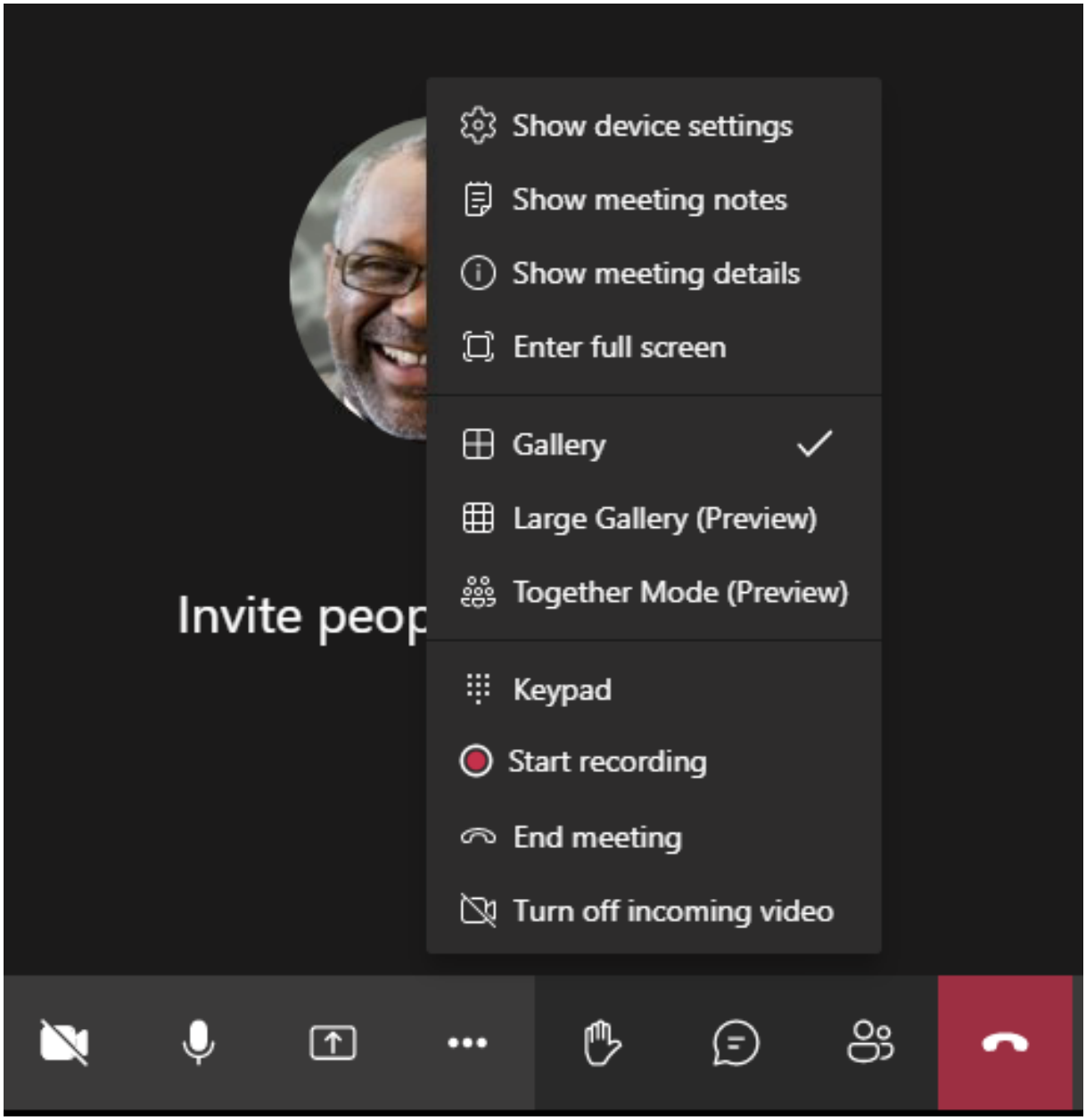
O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecidos como **Gallery**). Nesse caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham um vídeo, apenas os últimos quatro alto-falantes mais ativos aparecem na tela.

O Microsoft Teams também fornece a grande visualização da galeria com uma grade de até 7x7. Como resultado, o servidor de conferência Microsoft Teams compõe um único feed de vídeo e o envia para

o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Esse feed único, em estilo de matriz, também pode incluir os vídeos de pré-visualização automática dos usuários.

Por fim, o Microsoft Teams suporta o **Together mode**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para colocar digitalmente os participantes em um histórico compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada em conferência selecionando layouts de **Gallery**, **Large gallery** ou **Together mode** no menu de reticências.



Suporte para restrições de proporção de vídeo (aplicativo Citrix Workspace para Windows 2102, aplicativo Citrix Workspace para Linux 2106, aplicativo Citrix Workspace para MAC 2106 e posterior):

- A opção **Preencher a moldura** está disponível em Gallery/Large Gallery View. Essa opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts Gallery e Large Gallery:

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Layout/Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro últimos palestrantes mais ativos aparecem na tela e os outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.
Técnica mista	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central combina e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Esta ação introduz um pouco de latência adicional.
Alto-falante ativo	O novo alto-falante ativo substitui o alto-falante menos ativo na grade.	Exibe todos os participantes, independentemente de estarem ativos ou inativos.
Codificação no ponto de extremidade	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no ponto de extremidade se Simulcast estiver ativado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no ponto de extremidade	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no ponto de extremidade pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo de áudio e vídeo. Isso reduz o consumo de CPU no ponto de extremidade.

	Visualização do Gallery 2x2 (padrão)	Vista do Large Gallery
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo poderá ser maior.	720p para o layout composto ou misto. Não há necessidade de um stream de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente reduz a resolução ou a taxa de bits de upload.
Problema de "usuário lento"	O remetente modifica a qualidade de cada modalidade (áudio/vídeo/compartilhamento de tela) para a menor qualidade de rede comum entre os participantes. Esse fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com más condições de rede afeta a qualidade de todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência fornece qualidades diferentes com base nas condições de rede de participantes individuais.
Autovisualização	Mostra você em uma pequena miniatura em tempo real.	Mostra você em uma miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout do vídeo principal com algum atraso adicional.

Compartilhamento de tela no Microsoft Teams

O Microsoft Teams conta com o compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho que está sendo compartilhada com codecs de vídeo como o H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do aplicativo Citrix Workspace 2109 ou superior, para Windows, Linux e Mac, e do aplicativo Citrix Workspace 2303, para ChromeOS, os usuários podem compartilhar suas telas e câmeras de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera é pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O par deve então retomar manualmente o compartilhamento da câmera.

> **Nota sobre o PowerPoint Live**
>
> Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros colegas ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para ver outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar uma apresentação de slides do PowerPoint Live, clique no botão da "Bandeja de compartilhamento"e selecione um dos slides sugeridos do PowerPoint, ou clique em "Procurar"e localize um arquivo do PowerPoint no seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Aplicativos locais sobrepostos ao Desktop Viewer não são capturados.

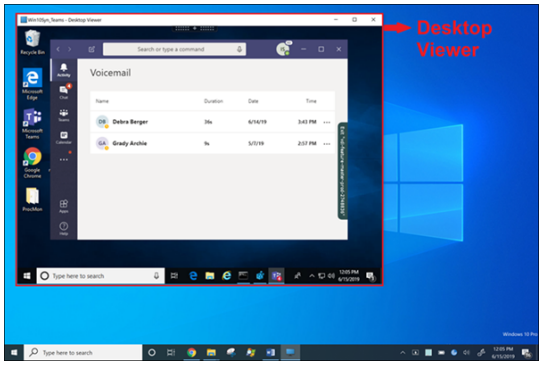
> **Nota**
>
> Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

Limitação conhecida:

- Se o Desktop Viewer estiver desativado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desativado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela com vários monitores.
- Nas versões do aplicativo Workspace anteriores à 2106, somente o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor primário para que os outros pares na chamada possam vê-lo.
- O compartilhamento de tela com vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout do monitor virtual (partição lógica de um único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.
- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento só

é possível se o aplicativo local está sobreposto no Desktop Viewer. Esse comportamento foi removido na versão 2009.6 ou posterior, e 1912 CU5 ou posterior.

- Durante o compartilhamento de tela, se você mudar do modo de janela para tela cheia, o compartilhamento de tela é interrompido. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.
- Não é possível fixar os controles de compartilhamento em um local específico no Microsoft Teams otimizado.
- Ao compartilhar um aplicativo minimizado, a barra de título do aplicativo também pode ser compartilhada.



Compartilhamento de tela a partir de um aplicativo integrado:

Se você estiver publicando o Microsoft Teams como um aplicativo integrado independente, o compartilhamento de tela capturará a área de trabalho local do seu ponto de extremidade físico. É necessário o aplicativo Citrix Workspace versão mínima 1909.

Compartilhamento de aplicativos

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

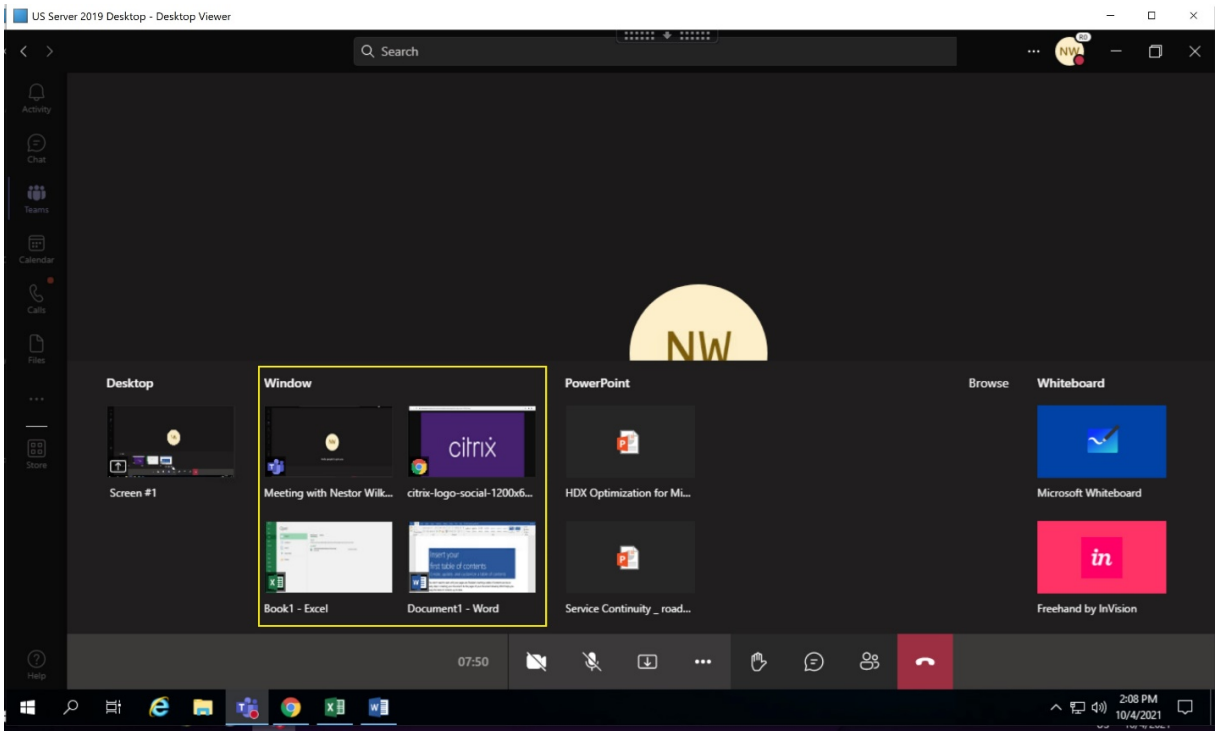
Começando com o aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Você também pode compartilhar aplicativos internos personalizados, como Java, usando o Microsoft Teams otimizado. Para compartilhar um aplicativo específico:

1. Navegue até o aplicativo Microsoft Teams em sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo que você selecionou e os colegas na chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desativar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`:
Nome: `UseWsProvider`
Tipo: `DWORD`
Valor: 0

> **Nota:**
>
> - Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
> - O compartilhamento de tela depende da captura do lado do VDA da janela. O conteúdo é retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para o servidor de conferência ou um par no mesmo nível.



Limitações conhecidas com o compartilhamento de tela de um aplicativo específico:

- O ponteiro do mouse não fica visível quando você está compartilhando a tela de um aplicativo.
- Se você minimizar um aplicativo ao compartilhá-lo, somente o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até você maximizar o aplicativo.
- Os aplicativos LAA (acesso a aplicativos locais) mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de área de trabalho no Microsoft Teams otimizado no VDA. No entanto, quando você seleciona o aplicativo na lista, o resultado pode não ser o esperado.

Compatibilidade com o App Protection
O compartilhamento de tela de um aplicativo específico é compatível com o recurso App Protection no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico, se tiver iniciado o aplicativo ou a área de trabalho a partir de um grupo de entrega que tenha o App Protection ativado.

Quando você clica em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Área de trabalho**. Você só pode selecionar a opção **Janela** para compartilhar um aplicativo aberto.

> **Nota:**
>
> Quando você inicia aplicativos ou áreas de trabalho de um grupo de entrega com o App Protection ativado, não é possível ver o vídeo recebido ou o compartilhamento de tela se estiver usando o aplicativo Citrix Workspace para Windows 2202 ou anterior.

Conceder e solicitar controle no Microsoft Teams Este recurso é suportado nas seguintes versões do aplicativo Citrix Workspace (não há dependência da versão do VDA ou do sistema operacional, sessão única ou multissessão):

- Aplicativo Citrix Workspace para Windows versão 2112.1 ou posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 ou posterior
- Aplicativo Citrix Workspace para Linux versão 2203 ou posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2303 ou posteriores

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de obter o controle, você pode fazer seleções, edições ou outras atividades usando o teclado e mouse na tela compartilhada.

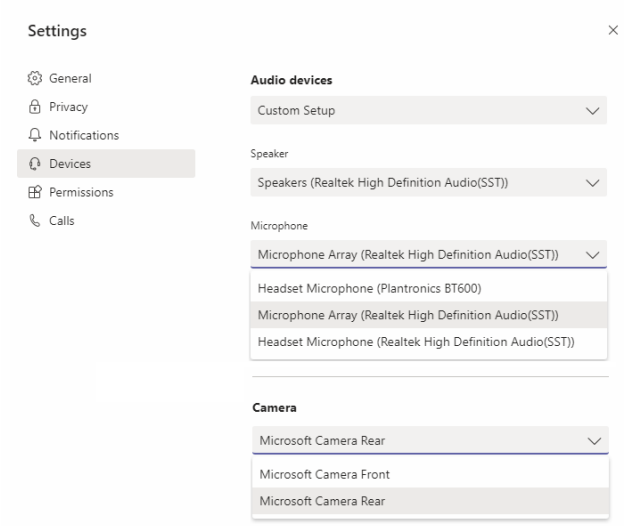
Para assumir o controle quando uma tela está sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar a sua solicitação.

Enquanto você tem controle, você pode fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar um teclado e um mouse. Quando terminar, clique em **Solicitar controle**.

> **Limitações:**
>
> - Conceder e solicitar controle não estarão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como compartilhamento de aplicativo). A área de trabalho ou o monitor completo devem ser compartilhados.
> - O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização do Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fone de ouvidos, microfones, câmeras, alto-falantes e assim por diante). Em seguida, os periféricos são listados devidamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele usa o mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão a partir do mesmo ponto de extremidade.

Recomendações:

- Headsets certificados pelo Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde 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 e pesquise câmeras certificadas pelo Microsoft Teams e periféricos certificados pelo Skype for

Business.

- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento de CPU com webcams que executam codificação H.264 integrada - UVC 1.1 e 1.5.

> **Nota:**
>
> O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio com 24 bits ou com frequências acima de 96 kHz.
>
> O HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou mais antigo) suporta apenas esses formatos de dispositivo de áudio específicos (canais, profundidade de bits e taxa de amostragem):
>
> - Dispositivos de reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
> - Dispositivos de gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz
>
> Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.
>
> **Webrpc** apresenta logs em **HdxTeams.exe** que mostram este tipo de informação:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing ...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!
> ```
>
> Como solução alternativa, desative o dispositivo específico ou:
>
> 1. Abra o **Painel de controle de som** (mmsys.cpl).
> 2. Selecione o dispositivo de reprodução ou gravação.
> 3. Vá para **Propriedades > Avançado** e altere as configurações para um modo suportado.

Modo de fallback

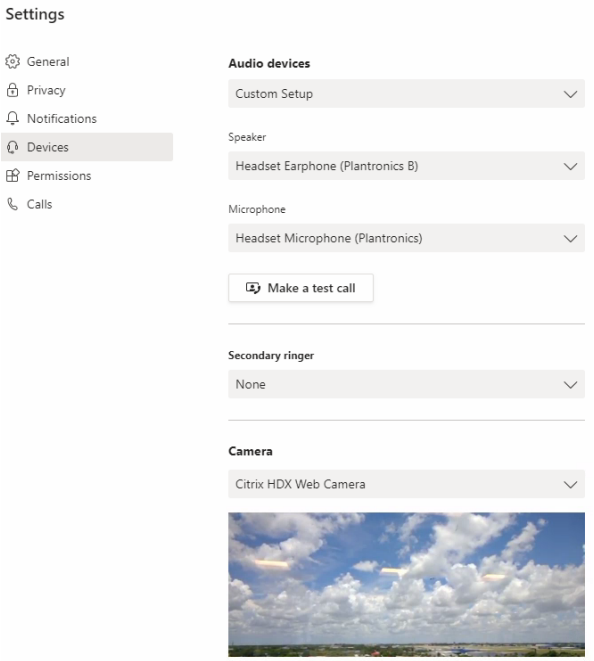
Se o Microsoft Teams não carregar no modo VDI otimizado (“Citrix HDX não conectado”em Microsoft Teams/About/Version), o VDA retornará às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento da webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando um sistema operacional de versão/plataforma do aplicativo Workspace que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não serão aplicadas.
No modo de reserva, os periféricos são traçados ao VDA. Os periféricos aparecem no aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no

VDA. Para obter mais informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados pelo registro.

Esse recurso requer o Microsoft Teams versão 1.3.0.13565 ou posterior.

Para determinar se você está no modo otimizado ou não otimizado ao observar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX herdadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX** como mostrado no gráfico a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) quando comparados com o modo otimizado.



Quando são usadas as tecnologias HDX herdadas, o Microsoft Teams não descarrega o processamento de compartilhamento de áudio, vídeo e tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do ponto de extremidade. Em vez disso, as tecnologias HDX usam renderização no lado do servidor. Espere alto consumo de CPU no VDA quando você liga o vídeo. O desempenho de áudio em tempo real pode não ser otimizado.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e terminar chamadas não têm suporte. Aumentar e diminuir volume têm suporte.

- As configurações de QoS no Admin Center for Microsoft Teams não se aplicam a usuários de VDI.
- Os usuários não podem fazer capturas de tela do conteúdo do Microsoft Teams enquanto usam uma ferramenta de captura no VDA. No entanto, se uma ferramenta de captura for usada no lado do cliente, o conteúdo poderá ser capturado.

Limitação no VDA:

- Quando você configura a configuração de **DPI alto do aplicativo Citrix Workspace** como `Yes`, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido com algum valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume no computador cliente, não no VDA.

Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams em Windows e Mac. Para Linux, consulte seu fornecedor de cliente fino.
Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes terminais são aprimoradas com a adaptação à resolução adequada para a melhor experiência de chamada para todos os chamadores.

Com essa experiência aprimorada, cada usuário pode enviar vários fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p e assim por diante), dependendo de vários fatores, incluindo capacidade do ponto de extremidade, condições da rede e outros. Depois, o ponto de extremidade receptor solicita a resolução de qualidade máxima que pode suportar, proporcionando a todos os usuários a melhor experiência de vídeo.

> **Nota:**
>
> Esse recurso está disponível somente após o lançamento da atualização do Microsoft Teams. Para obter informações sobre o ETA, acesse https://www.microsoft.com/ e pesquise o roadmap do Microsoft 365. Quando a atualização for lançada pela Microsoft, você poderá verificar o CTX253754 para obter a atualização da documentação e o anúncio.

Limitação da Microsoft

- Uma visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams —entre em contato com a Microsoft para saber para quando esperar a grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.

- A resolução máxima de fluxo de vídeo de entrada e saída é de 720p.
- O toque de retorno de chamada PSTN não é suportado
- O desvio de mídia para roteamento direto não tem suporte.
- As funções de produtor e apresentador de eventos de transmissão e ao vivo não têm suporte. A função de participante tem suporte, mas não é otimizada (renderiza no VDA).
- A função de aumentar zoom e diminuir zoom no Microsoft Teams não é suportada.
- Não há suporte para roteamento baseado na localização e bypass de mídia.
- A mesclagem de chamadas não é suportada (opção não exibida na interface do usuário).

Limitação da Citrix e Microsoft

- Ao fazer o compartilhamento de tela, a opção **incluir áudio do sistema** não está disponível.
- O Simulcast não é compatível com o ChromeOS.

Fim da vida útil (EOL) da janela única do Microsoft Teams

Em 31 de janeiro de 2024, a Microsoft retirará o suporte do Microsoft Teams para interface de usuário de janela única ao usar a otimização de VDI do Microsoft Teams e oferecerá suporte somente à experiência de várias janelas. A Microsoft notificou sobre essa descontinuação em 8/9/2023 no Centro de Administração do M365 (ID da publicação: MC674419).
Detalhes públicos sobre o recurso de várias janelas podem ser encontrados no artigo da Tech Community: New Meeting and Calling Experience in Microsoft Teams.

> **Nota:**
>
> A Citrix recomenda que você atualize seu VDA e o aplicativo Citrix Workspace para as versões com suporte para continuar usando o Microsoft Teams no modo otimizado para compartilhamento de vídeo e tela. Se você não atualizar sua infraestrutura e seus endpoints para oferecer suporte a várias janelas, suas chamadas, videochamadas e compartilhamento de tela não serão otimizados. Isso pode resultar em problemas de qualidade da chamada, aumento da latência e aumento da carga no servidor.

A tabela a seguir ilustra as versões mínimas, LTSR e recomendadas do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams no Citrix VDI:

Componente	Versão mínima (1)	Versão compatível com LTSR (2)	Versão recomendada (3)
Microsoft Teams	1.5.00.11865	Não aplicável	Mais recente
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+

Componente	Versão mínima (1)	Versão compatível com LTSR (2)	Versão recomendada (3)
Aplicativo Citrix Workspace para Windows	2112.1 CR	2203 CU2+ (4)	2309 CR+
Aplicativo Citrix Workspace para Mac	2203 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para Linux	2202 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para ChromeOS ou HTML5	2303 CR	Não aplicável	2309 CR+

Notas:

1. Versão mínima: essa é a versão em que a opção Várias janelas foi introduzida pela primeira vez. Algumas versões mínimas listadas aqui podem estar em fim de vida útil.
2. Versão compatível com LTSR: essa é a versão LTSR com suporte pela Citrix para várias janelas. As versões mais antigas dessas versões LTSR podem funcionar, mas o suporte não estará mais disponível para essas versões quando uma nova versão LTSR CU for lançada. Para obter mais informações sobre as políticas de suporte a LTSR, consulte https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
3. Versão recomendada: essa é a versão do software que a Citrix recomendará se o usuário/-cliente optar por atualizar seu software. Todas essas são versões CR.
4. A versão 2203 LTSR para as versões base VDA e CWA inclui a funcionalidade de várias janelas. Essas versões foram substituídas pela CU mais recente, que é a versão oficialmente compatível. Os clientes podem continuar usando essas versões sem suporte a seu critério. A Citrix incentiva os clientes da versão LTSR a atualizarem para a CU mais recente.

Anúncio de descontinuação do formato SDP (Plan B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP (Plan B) do WebRTC atual em versões futuras. Você deve usar o Unified Plan no WebRTC para ter suporte às funcionalidades otimizadas do Microsoft Teams.

Produtos afetados

Em uma das futuras versões do aplicativo Citrix Workspace, chamadas entre pontos de extremidade com a próxima versão do aplicativo Citrix Workspace e pontos de extremidade com o aplicativo Citrix Workspace 2108 ou versões anteriores não serão suportadas. Essa incompatibilidade de chamadas inclui clientes do aplicativo Citrix Workspace (CWA) 1912 LTSR. Os seguintes clientes do CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

Substituição do Plan B

Se você estiver executando a versão do aplicativo Citrix Workspace anterior à 2109, deverá atualizar para uma versão compatível (de preferência a versão CR mais recente). Caso contrário, chamadas com uma versão futura ou com pontos de extremidade mais recentes apresentarão falha na conexão. As chamadas entre versões futuras e seus parceiros de comunicação federados também podem não ser concluídas se o parceiro federado não tiver atualizado o seu Citrix Workspace.

O aplicativo Citrix Workspace encerrou a data de suporte à versão 2108 em março de 2023, devendo ser atualizado para uma versão mais recente. Para obter mais informações, consulte Workspace App para obter detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plan B, consulte a documentação do WebRTC.

Informações adicionais

- Monitoramento, resolução de problemas e suporte ao Microsoft Teams
- Implantar o Microsoft Teams da área de trabalho na VM
- Instalar o Microsoft Teams usando o MSI (seção Instalação da VDI)
- Clientes finos
- Ferramenta de avaliação de rede do Skype for Business
- Compreender a coexistência e a interoperabilidade do Microsoft Teams e do Skype for Business.