Citrix DaaS para Azure

Machine translated content

Disclaimer

Contents

Citrix DaaS Standard para Azure

September 7, 2022

Introdução

O Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure) é a maneira mais simples e rápida de fornecer aplicativos e desktops do Windows a partir do Microsoft Azure. O Citrix DaaS for Azure oferece gerenciamento baseado em nuvem, provisionamento e capacidade gerenciada para fornecer aplicativos e desktops virtuais para qualquer dispositivo.

Essa solução inclui:

- Gerenciamento e provisionamento baseados em nuvem para fornecer Desktops Virtuais do Azure hospedados pela Citrix e aplicativos de máquinas com várias sessões.
- Uma experiência de usuário de alta definição de uma ampla variedade de dispositivos, usando o aplicativo Citrix Workspace.
- Fluxos de trabalho simplificados de criação e gerenciamento de imagens, juntamente com imagens de sessão única e várias sessões preparadas pela Citrix para Windows e Linux com o Citrix Virtual Delivery Agent (VDA) mais recente instalado.
- Acesso remoto seguro de qualquer dispositivo usando pontos de presença globais do serviço Citrix Gateway.
- Recursos avançados de monitoramento e gerenciamento de help desk.
- IaaS do Azure gerenciado, incluindo computação, armazenamento e rede do Azure para fornecer desktops virtuais.

O recurso Acesso ao PC remoto da Citrix permite que os usuários usem remotamente máquinas físicas existentes localizadas no escritório. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

Se você estiver familiarizado com outros produtos Citrix DaaS, o Citrix DaaS for Azure simplifica a implantação de aplicativos e desktops virtuais. A Citrix pode gerenciar a infraestrutura para hospedar essas cargas de trabalho.

O Citrix DaaS for Azure é um serviço do Citrix Cloud. O Citrix Cloud é a plataforma que hospeda e administra os serviços do Citrix Cloud. Saiba mais sobre o Citrix Cloud.

Para saber mais sobre componentes, fluxo de dados e considerações de segurança, consulte Visão geral de segurança técnica. Esse artigo também descreve as responsabilidades do cliente e da Citrix.

Como os usuários acessam desktops e aplicativos

Os usuários (às vezes chamados de assinantes) acessam seus desktops e aplicativos diretamente pelo navegador, usando o cliente Citrix HTML5. Os usuários navegam para um URL do Citrix Workspace fornecido por você, o administrador deles. A plataforma Citrix Workspace enumera e entrega os recursos digitais aos usuários. Os usuários iniciam uma área de trabalho ou um aplicativo a partir do espaço de trabalho.

Depois de configurar um catálogo de máquinas que fornecem desktops e aplicativos (ou um catálogo contendo máquinas físicas para acesso remoto ao PC), o Citrix DaaS para Azure exibe a URL do espaço de trabalho. Em seguida, você notifica seus usuários para acessar esse URL para iniciar a área de trabalho e os aplicativos.

Como alternativa à navegação para o Citrix Workspace para acessar seus desktops e aplicativos, os usuários podem instalar um aplicativo Citrix Workspace em seus dispositivos. Baixe o aplicativo certo para o sistema operacional do dispositivo endpoint: https://www.citrix.com/downloads/workspace-app/.

Conceitos e terminologia

Esta seção apresenta alguns dos itens e termos que os administradores usam no Citrix DaaS para Azure:

- Catálogos
- Locais de recursos
- Imagens
- Assinaturas do Azure
- Conexões de rede
- Ingressou no domínio e não ingressado no domínio

Catálogos

Um catálogo é um grupo de máquinas.

- Os desktops e aplicativos que o Citrix DaaS for Azure entrega aos seus usuários residem em máquinas virtuais (VMs). Essas VMs são criadas (provisionadas) no catálogo.

  Quando você implanta áreas de trabalho, as máquinas no catálogo são compartilhadas com os usuários selecionados. Quando você publica aplicativos, máquinas com várias sessões hospedam aplicativos que são compartilhados com usuários selecionados.

- Para o Acesso ao PC remoto, um catálogo contém máquinas físicas de sessão única existentes. Uma implantação comum inclui máquinas localizadas em seu escritório. Você controla o acesso

do usuário a essas máquinas por meio do método de atribuição de usuário configurado e dos usuários selecionados.

Se você estiver familiarizado com outros produtos Citrix DaaS, um catálogo no Citrix DaaS é semelhante à combinação de um catálogo de máquinas e um grupo de entrega.

Para obter mais informações, consulte:

- Crie catálogos para áreas de trabalho e aplicativos publicados.
- Crie catálogos para o Acesso ao PC remoto.
- Gerencie catálogos.
- Usuários e autenticação.

Locais de recursos

As máquinas de um catálogo residem em um local de recurso. Um local de recurso também contém dois ou mais Cloud Connectors.

- Ao publicar desktops ou aplicativos, a Citrix cria automaticamente o local do recurso e os Cloud Connectors quando você cria o primeiro catálogo.
- Para o Acesso ao PC remoto, o administrador cria o local do recurso e os Cloud Connectors antes de criar um catálogo.

Quando você cria mais catálogos para áreas de trabalho e aplicativos publicados, a assinatura, a região e o domínio do Azure determinam se a Citrix cria outro local de recurso. Se esses critérios corresponderem a um catálogo existente, a Citrix tentará reutilizar esse local de recurso.

Para obter mais informações, consulte:

- Especifique as informações de localização do recurso ao criar um catálogo.
- Ações de localização de recursos.

Imagens

Quando você cria um catálogo para áreas de trabalho e aplicativos publicados, uma imagem de máquina é usada (com outras configurações) como um modelo para criar as máquinas.

- O Citrix DaaS for Azure fornece várias imagens preparadas pela Citrix:
  - Windows 10 Enterprise (sessão única)
  - Área de trabalho virtual do Windows 10 Enterprise (multissessão)
  - Área de Trabalho Virtual do Windows 10 Enterprise (multissessão) com o Office 365 ProPlus
  - Windows Server 2012 R2
  - Windows Server 2016

  - Windows Server 2019
  - Linux

  Cada imagem preparada pela Citrix tem um Citrix VDA e ferramentas de solução de problemas instaladas. O VDA é o mecanismo de comunicação entre as máquinas dos seus usuários e a infraestrutura do Citrix Cloud que gerencia o Citrix DaaS para Azure.

  A Citrix atualiza as imagens preparadas disponíveis quando uma nova versão do VDA é lançada.

- Você também pode importar e usar suas próprias imagens do Azure. Você deve instalar um VDA (e outro software) na imagem antes que ele possa ser usado para criar um catálogo.

O termo VDA geralmente se refere à máquina que fornece aplicativos ou desktops e ao componente de software instalado nessa máquina.

Para obter mais informações, consulte Imagens.

Assinaturas do Azure

Você pode criar catálogos para entregar desktops e aplicativos e criar/importar imagens em uma assinatura do Citrix Managed Azure ou em sua própria assinatura do Azure (gerenciada pelo cliente).

Se você solicitar apenas o Citrix DaaS para Azure, deverá importar (adicionar) e usar suas próprias assinaturas do Azure. Se você também solicitar um Fundo de Consumo do Citrix Azure, receberá uma assinatura do Citrix Managed Azure. Em seguida, você pode usar uma assinatura do Citrix Managed Azure ou uma de suas assinaturas importadas do Azure ao criar um catálogo ou criar uma nova imagem.

Para obter mais informações, consulte:

- Os cenários de implantação ilustram maneiras de usar as assinaturas do Azure com o Citrix DaaS for Azure.
- As assinaturas do Azure explicam as diferenças entre o Citrix Managed Azure e as assinaturas do Azure gerenciadas pelo cliente. Este artigo também descreve como visualizar, adicionar e remover assinaturas.
- Avisão geral da segurança técnica descreve as diferenças de responsabilidade com o Citrix Managed Azure e as assinaturas do Azure gerenciadas pelo cliente.

Conexões de rede

Ao criar um catálogo usando uma assinatura do Citrix Managed Azure, você indica se e como os usuários podem acessar locais e recursos em sua rede corporativa local a partir de seus desktops e

aplicativos publicados. As opções são sem conectividade, emparelhamento do Azure VNet e Citrix SD-WAN.

Ao usar sua própria assinatura do Azure, não há necessidade de criar uma conexão. Você só precisa importar (adicionar) sua assinatura do Azure ao serviço.

Para obter mais informações, consulte Conexões de rede.

Ingressou no domínio e não ingressado no domínio

Várias operações e recursos de serviço diferem, dependendo se as máquinas (VDAs) são unidas ao domínio ou não ingressadas no domínio. A associação ao domínio também afeta os cenários de implantação disponíveis.

- As máquinas ingressadas no domínio e não ingressadas no domínio suportam qualquer um dos métodos de autenticação do usuário disponíveis no espaço de trabalho do usuário.
- Você pode publicar áreas de trabalho, aplicativos ou ambos de máquinas ingressadas no domínio e não ingressadas no domínio. As máquinas nos catálogos de Acesso ao PC remoto devem estar unidas ao domínio.

A tabela a seguir lista várias diferenças entre máquinas não ingressadas no domínio e máquinas ingressadas no domínio ao entregar desktops e aplicativos.

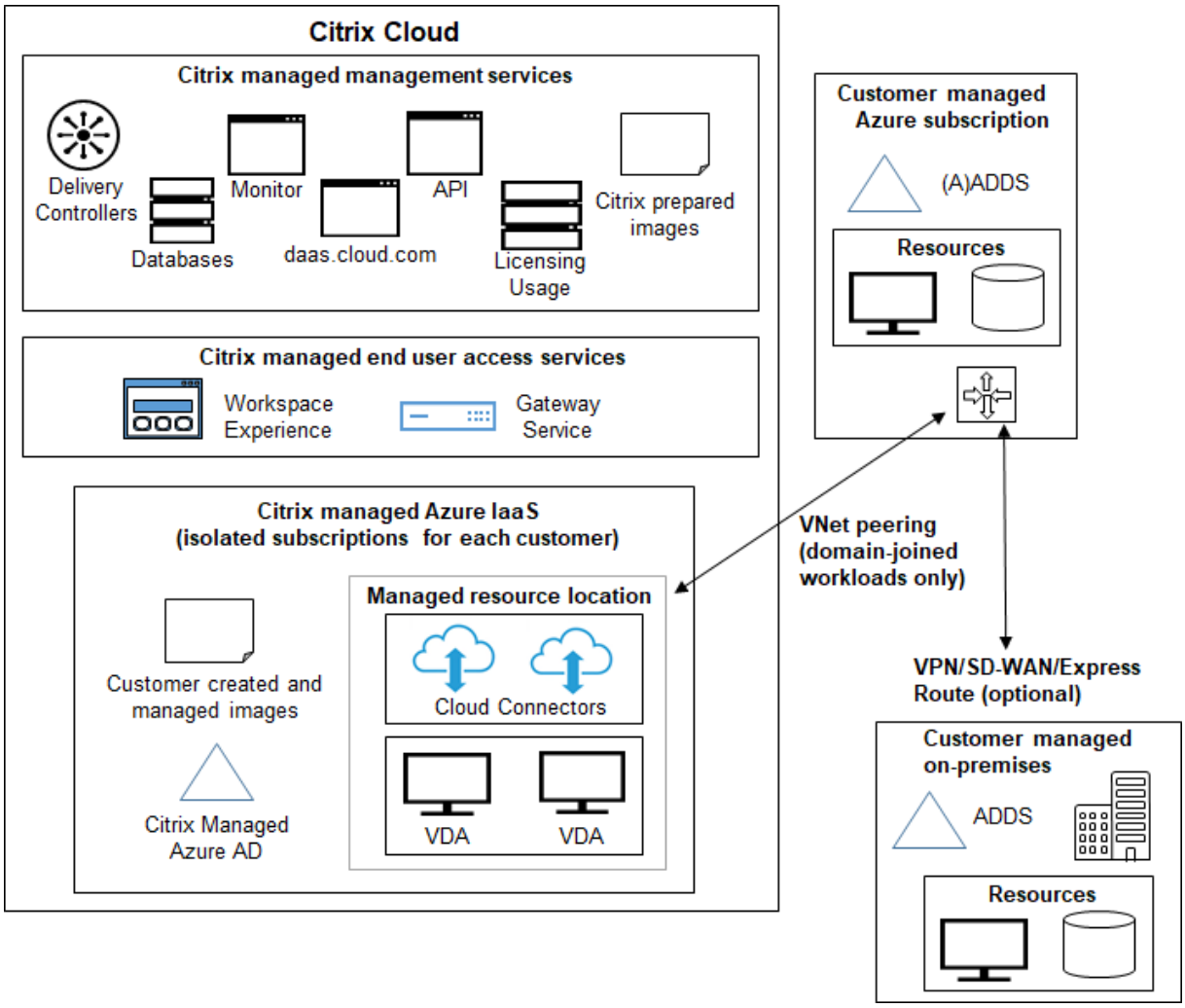
Não ingressado no domínio	Ingressou no domínio
O Active Directory não é usado para máquinas. As máquinas não estão associadas a um domínio do AD.	O Active Directory é usado para máquinas. As máquinas são unidas a um domínio do AD.
As políticas de grupo do Active Directory não podem ser aplicadas a máquinas (VDAs). (Você pode aplicar o GPO local na imagem usada para criar um catálogo.)	Os VDAs herdam políticas de grupo para a OU do AD especificada durante a criação do catálogo.
Os usuários fazem login usando o logon único.	Quando os usuários fazem logon no espaço de trabalho usando um método de autenticação diferente do Active Directory, eles também são solicitados a fazer login quando uma área de trabalho ou aplicativo é iniciado.
Não precisa de conexão com uma rede local.	(Ao usar uma assinatura do Citrix Managed Azure) Deve ter uma conexão para acessar uma rede local, usando o Microsoft Azure VNet ou o Citrix SD-WAN.

Não ingressado no domínio	Ingressou no domínio
É necessário usar uma assinatura do Citrix Managed Azure para provisionar VDAs. (Não é possível usar suas próprias assinaturas do Azure para provisionar VDAs. No entanto, os usuários podem ser conectados a partir do seu próprio Azure AD.)	Pode usar uma assinatura do Citrix Managed Azure e suas próprias assinaturas do Azure.
Não é possível solucionar problemas usando uma máquina bastion ou RDP direto.	Pode solucionar problemas usando uma máquina bastion ou RDP direto.
Não é possível usar o Citrix Profile Management. (Recomendar: Use catálogos persistentes.)	Pode usar o Citrix Profile Management ou o FSLogix.

Cenários de implantação

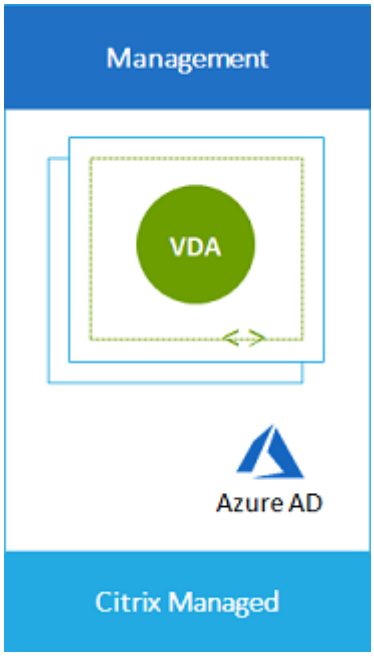
Os cenários de implantação para desktops e aplicativos publicados diferem, dependendo se você está usando uma assinatura do Citrix Managed Azure ou sua própria assinatura do Azure gerenciada pelo cliente.

Implantação em uma assinatura do Citrix Managed Azure

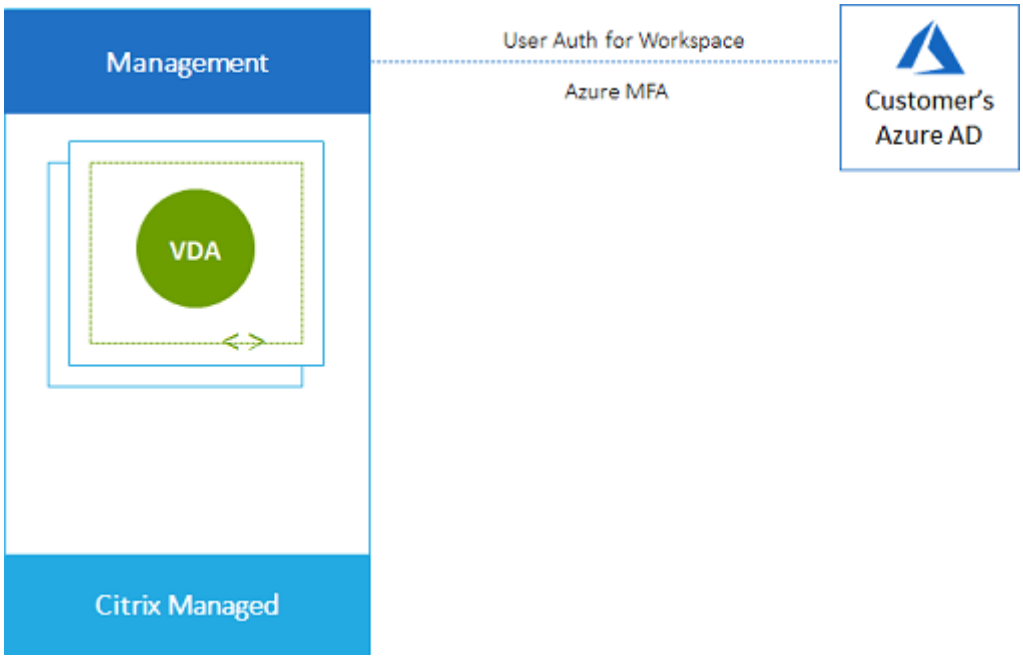


O Citrix DaaS for Azure oferece suporte a vários cenários de implantação para conexão e autenticação de usuário.

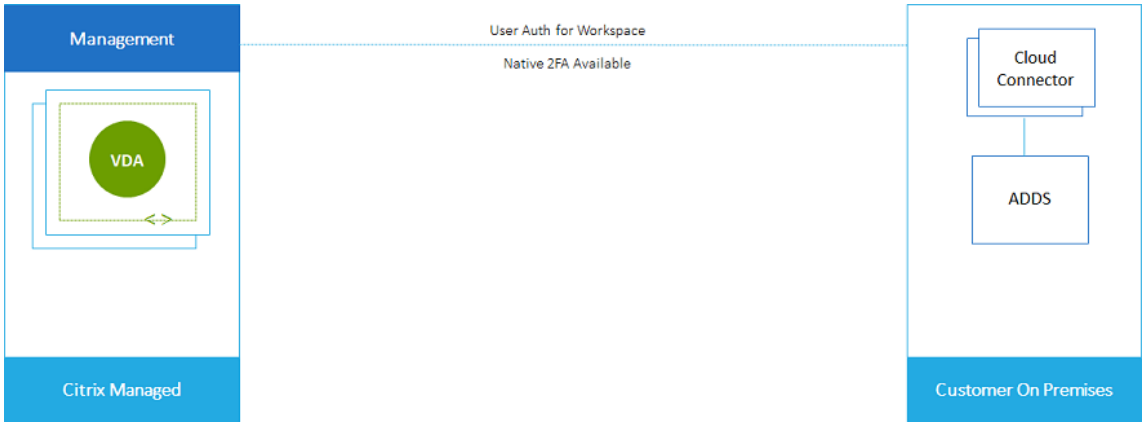
- **Azure AD gerenciado:** Essa é a implantação mais simples, com VDAs não ingressados no domínio. É recomendado para provas de conceito. Você usa o Managed Azure AD (que a Citrix gerencia) para gerenciar usuários. Seus usuários não precisam acessar recursos em sua rede local.



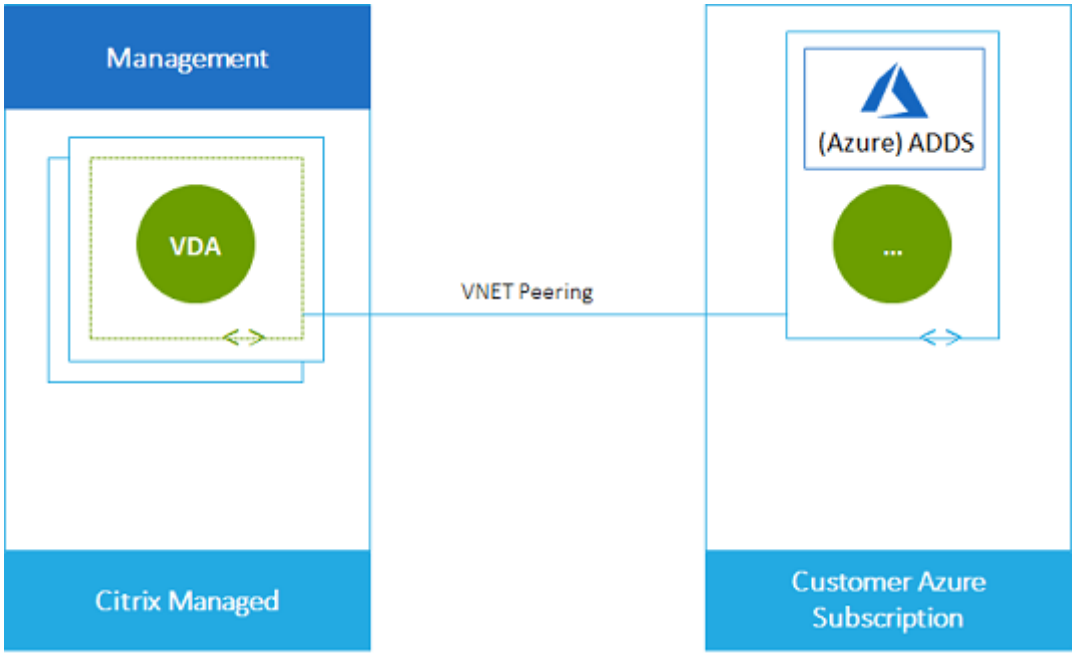
- **Azure Active Directory do cliente:** Esta implantação contém VDAs não ingressados no domínio. Você usa seu próprio Active Directory ou Azure Active Directory (AAD) para autenticação de usuário final. Nesse cenário, os usuários não precisam acessar recursos na rede local.



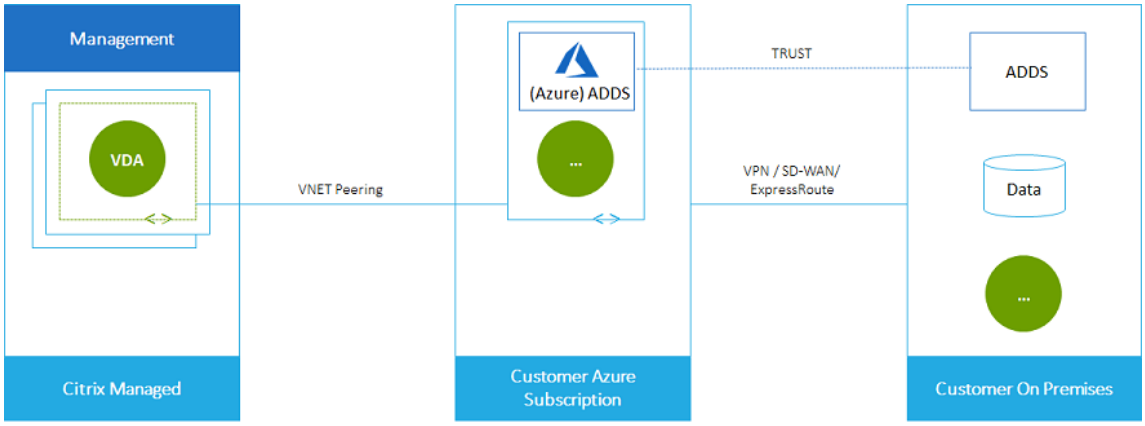
- **Azure Active Directory do cliente com acesso local:** Esta implantação contém VDAs não ingressados no domínio. Você usa seu próprio AD ou AAD para autenticação de usuário final. Nesse cenário, a instalação do Citrix Cloud Connectors em sua rede local permite o acesso aos recursos dessa rede.



- **Serviços de Domínio do Azure Active Directory e emparelhamento VNet do Cliente:** se o seu AD ou AAD residir em sua própria assinatura do Azure VNet e Azure, você poderá usar o recurso de emparelhamento VNet do Microsoft Azure para uma conexão de rede e os Serviços de Domínio do Azure Active Directory (AADDS) para autenticação do usuário final. Os VDAs são unidos ao seu domínio.

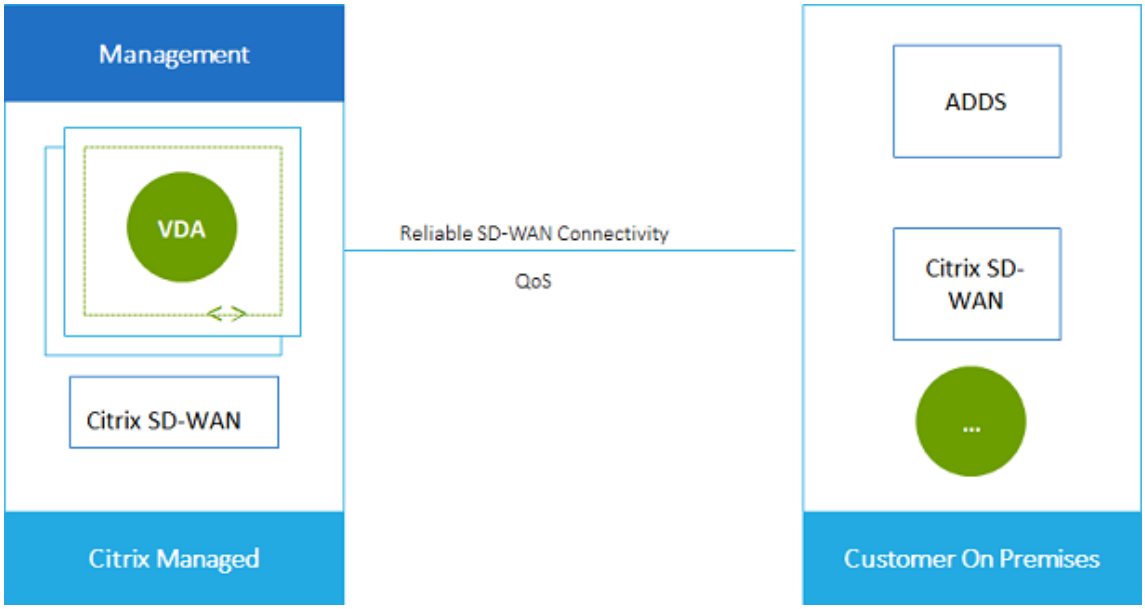


Para permitir que seus usuários acessem dados armazenados em sua rede local, você pode usar sua conexão VPN da sua assinatura do Azure para o local. O emparelhamento do Azure VNet é usado para conectividade de rede. Os Serviços de Domínio do Active Directory no local são usados para autenticação do usuário final.

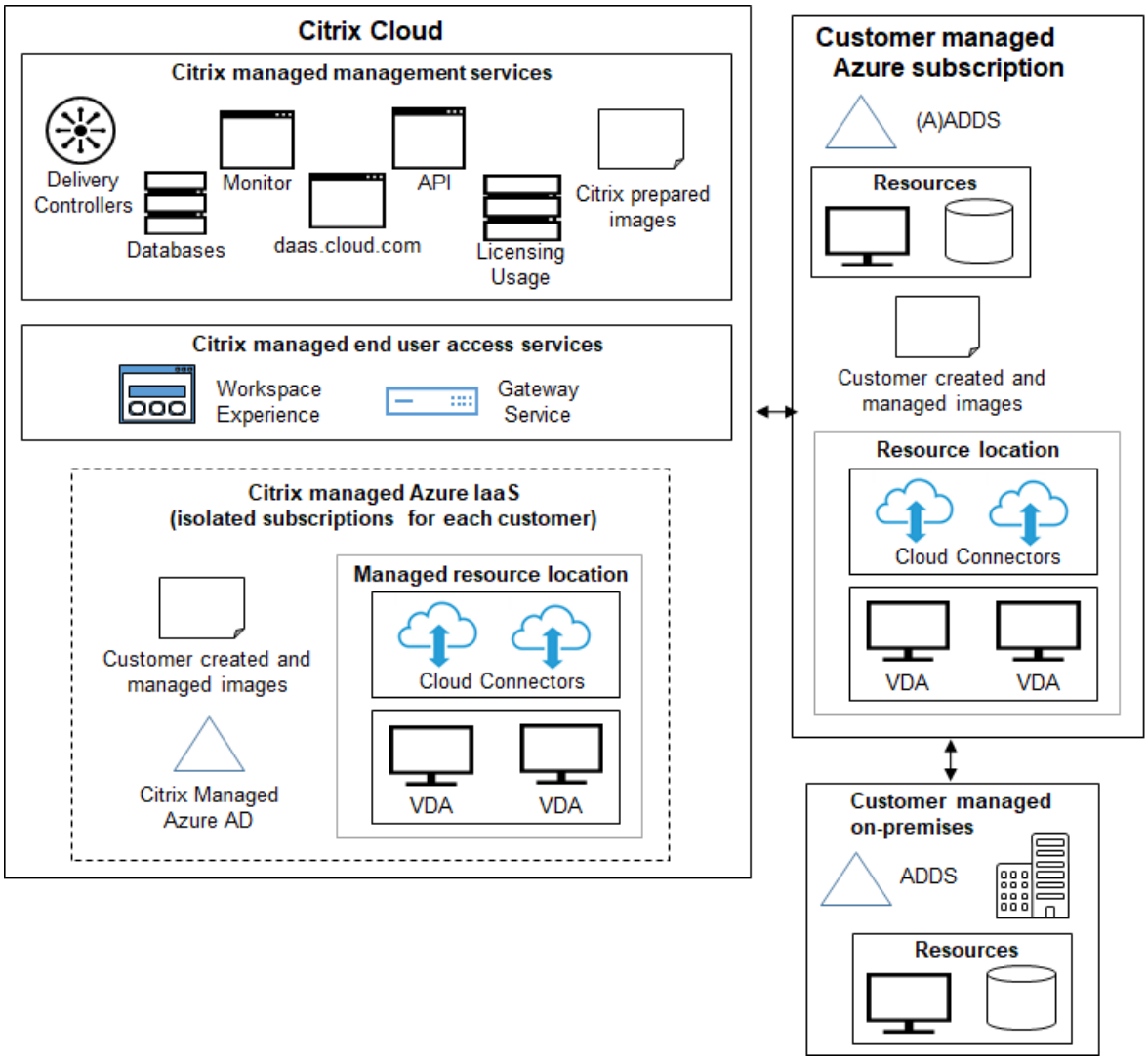


- **Active Directory e SD-WAN do cliente:** você pode fornecer aos usuários acesso a arquivos e outros itens de suas redes SD-WAN locais ou na nuvem.

  O Citrix SD-WAN otimiza todas as conexões de rede necessárias para o Citrix DaaS for Azure. Trabalhando em conjunto com as tecnologias HDX, o Citrix SD-WAN fornece qualidade de serviço e confiabilidade de conexão para ICA e Citrix DaaS fora de banda para tráfego Azure.



Implantação em uma assinatura do Azure gerenciada pelo cliente



A implantação no gráfico anterior usa uma assinatura do Azure gerenciada pelo cliente. No entanto, a assinatura do Citrix Managed Azure continua sendo uma opção para outros catálogos e imagens, conforme indicado pelo contorno pontilhado.

Interfaces de gerenciamento

O Citrix DaaS para Azure tem duas interfaces gráficas de gerenciamento: Implantação rápida e Configuração completa.

- O**Quick Deploy** permite que você crie catálogos rapidamente e comece a fornecer desktops e aplicativos para seus usuários. (Daí o nome, Quick Deploy.) É a interface padrão quando você inicia o Citrix DaaS para Azure. Você também pode acessar essa interface selecionando **Geren-**

ciar > Implantação Rápida do Azure. As instruções neste conjunto de documentação do produto pressupõem que você esteja usando o Quick Deploy.

Se você planeja usar uma assinatura do Citrix Managed Azure ao criar um catálogo ou uma imagem, você deve usar o Quick Deploy.

- A**configuração completa** oferece recursos avançados e opções de configuração para personalizar e gerenciar sua implantação. Os catálogos que você cria no Quick Deploy aparecem automaticamente em Configuração completa. Para passar da Implantação Rápida para a Configuração Completa, selecione **Gerenciar > Configuração Completa**.

  Quando você cria um catálogo na Implantação rápida, um grupo de entrega associado e uma conexão de host são criados automaticamente na Configuração completa.

  A Configuração Completa também oferece seu próprio processo de criação de catálogo, que inclui a criação de uma conexão com o host do Azure e, em seguida, a criação de um catálogo e um grupo de entrega. Esse processo só terá suporte se você usar sua própria assinatura do Azure. É muito mais fácil criar o catálogo no Quick Deploy.

  A Configuração Completa oferece suporte a processos relacionados a hosts de serviço de nuvem e hipervisor que não o Azure. Eles não estão disponíveis para o Citrix DaaS para clientes do Azure.

Gerenciar catálogos criados na interface Quick Deploy

Depois de criar um catálogo na interface Quick Deploy, você pode continuar a gerenciar esse catálogo nessa interface. Para obter detalhes, consulte Gerenciar catálogos. Você também pode usar a interface de configuração completa.

Quando você cria um catálogo no Quick Deploy, o catálogo (mais o grupo de entrega e a conexão de hospedagem que são criados automaticamente nos bastidores) recebem um escopo de `Citrix managed object`. Os escopos são usados na administração delegada para objetos de grupo.

Catálogos, grupos de entrega e conexões com o escopo `Citrix managed object` são proibidos de determinadas ações na interface Full Configuration. (Permitir essas ações na Full Configuration pode afetar adversamente a capacidade do sistema de oferecer suporte à Quick Deploy e à Full Configuration, portanto, essas ações são desativadas.) Na interface Full Configuration:

- **Catálogo:** a maioria das ações de gerenciamento de catálogos não está disponível. Você não pode excluir um catálogo.
- **Grupo de entrega:** a maioria das ações de gerenciamento do grupo de entrega está disponível. Você não pode excluir o grupo de entrega.
- **Conexão:** A maioria das ações de gerenciamento de conexão não está disponível. Você não pode excluir uma conexão. Você não pode criar uma conexão baseada em uma conexão que tenha o escopo `Citrix managed object`.

Se você criar um catálogo na Quick Deploy usando sua própria assinatura do Azure (adicionada à Quick Deploy) e quiser gerenciar o catálogo (e seu grupo de entrega e conexão) inteiramente na Full Configuration, poderá *converter* o catálogo.

- A conversão de um catálogo restringe seu gerenciamento somente à interface Full Configuration. Depois que um catálogo é convertido, você não pode mais usar a interface de Quick Deploy para gerenciar esse catálogo.
- Depois que um catálogo é convertido, as ações que estavam anteriormente indisponíveis na Full Configuration podem ser selecionadas. (O escopo `Citrix managed object` é removido do catálogo convertido, do grupo de entrega e da conexão de hospedagem.)
- Para converter um catálogo:

  No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, clique em qualquer lugar na entrada do catálogo. Na guia **Details**, em **Advanced settings**, selecione **Convert Catalog**. Quando solicitado, confirme a conversão.
- Você não pode converter um catálogo que foi criado no Quick Deploy usando uma assinatura do Citrix Managed Azure.

Para obter informações sobre como gerenciar catálogos convertidos em Configuração completa, consulte:

- Gerenciar catálogos de máquinas (Configuração Completa refere-se a catálogos como catálogos de máquinas)
- Gerenciar grupos de entrega

Mais informações

Para obter detalhes técnicos, consulte:

- Arquitetura de referênciaCitrix Tech Zone
- Resumo técnico da Citrix TechZone

Para obter informações sobre como automatizar suas implantações, consulte a visualização da API pública de áreas de trabalho gerenciadas.

Quando você estiver pronto, comece.

Novidades

July 17, 2024

Uma meta da Citrix é fornecer novos recursos e atualizações de produtos aos clientes do Citrix DaaS for Azure quando eles estiverem disponíveis. Os novos lançamentos oferecem mais valor, então não há motivo para atrasar as atualizações. Para você, administrador do cliente, esse processo é transparente.

Atualizações de imagens preparadas pela Citrix

As imagens preparadas pela Citrix têm um Citrix Virtual Delivery Agent (VDA) instalado. Geralmente, novas versões do VDA são lançadas várias vezes por ano, e as imagens preparadas pela Citrix disponíveis são atualizadas automaticamente com o VDA mais recente. Para saber mais sobre recursos novos e aprimorados na versão atual do VDA, consulte:

- VDAs do Windows
- VDAs Linux

Julho 2024

Suporte à hibernação. Agora você pode criar máquinas virtuais que podem ser hibernadas. Enquanto uma máquina está hibernando, você não é cobrado pelo uso e economiza no consumo de energia. Os aplicativos e arquivos abertos são salvos quando a máquina começa a hibernar e ficam rapidamente disponíveis na próxima vez que um usuário se conecta à máquina. Para obter informações sobre como criar catálogos de máquinas que podem ser hibernadas e definir horários de hibernação, consulte Criar um catálogo usando a criação personalizada. Você também pode colocar máquinas individuais em hibernação usando a interface de gerenciamento de configuração completa. Para obter informações, consulte Desligar e reiniciar máquinas em um grupo de entrega.

Agosto 2022

- Esse recurso está disponível ao público em geral: agora você pode criar catálogos de máquinas associadas ao seu Azure Active Directory. Consulte Criar catálogos.

Maio 2022

- Agora você pode criar catálogos de máquinas associadas ao seu Azure Active Directory. Esse recurso está como Preview. Consulte Criar catálogos.
- Os Provedores de Serviços Citrix agora podem remover o serviço Citrix DaaS for Azure dos clientes. Consulte Remover um serviço.

Abril 2022

- A criação de conexão de host para Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central e Nutanix AHV já está disponível. Dessa forma, agora você pode usar hipervisores locais além do Azure.
- Alteração do nome do produto de Citrix Virtual Apps and Desktops Standard for Azure para Citrix DaaS Standard for Azure. Para obter mais informações sobre o rebranding de todas as ofertas do Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops), consulte O que há de novo no Citrix DaaS. Saiba mais sobre as mudanças de nome em nosso anúncio em nosso blog.

Janeiro 2022

- Ao criar catálogos, agora você pode armazenar suas máquinas no armazenamento SSD padrão. Anteriormente, apenas discos padrão (HDD) e SSD premium eram suportados.
- Suporte para essas novas regiões para hospedagem de cargas de trabalho VDA: Sul do Brasil, Índia Central, Leste do Japão, Centro-Sul dos EUA e Sul do Reino Unido.
- Instantâneos e restauração agora estão disponíveis para áreas de trabalho persistentes hospedadas no Citrix Managed Azure e BYO Azure. Veja instantâneo e restauração do VDA.
- O endereço IP público estático para todo o tráfego de saída dos VDAs hospedados agora está disponível. Você pode configurar um Gateway NAT do Azure para obter o endereço IP. Consulte Criar um endereço IP estático público.
- A VPN do Azure está disponível para visualização técnica. O Azure VPN permite conectar o Citrix Managed Azure diretamente aos datacenters locais. Consulte o Azure VPN Technical Preview.
- Novas imagens do Linux estão disponíveis para imagens preparadas pela Citrix.

Novembro 2021

- Testes de 7 dias aprovados automaticamente já estão disponíveis (além dos testes aprovados por vendas).
- Os Provedores de Serviços Citrix agora podem gerenciar usuários no painel **Gerenciar > Implantação Rápida do Azure** ou no console do Citrix Cloud. Para obter detalhes, consulte Acesso do parceiro ao provedor de identidade do cliente.

Outubro 2021

- Novas informações sobre o gerenciamento de catálogos criados no Quick Deploy.

Setembro 2021

- O conteúdo da API de visualização está disponível.
- Suporte para Windows Server 2022 (requer o mínimo de VDA 2106).

Julho 2021

- Interface de gerenciamento do Web Studio renomeada Configuração Completa.

Junho 2021

- Suporte para duas interfaces de gerenciamento: Quick Deploy e Web Studio.

Maio de 2021

- Este serviço oferece suporte à visualização da Continuidade do serviço.
- As imagens preparadas pela Citrix agora incluem versões de sessão única e multissessão do Ubuntu.
- Ao adicionar um Cloud Connector a um local de recurso, usando uma assinatura do Citrix Managed Azure, você pode especificar o tipo de desempenho da máquina do Cloud Connector.
- Ao criar um catálogo, as opções de desempenho da máquina incluem opções que correspondem ao tipo de geração (gen1 ou gen2) da imagem selecionada. Você pode atualizar um catálogo com uma imagem de tipo de geração diferente, se as máquinas do catálogo suportarem esse tipo de geração.

Abril 2022

- Alteração do nome do produto de Citrix Virtual Apps and Desktops Standard for Azure para Citrix DaaS Standard for Azure.

Janeiro 2021

- Suporte de visualização para visualizar o uso do compromisso de consumo.

Outubro 2020

- Você pode usar o recurso de sombra Monitorar para exibir ou trabalhar na VM ou sessão de um usuário.
- Suporte de produção para Acesso ao PC remoto.
- Opção de criação de catálogo aprimorada para usar sua licença qualificada do Azure Virtual Desktop ou Azure Hybrid Benefit
- Se uma ação de reinicialização em um computador não for bem-sucedida, você poderá usar uma ação de reinicialização forçada.

Setembro 2020

- Detalhes sobre imagens são reorganizados e expandidos. Por exemplo, agora você pode adicionar e editar notas sobre imagens que você preparou ou importou. Você também pode limitar o acesso apenas a endereços IP especificados.
- Ao criar uma conexão de emparelhamento VNet do Azure que usará um gateway de rede virtual do Azure, agora você também pode habilitar a propagação de rota do gateway de rede virtual.
- Alteração do nome do produto de Citrix Managed Desktops para Citrix Virtual Apps and Desktops Standard for Azure.

Agosto 2020

- Suporte de visualização para Acesso ao PC remoto.
- Uma imagem do Windows Server 2019 preparada pela Citrix já está disponível.

Julho de 2020

- Ao adicionar um Cloud Connector a um local de recurso, usando uma assinatura do Azure gerenciada pelo cliente, você pode especificar o tipo de desempenho da máquina do Cloud Connector e o grupo de recursos do Azure. Para obter detalhes, consulte Ações de localização do recurso.
- Ao criar um catálogo, você pode especificar um esquema de nomeação de máquina. Consulte Criar um catálogo usando a criação personalizada.

Junho 2020

- Em um ambiente CSP, as conexões SD-WAN são criadas por inquilino. Para que a opção de conexão SD-WAN esteja disponível para o administrador do CSP, o locatário deve ter um dire-

ito de serviço SD-WAN Orchestrator. Para obter detalhes, consulte Filtrar recursos por cliente (implantações de vários locatários).
- Suporte de produção para VDAs do Linux ao usar uma assinatura do Azure gerenciada pelo cliente.
- O limite de VDAs por assinatura agora é de 1.200.

Maio 2020

- Você pode adicionar outra assinatura do Citrix Managed Azure quando precisar de mais máquinas do que o limite por assinatura do Citrix Managed Azure.
- Informações adicionais sobre servidores DNS.

Março 2020

- Suporte de produção para conexões SD-WAN.

Fevereiro 2020

- Para visualizar as informações de uso da licença Citrix, siga as orientações em Monitorar a licença e o monitoramento de uso do Citrix DaaS Standard for Azure.
- Suporte de pré-visualização para catálogos contendo máquinas Red Hat Enterprise Linux ou Ubuntu. Esse recurso é válido somente ao usar uma assinatura do Azure gerenciada pelo cliente e requer uma imagem importada contendo um Citrix Linux VDA.
- Agora você pode configurar o balanceamento de carga vertical ou horizontal para todas as suas máquinas com várias sessões. (Anteriormente, todas as máquinas usavam balanceamento de carga horizontal.) Essa seleção global se aplica a todos os catálogos em sua implantação. Consulte Balanceamento de carga.
- Agora você pode adicionar uma assinatura do Azure se você não for um administrador global.
- Uma imagem preparada pela Citrix agora está disponível para o Windows 10 Enterprise Virtual Desktop (várias sessões) com o Office 365 ProPlus.

Janeiro 2020

- Adicione suporte para rotas personalizadas em conexões de emparelhamento VNet.
- Atualizações no artigo de segurança para aprimorar as informações de portas e regras.

Novembro 2019

- Suporte de visualização para conexões SD-WAN.

Outubro 2019

- Em Sistemas operacionais compatíveis, foram adicionadas entradas para:
  - Windows 7 (suporta apenas o VDA 7.15 com a atualização cumulativa mais recente).
  - Windows Server 2019.
- Uma imagem preparada para o Windows Server 2012 R2 Citrix já está disponível.
- Adicionadas informações de configurações de localização de recursos. Para obter detalhes, consulte Ações de localização do recursoe Configurações de localização do recurso ao criar um catálogo.

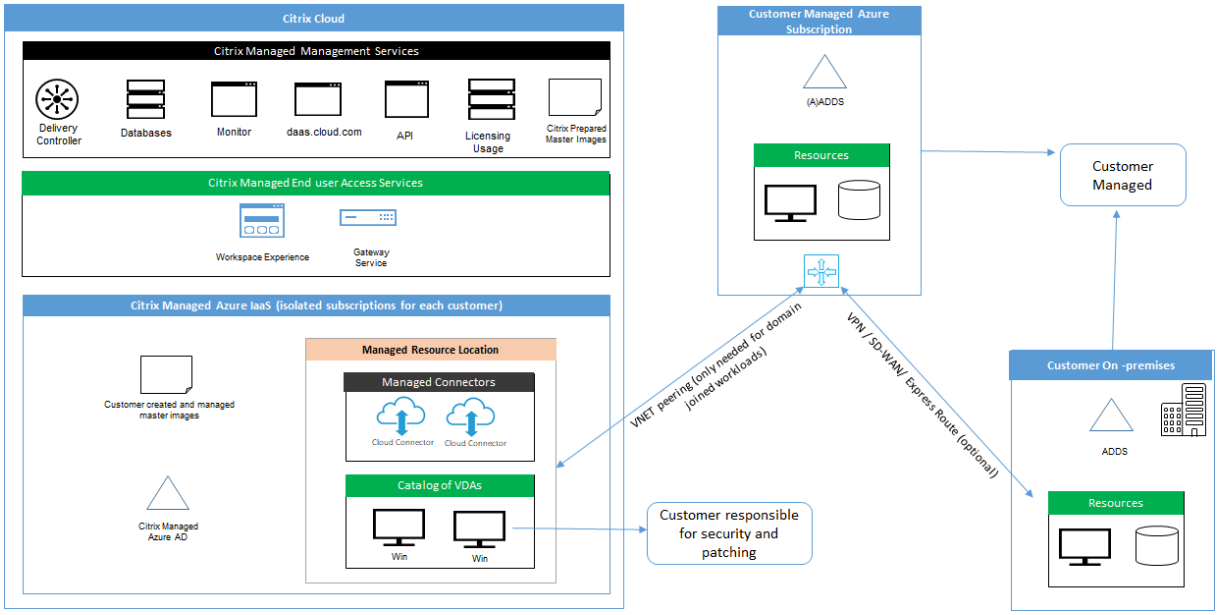
Setembro 2019

- Por padrão, as máquinas são criadas em uma assinatura do Citrix Managed Azure. Agora você também pode criar catálogos e imagens em sua própria assinatura do Azure gerenciada pelo cliente.

Visão técnica geral da segurança

July 20, 2022

O diagrama a seguir mostra os componentes em uma implantação do Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure). Este exemplo usa uma conexão de emparelhamento VNet.



Com o Citrix DaaS for Azure, os Virtual Delivery Agents (VDAs) do cliente que fornecem desktops e aplicativos, além do Citrix Cloud Connectors, são implantados em uma assinatura e locatário do Azure que a Citrix gerencia.

> **NOTA:**
>
> Este artigo fornece uma visão geral dos requisitos de segurança para clientes que implantam o Citrix DaaS for Azure usando uma assinatura do Citrix Managed Azure. Para obter uma visão geral da arquitetura de uma implantação do Citrix DaaS for Azure usando uma assinatura do Azure gerenciada pelo cliente, incluindo informações de segurança, consulte Arquitetura de referência: Virtual Apps and Desktops Service - Azure.

Conformidade de uso baseado em nuvem da Citrix

Desde janeiro de 2021, o uso da capacidade Citrix Managed Azure com várias edições do Citrix DaaS e Workspace Premium Plus ainda não foi avaliado em relação a Citrix SOC 2 (Tipo 1 ou 2), ISO 27001, HIPAA ou outros requisitos de conformidade na nuvem. Visite o Citrix Trust Center para obter mais informações sobre as certificações do Citrix Cloud e volte com frequência para ver mais atualizações.

Responsabilidade da Citrix

Citrix Cloud Connectors para catálogos não associados ao domínio

O Citrix DaaS for Azure implanta pelo menos dois Cloud Connectors em cada local de recurso. Alguns catálogos podem compartilhar um local de recurso se estiverem na mesma região que os outros catálogos para o mesmo cliente.

A Citrix é responsável pelas seguintes operações de segurança nos Cloud Connectors no catálogo não associado ao domínio:

- Aplicação de atualizações do sistema operacional e patches de segurança
- Instalação e manutenção do software antivírus
- Aplicação de atualizações de software do Cloud Connector

Os clientes não têm acesso aos Cloud Connectors. Portanto, a Citrix é totalmente responsável pelo desempenho dos Cloud Connectors no catálogo não associado ao domínio.

Assinatura do Azure e Azure Active Directory

A Citrix é responsável pela segurança da assinatura do Azure e do Azure Active Directory (AAD) criados para o cliente. A Citrix garante o isolamento do locatário, para que cada cliente tenha sua própria assinatura do Azure e AAD, e o crosstalk entre diferentes locatários seja evitado. A Citrix também

restringe o acesso ao AAD apenas ao pessoal de operações do Citrix DaaS for Azure e Citrix. O acesso da Citrix à assinatura do Azure de cada cliente é auditado.

Os clientes que empregam catálogos não associados ao domínio podem usar o AAD gerenciado pela Citrix como um meio de autenticação no Citrix Workspace. Para esses clientes, a Citrix cria contas de usuário com privilégios limitados no AAD gerenciado pela Citrix. No entanto, nem os usuários nem os administradores dos clientes podem realizar ações no AAD gerenciado pela Citrix. Se esses clientes optarem por usar seus próprios AAD, eles serão totalmente responsáveis por sua segurança.

Redes virtuais e infraestrutura

Na assinatura do Citrix Managed Azure do cliente, a Citrix cria redes virtuais para isolar os locais de recursos. Dentro dessas redes, a Citrix cria máquinas virtuais para VDAs, Cloud Connectors e máquinas com construtor de imagens, além de contas de armazenamento, cofres de chaves e outros recursos do Azure. A Citrix, em parceria com a Microsoft, é responsável pela segurança das redes virtuais, incluindo o firewall das redes virtuais.

A Citrix garante que a política de firewall padrão do Azure (grupos de segurança de rede) esteja configurada para limitar o acesso às interfaces de rede no emparelhamento VNet e conexões SD-WAN. Geralmente, isso controla o tráfego de entrada para VDAs e Cloud Connectors. Para obter detalhes, consulte:

- Política de firewall para conexões de emparelhamento Azure VNet
- Política de firewall para conexões SD-WAN

Os clientes não podem alterar essa política de firewall padrão, mas podem implantar regras de firewall adicionais em máquinas VDA criadas pela Citrix; por exemplo, para restringir parcialmente o tráfego de saída. Os clientes que instalam uma rede privada virtual cliente, ou outro software capaz de ignorar as regras de firewall, em máquinas VDA criadas pela Citrix são responsáveis por quaisquer riscos de segurança que possam resultar.

Ao usar o construtor de imagens no Citrix DaaS for Azure para criar e personalizar uma nova imagem de máquina, as portas 3389-3390 são abertas temporariamente na VNet gerenciada pela Citrix, para que o cliente possa fazer RDP para a máquina que contém a nova imagem da máquina, para personalizá-la.

Responsabilidade da Citrix ao usar conexões de emparelhamento Azure VNet

Para que os VDAs no Citrix DaaS for Azure entrem em contato com controladores de domínio locais, compartilhamentos de arquivos ou outros recursos da intranet, o Citrix DaaS for Azure fornece um fluxo de trabalho de emparelhamento de VNet como uma opção de conectividade. A rede virtual gerenciada pela Citrix do cliente é emparelhada com uma rede virtual Azure gerenciada pelo cliente.

A rede virtual gerenciada pelo cliente pode permitir a conectividade com os recursos locais do cliente usando a solução de conectividade de nuvem para local de escolha do cliente, como o Azure Express-Route ou túneis iPsec.

A responsabilidade da Citrix pelo emparelhamento de VNet é limitada ao suporte ao fluxo de trabalho e à configuração de recursos relacionados do Azure para estabelecer uma relação de emparelhamento entre a Citrix e as VNets gerenciadas pelo cliente.

Política de firewall para conexões de emparelhamento Azure VNet A Citrix abre ou fecha as seguintes portas para tráfego de entrada e saída que usa uma conexão de emparelhamento VNet.

VNet gerenciada pela Citrix com máquinas não associadas ao domínio

- Regras de entrada
  - Permitir a entrada nas portas 80, 443, 1494 e 2598 de VDAs para Cloud Connectors e de Cloud Connectors para VDAs.
  - Permitir a entrada pelas portas 49152-65535 para os VDAs a partir de um intervalo de IP usado pelo recurso de sombreamento Monitor. Consulte Portas de comunicação usadas pela Citrix Technologies.
  - Negar todas as outras entradas. Isso inclui o tráfego intra-VNet do VDA para o VDA e do VDA para o Cloud Connector.
- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pela Citrix com máquinas associadas ao domínio

- Regras de entrada:
  - Permitir a entrada nas portas 80, 443, 1494 e 2598 de VDAs para Cloud Connectors e de Cloud Connectors para VDAs.
  - Permitir a entrada pelas portas 49152-65535 para os VDAs a partir de um intervalo de IP usado pelo recurso de sombreamento Monitor. Consulte Portas de comunicação usadas pela Citrix Technologies.
  - Negar todas as outras entradas. Isso inclui o tráfego intra-VNet do VDA para o VDA e do VDA para o Cloud Connector.
- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pelo cliente com máquinas associadas ao domínio

- O cliente é responsável por configurar sua VNet corretamente. Isso inclui abrir as seguintes portas para associação do domínio.
- Regras de entrada:
  - Permitir a entrada na 443, 1494, 2598 de seus IPs clientes para inicializações internas.
  - Permitir a entrada na 53, 88, 123, 135-139, 389, 445, 636 do Citrix VNet (intervalo de IP especificado pelo cliente).
  - Permitir a entrada pelas portas abertas com uma configuração de proxy.
  - Outras regras criadas pelo cliente.
- Regras de saída:
  - Permitir a saída na 443, 1494, 2598 para o Citrix VNet (intervalo de IP especificado pelo cliente) para inicializações internas.
  - Outras regras criadas pelo cliente.

Responsabilidade da Citrix ao usar a conectividade SD-WAN

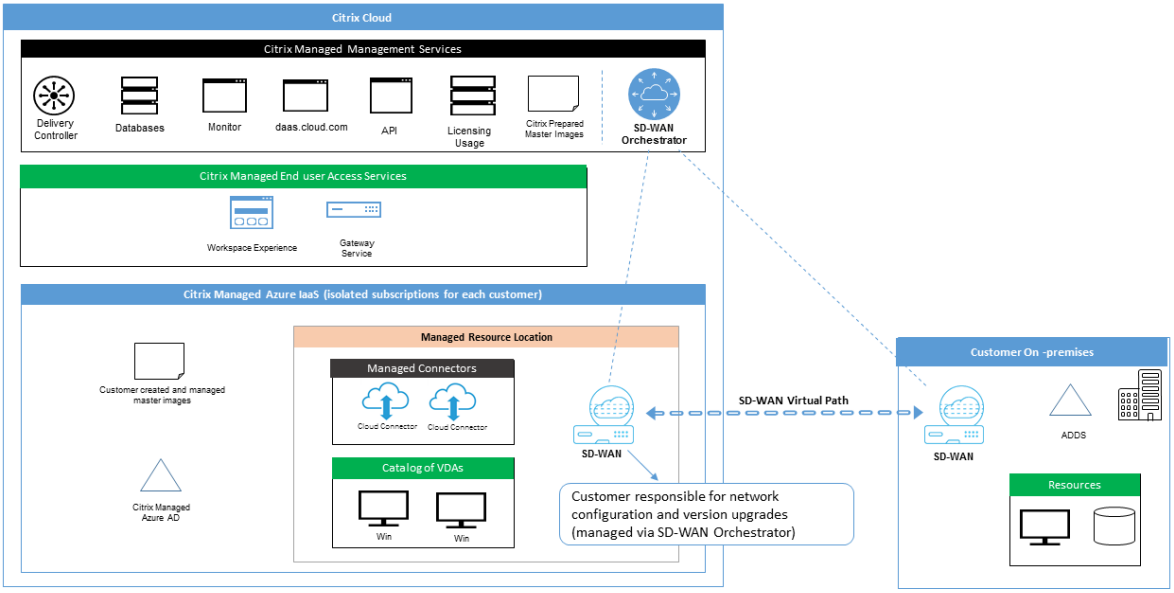
A Citrix oferece suporte a uma maneira totalmente automatizada de implantar instâncias virtuais do Citrix SD-WAN para permitir a conectividade entre o Citrix DaaS for Azure e os recursos locais. A conectividade Citrix SD-WAN tem várias vantagens em comparação com o emparelhamento VNet, incluindo:

Alta confiabilidade e segurança das conexões VDA-to-datacenter e VDA-to-branch (ICA).

- A melhor experiência de usuário final para funcionários de escritório, com recursos avançados de QoS e otimizações de VoIP.
- Capacidade interna de inspecionar, priorizar e gerar relatórios sobre o tráfego de rede do Citrix HDX e outros usos de aplicativo.

A Citrix exige que os clientes que desejam aproveitar a conectividade SD-WAN para Citrix DaaS for Azure usem o SD-WAN Orchestrator para gerenciar suas redes Citrix SD-WAN.

O diagrama a seguir mostra os componentes adicionados em uma implantação do Citrix DaaS para Azure usando a conectividade SD-WAN.



A implantação do Citrix SD-WAN para o Citrix DaaS for Azure é semelhante à configuração de implantação padrão do Azure para o Citrix SD-WAN. Para obter mais informações, consulte Implantar uma instância do Citrix SD-WAN Standard Edition no Azure. Em uma configuração de alta disponibilidade, um par ativo/em espera de instâncias de SD-WAN com balanceadores de carga do Azure é implantado como um gateway entre a sub-rede que contém VDAs e Cloud Connectors e a Internet. Em uma configuração sem HA (alta disponibilidade), apenas uma única instância de SD-WAN é implantada como gateway. As interfaces de rede dos dispositivos SD-WAN virtuais recebem endereços de um pequeno intervalo de endereços separado dividido em duas sub-redes.

Ao configurar a conectividade SD-WAN, a Citrix faz algumas alterações na configuração de rede das áreas de trabalho gerenciadas descritas acima. Em particular, todo o tráfego de saída da VNet, incluindo o tráfego para destinos da Internet, é roteado por meio da instância SD-WAN da nuvem. A instância de SD-WAN também está configurada para ser o servidor DNS da VNet gerenciada pela Citrix.

O acesso de gerenciamento às instâncias virtuais de SD-WAN requer login e senha de administrador. Cada instância de SD-WAN recebe uma senha segura exclusiva e aleatória que pode ser usada pelos administradores de SD-WAN para o login remoto e a solução de problemas por meio da interface do usuário do SD-WAN Orchestrator, interface do usuário de gerenciamento do dispositivo virtual e CLI.

Assim como outros recursos específicos do locatário, as instâncias virtuais de SD-WAN implantadas em uma VNet de cliente específica são totalmente isoladas de todas as outras VNets.

Quando o cliente habilita a conectividade do Citrix SD-WAN, a Citrix automatiza a implantação inicial de instâncias virtuais de SD-WAN usadas com o Citrix DaaS for Azure, mantém os recursos subjacentes

do Azure (máquinas virtuais, balanceadores de carga, etc.), fornece padrões prontos para uso seguros e eficientes para os configuração de instâncias virtuais de SD-WAN e permite manutenção e solução de problemas contínuas por meio do SD-WAN Orchestrator. A Citrix também toma medidas razoáveis para realizar a validação automática da configuração de rede SD-WAN, verificar riscos de segurança conhecidos e exibir alertas correspondentes por meio do SD-WAN Orchestrator.

Política de firewall para conexões SD-WAN A Citrix usa políticas de firewall do Azure (grupos de segurança de rede) e atribuição de endereço IP público para limitar o acesso às interfaces de rede de dispositivos SD-WAN virtuais:

- Somente interfaces WAN e de gerenciamento recebem endereços IP públicos e permitem conectividade de saída com a Internet.
- As interfaces LAN, atuando como gateways para a VNet gerenciada pela Citrix, só podem trocar tráfego de rede com máquinas virtuais na mesma VNet.
- As interfaces WAN limitam o tráfego de entrada para a porta UDP 4980 (usada pelo Citrix SD-WAN para conectividade de caminho virtual) e negam o tráfego de saída para a VNet.
- As portas de gerenciamento permitem o tráfego de entrada para as portas 443 (HTTPS) e 22 (SSH).
- As interfaces HA só podem trocar tráfego de controle entre si.

Acesso à infraestrutura

A Citrix pode acessar a infraestrutura do cliente gerenciada pela Citrix (Cloud Connectors) para executar determinadas tarefas administrativas, como coletar logs (incluindo o Windows Event Viewer) e reiniciar serviços sem notificar o cliente. A Citrix é responsável por executar essas tarefas com segurança e com impacto mínimo para o cliente. A Citrix também é responsável por garantir que todos os arquivos de log sejam recuperados, transportados e manipulados com segurança. Os VDAs do cliente não podem ser acessados dessa forma.

Backups de catálogos não associados ao domínio

A Citrix não é responsável por realizar backups de catálogos não associados ao domínio.

Backups de imagens de máquinas

A Citrix é responsável por fazer backup de todas as imagens de máquina carregadas no Citrix DaaS for Azure, incluindo imagens criadas com o construtor de imagens. A Citrix usa armazenamento com redundância local para essas imagens.

Bastions para catálogos não associados ao domínio

O pessoal de operações da Citrix tem a capacidade de criar um bastion, se necessário, para acessar a assinatura do Azure gerenciado pela Citrix do cliente para diagnosticar e reparar problemas do cliente, possivelmente antes que o cliente esteja ciente do problema. A Citrix não precisa do consentimento do cliente para criar um bastion. Quando a Citrix cria o bastion, a Citrix cria uma senha forte gerada aleatoriamente para o bastion e restringe o acesso RDP aos endereços IP NAT da Citrix. Quando o bastion não é mais necessário, a Citrix o descarta e a senha não é mais válida. O bastion e as regras de acesso RDP que o acompanham são descartados quando a operação é concluída. Com o bastion, a Citrix pode acessar apenas os Cloud Connectors não associados ao domínio do cliente. A Citrix não tem a senha para fazer login em VDAs não associados ao domínio ou em VDAs e Cloud Connectors associados ao domínio.

Política de firewall ao usar ferramentas de solução de problemas

Quando um cliente solicita a criação de uma máquina bastion para a solução de um problema, as seguintes modificações do grupo de segurança são feitas na VNet gerenciada pela Citrix:

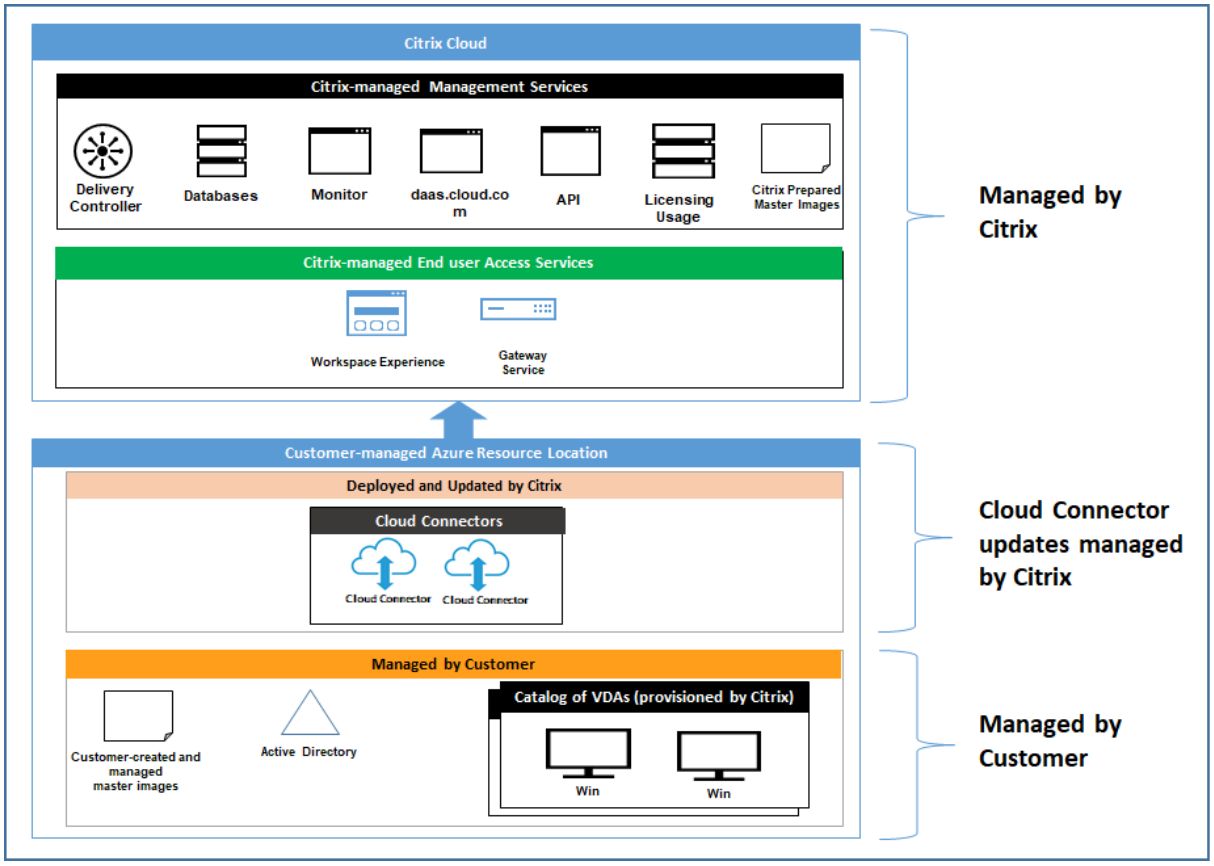
- Permitir temporariamente a entrada pela 3389 do intervalo de IP especificado pelo cliente para o bastion.
- Permitir temporariamente a entrada pela 3389 do endereço IP do bastion para qualquer endereço na VNet (VDAs e Cloud Connectors).
- Continuar e bloquear o acesso RDP entre os Cloud Connectors, os VDAs e outros VDAs.

Quando um cliente habilita o acesso RDP para a solução de um problema, as seguintes modificações do grupo de segurança são feitas na VNet gerenciada pela Citrix:

- Permitir temporariamente a entrada pela 3389 do intervalo de IP especificado pelo cliente para qualquer endereço na VNet (VDAs e Cloud Connectors).
- Continuar e bloquear o acesso RDP entre os Cloud Connectors, os VDAs e outros VDAs.

Assinaturas gerenciadas pelo cliente

Para assinaturas gerenciadas pelo cliente, a Citrix adere às responsabilidades acima durante a implantação dos recursos do Azure. Após a implantação, tudo acima é de responsabilidade do cliente, porque o cliente é o proprietário da assinatura do Azure.



Responsabilidade do cliente

VDAs e imagens de máquinas

O cliente é responsável por todos os aspectos do software instalado nas máquinas VDA, incluindo:

- Atualizações do sistema operacional e patches de segurança
- Antivírus e antimalware
- Atualizações de software do VDA e patches de segurança
- Regras adicionais de firewall de software (especialmente tráfego de saída)
- Siga as considerações de segurança e práticas recomendadas da Citrix

A Citrix fornece uma imagem preparada que se destina a ser um ponto de partida. Os clientes podem usar essa imagem para fins de prova de conceito ou demonstração ou como base para criar sua própria imagem de máquina. A Citrix não garante a segurança dessa imagem preparada. A Citrix tentará manter o sistema operacional e o software do VDA na imagem preparada atualizados e habilitará o Windows Defender nessas imagens.

Responsabilidade do cliente ao usar o emparelhamento VNet

O cliente deve abrir todas as portas especificadas na VNet gerenciada pelo cliente com máquinas associadas ao domínio.

Quando o emparelhamento VNet é configurado, o cliente é responsável pela segurança de sua própria rede virtual e da conectividade da rede com seus recursos locais. O cliente também é responsável pela segurança do tráfego de entrada da rede virtual emparelhada gerenciada pela Citrix. A Citrix não toma nenhuma ação para bloquear o tráfego da rede virtual gerenciada pela Citrix aos recursos locais do cliente.

Os clientes têm as seguintes opções para restringir o tráfego de entrada:

- Dar à rede virtual gerenciada pela Citrix um bloco de IP que não está em uso em nenhum outro lugar na rede local do cliente ou na rede virtual conectada gerenciada pelo cliente. Isso é necessário para o emparelhamento VNet.
- Adicionar firewalls e grupos de segurança de rede do Azure à rede virtual e à rede local do cliente para bloquear ou restringir o tráfego do bloco de IP gerenciado pela Citrix.
- Implementar medidas como sistemas de prevenção de intrusões, firewalls de software e mecanismos de análise comportamental na rede virtual e na rede local do cliente, visando o bloco de IP gerenciado pela Citrix.

Responsabilidade do cliente ao usar a conectividade SD-WAN

Quando a conectividade SD-WAN é configurada, os clientes têm total flexibilidade para configurar instâncias virtuais de SD-WAN usadas com o Citrix DaaS for Azure de acordo com seus requisitos de rede, com exceção de alguns elementos necessários para garantir a operação correta da SD-WAN na VNet gerenciada pela Citrix. As responsabilidades do cliente incluem:

- Projeto e configuração de regras de roteamento e firewall, incluindo regras de ruptura de tráfego de DNS e Internet.
- Manutenção da configuração de rede SD-WAN.
- Monitoramento do status operacional da rede.
- Implantação rápida de atualizações de software Citrix SD-WAN ou correções de segurança. Como todas as instâncias do Citrix SD-WAN em uma rede de cliente devem executar a mesma versão do software SD-WAN, as implantações de versões de software atualizadas no Citrix DaaS para instâncias do Azure SD-WAN precisam ser gerenciadas pelos clientes de acordo com suas programações e restrições de manutenção de rede.

A configuração incorreta das regras de roteamento e firewall da SD-WAN ou o gerenciamento incorreto de senhas de gerenciamento da SD-WAN podem resultar em riscos de segurança para os recursos virtuais no Citrix DaaS for Azure e recursos locais acessíveis por meio de caminhos virtuais do Citrix

SD-WAN. Outro possível risco de segurança decorre da não atualização do software Citrix SD-WAN com a versão de patch mais recente disponível. Embora o SD-WAN Orchestrator e outros serviços do Citrix Cloud forneçam os meios para lidar com esses riscos, os clientes são responsáveis por garantir que as instâncias virtuais de SD-WAN sejam configuradas adequadamente.

Proxy

O cliente pode optar por usar um proxy para o tráfego de saída do VDA. Se for usado um proxy, o cliente será responsável por:

- Configurar os parâmetros do proxy na imagem da máquina VDA ou, se o VDA estiver associado a um domínio, usar a Política de Grupo do Active Directory.
- Cuidar da manutenção e segurança do proxy.

Proxies não são permitidos para uso com Citrix Cloud Connectors ou outra infraestrutura gerenciada pela Citrix.

Resiliência de catálogo

A Citrix fornece três tipos de catálogos com diferentes níveis de resiliência:

- **Estático:** cada usuário é atribuído a um único VDA. Esse tipo de catálogo não oferece alta disponibilidade. Se o VDA de um usuário sair do ar, ele precisará ser colocado em um novo para se recuperar. O Azure fornece um SLA de 99,5% para VMs de instância única. O cliente ainda pode fazer backup do perfil do usuário, mas todas as personalizações feitas no VDA (como instalar programas ou configurar o Windows) serão perdidas.
- **Aleatório:** cada usuário é atribuído aleatoriamente a um servidor VDA no momento da inicialização. Esse tipo de catálogo fornece alta disponibilidade por meio de redundância. Se um VDA sair do ar, nenhuma informação será perdida porque o perfil do usuário reside em outro lugar.
- **Windows 10 multissessão:** esse tipo de catálogo opera da mesma maneira que o tipo aleatório, mas usa VDAs de estação de trabalho do Windows 10 em vez de VDAs de servidor.

Backups para catálogos associados ao domínio

Se o cliente usar catálogos associados ao domínio com um emparelhamento VNet, o cliente será responsável por fazer backup de seus perfis de usuário. A Citrix recomenda que os clientes configurem compartilhamentos de arquivos locais e definam políticas em seus Active Directory ou VDAs para extrair perfis de usuário desses compartilhamentos de arquivos. O cliente é responsável pelo backup e pela disponibilidade desses compartilhamentos de arquivos.

Recuperação de desastres

No caso de perda de dados do Azure, a Citrix recuperará o maior número possível de recursos na assinatura do Azure gerenciada pela Citrix. A Citrix tentará recuperar os Cloud Connectors e os VDAs. Se a Citrix não conseguir recuperar esses itens, os clientes serão responsáveis pela criação de um novo catálogo. A Citrix pressupõe que o backup das imagens da máquina seja feito regularmente e que os clientes fizeram backup de seus perfis de usuário, permitindo que o catálogo seja reconstruído.

No caso de perda de uma região inteira do Azure, o cliente é responsável por recriar sua rede virtual gerenciada pelo cliente em uma nova região e criar um novo emparelhamento de VNet ou uma nova instância de SD-WAN no Citrix DaaS for Azure.

Responsabilidades compartilhadas entre a Citrix e o cliente

Citrix Cloud Connector para catálogos associados ao domínio

O Citrix DaaS for Azure implanta pelo menos dois Cloud Connectors em cada local de recurso. Alguns catálogos podem compartilhar um local de recurso se estiverem na mesma região, emparelhamento VNet e domínio que outros catálogos para o mesmo cliente. A Citrix configura os Cloud Connectors associados ao domínio do cliente para as seguintes configurações de segurança padrão na imagem:

- Atualizações do sistema operacional e patches de segurança
- Software antivírus
- Atualizações do software Cloud Connector

Os clientes normalmente não têm acesso aos Cloud Connectors. No entanto, eles podem adquirir acesso usando as etapas de solução de problemas do catálogo e fazendo login com as credenciais do domínio. O cliente é responsável por quaisquer alterações que fizer ao fazer login pelo bastion.

Os clientes também têm controle sobre os Cloud Connectors associados ao domínio por meio da Política de Grupo do Active Directory. O cliente é responsável por garantir que as políticas de grupo que se aplicam ao Cloud Connector sejam seguras e sensatas. Por exemplo, se o cliente optar por desativar as atualizações do sistema operacional usando a Política de Grupo, o cliente será responsável por realizar atualizações do sistema operacional nos Cloud Connectors. O cliente também pode optar por usar a Política de Grupo para impor uma segurança mais rígida do que os padrões do Cloud Connector, por exemplo, instalando um software antivírus diferente. Em geral, a Citrix recomenda que os clientes coloquem os Cloud Connectors em suas próprias unidades organizacionais do Active Directory sem políticas, pois isso garantirá que os padrões usados pela Citrix possam ser aplicados sem problemas.

Solução de problemas

Caso o cliente tenha problemas com o catálogo no Citrix DaaS for Azure, há duas opções de solução de problemas: usar bastiões e habilitar o acesso RDP. Ambas as opções apresentam risco de segurança para o cliente. O cliente deve entender, consentir e assumir esse risco antes de usar essas opções.

A Citrix é responsável por abrir e fechar as portas necessárias para realizar operações de solução de problemas e restringir quais máquinas podem ser acessadas durante essas operações.

Com bastions ou acesso RDP, o usuário ativo que executa a operação é responsável pela segurança das máquinas que estão sendo acessadas. Se o cliente acessar o VDA ou o Cloud Connector por meio do RDP e contrair um vírus acidentalmente, o cliente será responsável. Se a equipe de suporte Citrix acessar essas máquinas, esse pessoal terá a responsabilidade de realizar as operações com segurança. A responsabilidade por vulnerabilidades expostas por qualquer pessoa que acesse o bastion ou outras máquinas na implantação (por exemplo, a responsabilidade do cliente de adicionar intervalos de IP à lista de permissão, a responsabilidade da Citrix de implementar intervalos de IP corretamente) é abordada em outro lugar neste documento.

Nos dois cenários, a Citrix é responsável por criar corretamente exceções de firewall para permitir o tráfego RDP. A Citrix também é responsável por revogar essas exceções depois que o cliente se desfaz do bastião ou encerra o acesso RDP por meio do Citrix DaaS for Azure.

Bastions A Citrix pode criar bastions na rede virtual gerenciada pela Citrix do cliente dentro da assinatura gerenciada pela Citrix do cliente para diagnosticar e reparar problemas, de forma proativa (sem notificação do cliente) ou em resposta a um problema levantado pelo cliente. O bastion é uma máquina que o cliente pode acessar por meio do RDP e usar para acessar os VDAs e Cloud Connectors (para catálogos associados ao domínio) por meio do RDP para coletar logs, reiniciar serviços ou executar outras tarefas administrativas. Por padrão, a criação de um bastion abre uma regra de firewall externo para permitir o tráfego RDP de um intervalo de endereços IP especificado pelo cliente para a máquina bastion. Também abre uma regra de firewall interno para permitir o acesso aos Cloud Connectors e VDAs por meio do RDP. Abrir essas regras representa um grande risco de segurança.

O cliente é responsável por fornecer uma senha forte usada para a conta local do Windows. O cliente também é responsável por fornecer um intervalo de endereços IP externo que permita o acesso RDP ao bastion. Se o cliente optar por não fornecer um intervalo de IP (permitindo que qualquer pessoa tente o acesso RDP), o cliente será responsável por qualquer tentativa de acesso por endereços IP maliciosos.

O cliente também é responsável por excluir o bastion após concluir solução de problemas. O host bastion expõe a superfície de ataque adicional, assim a Citrix desliga automaticamente a máquina oito (8) horas depois que ela é ligada. No entanto, a Citrix nunca exclui um bastion automaticamente. Se o cliente optar por usar o bastion por um longo período de tempo, ele será responsável por aplicar patches e atualizá-lo. A Citrix recomenda que um bastion seja usado apenas por alguns dias antes de

excluí-lo. Se o cliente quiser um bastion atualizado, ele poderá excluir o atual e criar um novo bastion, que provisionará uma nova máquina com os patches de segurança mais recentes.

Acesso RDP Para catálogos associados ao domínio, se o emparelhamento VNet do cliente estiver funcional, o cliente poderá habilitar o acesso RDP da sua VNet emparelhada à VNet gerenciada pela Citrix. Se o cliente usar essa opção, o cliente será responsável por acessar os VDAs e os Cloud Connectors através do emparelhamento VNet. Os intervalos de endereços IP de origem podem ser especificados para que o acesso RDP possa ser restringido ainda mais, mesmo dentro da rede interna do cliente. O cliente precisará usar credenciais de domínio para fazer login nessas máquinas. Se o cliente estiver trabalhando com o Suporte Citrix para resolver um problema, talvez seja necessário que o cliente compartilhe essas credenciais com a equipe de suporte. Depois que o problema for resolvido, o cliente será responsável por desativar o acesso RDP. Manter o acesso RDP aberto a partir da rede local ou emparelhada do cliente representa um risco à segurança.

Credenciais de domínio

Se o cliente optar por usar um catálogo associado ao domínio, o cliente será responsável por fornecer ao Citrix DaaS for Azure uma conta de domínio (nome de usuário e senha) com permissões para unir máquinas ao domínio. Ao fornecer credenciais de domínio, o cliente é responsável por aderir aos seguintes princípios de segurança:

- **Auditável:** a conta deve ser criada especificamente para o Citrix DaaS para uso do Azure, para que seja fácil auditar para que a conta é usada.
- **Com escopo:** a conta requer apenas permissões para associar máquinas a um domínio. Ela não deve ter permissões completas de administrador de domínio.
- **Seguro:** uma senha forte deve ser usada para a conta.

A Citrix é responsável pelo armazenamento seguro dessa conta de domínio em um Azure Key Vault na assinatura do Azure gerenciada pela Citrix do cliente. A conta será recuperada somente se uma operação exigir a senha da conta de domínio.

Mais informações

Para obter informações relacionadas, consulte:

- Guia de implantação segura para a plataforma Citrix Cloud: informações de segurança para a plataforma Citrix Cloud.
- Visão técnica geral da segurança: informações de segurança para o Citrix DaaS
- Notificações de terceiros

Assine o Citrix DaaS para Azure

December 21, 2022

Introdução

Você pode assinar o Citrix DaaS Standard for Azure (antigo serviço Citrix Virtual Apps and Desktops Standard for Azure) e solicitar o Citrix Azure Consumption Fund, por meio da Citrix ou do Azure Marketplace. Você pode avaliar o Citrix DaaS for Azure por meio do Citrix.

Se você atualmente assina o Citrix Virtual Apps Essentials ou o Citrix Virtual Desktops Essentials, poderá atualizar para o Citrix DaaS Standard for Azure.

Um pedido abrangente tem duas partes:

- **Citrix DaaS Standard for Azure:** permite que você use suas próprias assinaturas do Azure (gerenciadas pelo cliente).
- **Fundo de Consumo do Citrix Azure:** Além disso, permite que você use uma assinatura do Citrix Managed Azure, além de suas próprias assinaturas do Azure. O uso de uma assinatura do Citrix Managed Azure oferece os seguintes benefícios:
  - Faturamento único da Citrix, em vez de faturamento de várias empresas.
  - Diferenças de recursos de assinatura do Azure.
  - Suporte Microsoft de nível premium por meio da Citrix.

O Fundo de Consumo do Citrix Azure não é obrigatório. No entanto, se você não tiver, estará restrito a usar apenas suas próprias assinaturas do Azure e não receberá os outros benefícios do recurso.

O processo de pedido difere um pouco, dependendo se você faz o pedido por meio da Citrix ou do Azure Marketplace:

- Ao fazer pedidos pela Citrix, você pode solicitar o Citrix DaaS Standard for Azure e o Citrix Azure Consumption Fund ao mesmo tempo.
- Ao fazer pedidos pelo Azure Marketplace, você primeiro pede o Citrix DaaS Standard for Azure. Em seguida, você pede o Citrix Azure Consumption Fund.

  Se você decidir solicitar apenas o Citrix DaaS para Azure, poderá solicitar o Fundo de Consumo do Citrix Azure posteriormente, por meio do Azure Marketplace ou por meio de seu representante de conta Citrix.

Independentemente de onde você compra o Citrix DaaS Standard for Azure e do fundo de consumo, a Citrix fornece ajuda de integração. Também verificaremos se o Citrix DaaS Standard for Azure está sendo executado e configurado corretamente.

Resumo do pedido

Resumo das etapas do pedido:

1. Obtenha uma conta do Citrix Cloud.

   Se você já tem uma conta do Citrix Cloud e atualmente assina o Citrix DaaS, consulte Se você atualmente assina o Citrix DaaS.

2. Encomende o Citrix DaaS Standard for Azure e o fundo de consumo por meio do Azure Marketplaceou faça o pedido pelo Citrix.

Julgamentos

O Citrix DaaS Standard for Azure oferece dois tipos de testes:

- **Aprovado por vendas:** em uma avaliação aprovada por vendas, você pode usar uma assinatura do Citrix Managed Azure para criar catálogos, imagens e outras tarefas. Na avaliação, você pode converter para uma assinatura de serviço paga e solicitar o Citrix Managed Azure Consumption Fund. Se você não comprar o consumo, todos os recursos criados usando a assinatura do Citrix Managed Azure serão excluídos automaticamente, o que pode afetar os usuários.
- **Aprovado automaticamente:** em uma avaliação aprovada automaticamente, você pode usar sua própria assinatura do Azure (gerenciada pelo cliente) para criar catálogos, imagens e outras tarefas. Na avaliação, você pode converter para uma assinatura paga. Para obter mais informações, consulte Avaliações de serviço aprovadas automaticamente.

Para obter mais informações sobre avaliações, consulte Avaliações de serviço do Citrix Cloud.

Testes de serviço aprovados automaticamente

- Uma avaliação aprovada automaticamente do Citrix DaaS Standard for Azure dura 7 dias corridos.
- Durante uma avaliação aprovada automaticamente, você pode criar catálogos usando sua assinatura do Azure. Os catálogos contêm as máquinas que fornecem desktops ou aplicativos.
- Você pode criar catálogos usando uma imagem preparada pela Citrix, uma imagem importada do Azure ou uma imagem criada no Citrix DaaS Standard for Azure.
- Os usuários devem ser configurados em um provedor de identidade compatívelcom o Citrix Workspace.
- Você pode atribuir até 25 usuários a catálogos em sua implantação de avaliação. Embora você possa atribuir um usuário a mais de um catálogo, um total de 25 usuários nomeados exclusivos são permitidos em uma implantação de avaliação.

- Você deve ter uma conta de usuário do Microsoft Azure e pelo menos uma assinatura do Azure nessa conta. (As avaliações são compatíveis apenas com casos de uso de assinatura do Azure de propriedade do cliente (traga seus próprios).)

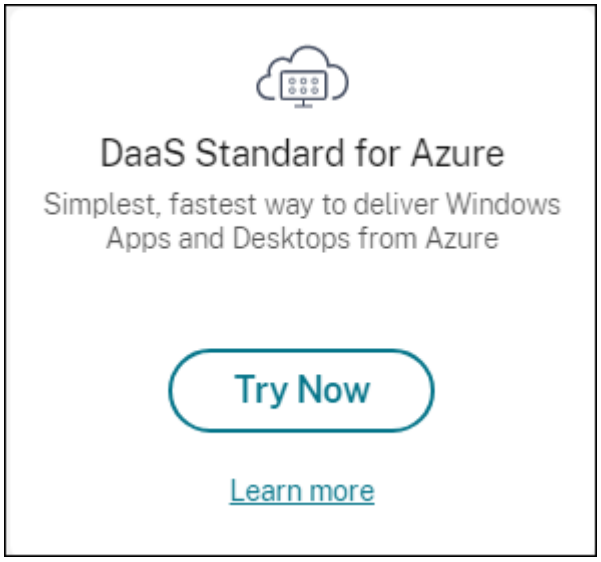
Solicitar e usar uma avaliação de serviço aprovada automaticamente

1. Inscreva-se para uma conta do Citrix Cloud (se você ainda não tiver uma).

   a) Navegue até o Citrix Cloud.
   b) Selecione **Inscrever-se e experimente gratuitamente**.
   c) Siga as orientações na tela.

   Em alguns instantes, você receberá um e-mail sobre sua conta do Citrix Cloud. Selecione o link de login no e-mail.

2. Solicite um teste. No console do Citrix Cloud, selecione **Experimente agora** no bloco **DaaS Standard for Azure** .

   Você receberá um e-mail quando a avaliação do serviço estiver ativada e pronta (geralmente cerca de duas horas depois de solicitar a avaliação).

3. Faça login no Citrix Cloud.
4. Clique em **Gerenciar** no bloco **DaaS Standard for Azure** .
5. Configure e configure seu ambiente de avaliação. Durante a configuração, você irá:

   a) Adicione sua assinatura do Azure ao serviço.
   b) Conecte seu provedor de identidade por meio do console do Citrix Cloud.
   c) Crie um catálogo.
   d) Adicione usuários do seu provedor de identidade ao catálogo.

e) Notifique seus usuários sobre o URL do Citrix Workspace.

A interface gráfica o orienta durante o processo de configuração. Para obter detalhes, consulte a documentação do produto:

- Familiarize-se com o produto e sua terminologia.
- Analise os resumos e os detalhes da configuração.

Obtenha uma conta do Citrix Cloud

Para se inscrever em uma conta do Citrix Cloud e solicitar uma avaliação, acesse https://onboarding.cloud.com. Para obter detalhes sobre esse processo, consulte Inscrever-se no Citrix Cloud. Sua conta tem um Organization ID (OrgID) que sempre aparece no canto superior direito do console do Citrix Cloud.

Próximas etapas: Encomende o Citrix DaaS Standard for Azure por meio do Citrix ou do Azure Marketplace.

Se você atualmente assina o Citrix DaaS

Uma conta Citrix Cloud (OrgID) permite que você assine apenas uma edição do Citrix DaaS por vez.

Você pode atualizar do Citrix DaaS Standard for Azure para uma das seguintes edições:

- Edição Citrix DaaS Advanced
- Edição Citrix DaaS Premium.

Entre em contato com seu representante Citrix para obter detalhes.

Se você atualmente assina uma edição do Citrix DaaS diferente de Advanced ou Premium (por exemplo, Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials) e deseja assinar o Citrix DaaS Standard for Azure, você deve:

- Assine o Citrix DaaS Standard for Azure usando uma conta diferente do Citrix Cloud (OrgID). Para obter detalhes, consulte Atualizar para o Citrix DaaS Standard for Azure.
- Descomissione o serviço que você tem e, em seguida, solicite o Citrix DaaS Standard for Azure. Para obter instruções para desinstalação, consulte CTX239027.

Você pode usar uma assinatura do Citrix Managed Azure comprando o Fundo de Consumo do Citrix Azure com qualquer uma das seguintes edições de serviço:

- Citrix DaaS Standard para Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Pedidos pela Citrix

Você pode solicitar o Citrix DaaS Standard for Azure (incluindo o fundo de consumo) por meio do Citrix Cloud ou do representante da sua conta Citrix.

Por meio do Citrix Cloud:

1. Faça login no Citrix Cloud. Clique em **Experimentar agora** no bloco **DaaS Standard for Azure** . Preencha as informações solicitadas. O texto no bloco muda para **Teste solicitado**.
2. A Citrix entra em contato com você. Quando o Citrix DaaS Standard for Azure está disponível para você usar, o texto no bloco muda para **Gerenciar**.
3. Faça login no Citrix Cloud. No bloco **DaaS Standard for Azure**, clique em **Gerenciar**. Na primeira vez que você acessa o Citrix DaaS Standard for Azure, você será direcionado para a página de **boas-vindas** da Implantação rápida.

Cancelar uma assinatura mensal por meio da Citrix

As assinaturas mensais são renovadas automaticamente no início de cada mês. Você pode usar o painel Citrix DaaS Standard for Azure para cancelar uma assinatura mensal que você solicitou por meio da Citrix.

(Você não pode usar o painel do Citrix DaaS Standard for Azure para cancelar outros tipos de assinatura que você solicitou por meio da Citrix ou pedidos feitos por meio do Azure Marketplace.)

Para cancelar uma assinatura mensal:

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
3. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Geral** à direita.
4. Clique em **Cancelar assinatura**.
5. Seus recursos ativos são listados, como catálogos, imagens e conexões. A página descreve as ações que a Citrix toma durante um cancelamento. Ele também informa sobre as ações que você deve tomar, se houver. Indique por que você está cancelando o serviço. Opcionalmente, forneça mais feedback. Quando terminar, clique em **Cancelar assinatura**.
6. Confirme que você entende os termos do cancelamento.

Um banner no painel do Citrix DaaS Standard for Azure indica o recebimento da sua solicitação de cancelamento.

Se você cancelar sua assinatura acidentalmente, entre em contato com seu representante de vendas Citrix ou parceiro Citrix antes do final do mês para reativar o Citrix DaaS Standard for Azure.

Pedido pelo Azure Marketplace

Peça o Citrix DaaS Standard for Azure primeiro e, em seguida, solicite o Citrix Azure Consumption Fund.

Você não pode solicitar o fundo de consumo, a menos que tenha comprado anteriormente o Citrix DaaS Standard for Azure. Você não pode combinar o Citrix DaaS Standard for Azure e o fundo de consumo em um único pedido.

O Citrix DaaS Standard para Azure não é oferecido por meio do portal Azure Cloud Solutions Providers. Se você for um cliente de suporte prioritário ou estiver interessado em suporte prioritário, entre em contato com seu representante de conta Citrix.

Requisitos:

- O OrgID da sua conta do Citrix Cloud.
  - Se você tem uma conta do Citrix Cloud, mas não conhece o OrgID, procure no canto superior direito do console do Citrix Cloud. Ou veja o e-mail que você recebeu quando criou a conta.
  - Se você não tiver uma conta do Citrix Cloud, siga as orientações em Obter uma conta do Citrix Cloud.
- Uma conta do Azure e pelo menos uma assinatura do Azure na conta.

Encomende o Citrix DaaS Standard for Azure por meio do Azure Marketplace

1. Faça login no Azure Marketplace usando suas credenciais de conta do Azure.
2. Pesquise e navegue até o **Citrix DaaS Standard for Azure**.
3. Clique em **OBTENHA AGORA**.
4. Na mensagem **Mais uma coisa**, ative a caixa de seleção e clique em **Continuar**.
5. As guias contêm informações sobre o produto, planos, preços e uso. Quando estiver pronto, selecione um plano (se houver mais de um disponível) e clique em **Configurar + assinar**.
6. Na guia **Basics**:
   - **Assinatura**: indica o plano que você selecionou.
   - **Nome**: Insira um nome para o pedido de assinatura.
   - A seção **Plano** mostra o preço do plano selecionado, com base em termos mensais e plurianuais (anuais).

     Para alterar o prazo do plano (mensal ou anual), selecione **Alterar plano**. Selecione o termo desejado e clique em **Alterar plano**.

7. Na guia **Assinar Revisar +** :
    - Revise os detalhes de contato que você forneceu anteriormente para o perfil básico do Azure. Você pode alterar seu endereço, número de telefone ou ambos.
    - Clique em **Assinar**.
8. Na página **Assinatura em andamento**, clique em **Configurar conta agora**. (Se o botão estiver desativado, aguarde um momento.) Você é direcionado para uma página de ativação da Citrix.
9. Na página de ativação:
    - Use o link **Sign in** para fazer login no Citrix Cloud. Um login bem-sucedido preenche automaticamente o campo **ID da organização**.
    - **Quantity:** informe o número de usuários. (Um pedido inicial deve ter pelo menos 25.) Um preço estimado é exibido.
    - Concorde com os termos e condições e clique em **Ativar pedido**.

A Citrix envia um e-mail quando o serviço é provisionado. O provisionamento pode demorar um pouco. Se você não receber o e-mail até o dia seguinte, entre em contato com o Suporte Citrix.

Ao receber o e-mail da Citrix, você pode começar a usar o Citrix DaaS Standard for Azure. Lembre-se: com apenas o Citrix DaaS Standard for Azure, você pode usar apenas suas próprias assinaturas do Azure.

Não exclua o recurso Citrix DaaS Standard for Azure no Azure. A exclusão desse recurso cancela a sua assinatura.

Solicite o fundo de consumo por meio do Azure Marketplace

1. Faça login no Azure Marketplace usando suas credenciais de conta do Azure.
2. Pesquise e navegue até o **Citrix Azure Consumption Fund**.
3. Clique em **OBTENHA AGORA**.
4. Clique em **Configurar + assinar**.
5. Na página **Assinar** :
    - Em **Nome**, insira um nome facilmente reconhecível, como “Minhas áreas de trabalho gerenciadas”. Você pode usar esse nome mais tarde, se quiser alterar a assinatura do serviço.
    - Indique quantos usuários você deseja oferecer suporte, no intervalo de 25 a 100.000.
    - Digite seu endereço de e-mail e número de telefone.

    Quando terminar, clique em **Inscrever-se**.

6. Na página **Progresso da assinatura**, quando o botão **Configurar conta SaaS no site do editor** ficar ativo (azul), clique nele. Você é direcionado automaticamente para uma página de ativação de pedidos da Citrix.
7. Na página de ativação de pedidos da Citrix, insira seu Citrix Cloud OrgID. O endereço de e-mail que você inseriu anteriormente é mostrado. Você pode alterá-lo, se necessário. Quando terminar, clique em **Ativar pedido**.
8. O cumprimento da ordem do fundo de consumo não leva muito tempo. Quando a Citrix é notificada sobre o pedido, um banner aparece no console do Citrix DaaS for Azure, indicando que uma assinatura do Citrix Managed Azure está sendo preparada para você.

   O painel **Assinaturas na nuvem** à direita do painel **Gerenciar > Implantação Rápida do Azure** indica quando essa assinatura está pronta para uso.

Aumentar ou diminuir as licenças de usuário por meio do Azure Marketplace

Se você precisar aumentar as licenças de usuário, crie um novo pedido do Azure Marketplace para o número adicional de licenças desejado.

Para reduzir o número de licenças que você tem, cancele o Citrix DaaS Standard for Azure no Azure Marketplace e, em seguida, faça um pedido para o número desejado de licenças.

Cancelar o Citrix DaaS Standard for Azure ou o fundo de consumo por meio do Azure Marketplace

Para cancelar o Citrix DaaS Standard for Azure ou o fundo de consumo por meio do Azure Marketplace:

1. Faça login no Azure Marketplace.
2. Pesquise **DaaS**.
3. Selecione **Novo > Exibir**.
4. Selecione o recurso que você deseja cancelar.
5. No menu de reticências do recurso, selecione **Excluir**.
6. Clique em **Sim** na caixa de confirmação para confirmar que você conhece a política de reembolso e deseja cancelar o recurso.

> **Importante:**
>
> Não cancele o Fundo de Consumo do Citrix Azure se você estiver usando recursos gerenciados pela Citrix, como catálogos ou imagens criadas na assinatura do Citrix Managed Azure.

Quando seu pedido for aprovado e processado

Depois que sua avaliação ou serviço for aprovado, vários blocos aparecerão na página inicial do Citrix Cloud:

- Citrix DaaS para Azure
- Citrix DaaS
- Gateway

O Citrix DaaS for Azure é o único serviço ativado para seu uso.

Para começar a usar o Citrix DaaS Standard for Azure, faça login no Citrix Cloud. Acesse o Citrix DaaS Standard for Azure usando um dos seguintes métodos:

- No bloco **DaaS Standard for Azure**, clique em **Gerenciar**.
- No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.

Para obter orientações de configuração, consulte Primeiros passos.

Atualize para o Citrix DaaS Standard for Azure

Se você atualmente assina o serviço Citrix Virtual Apps Essentials ou Citrix Virtual Desktops Essentials, atualize para o Citrix DaaS Standard for Azure concluindo as seguintes tarefas.

1. Crie uma nova Organizational ID (OrgID) para usar com o Citrix DaaS Standard for Azure em https://onboarding.cloud.com/. (Conforme descrito anteriormente neste artigo, você não pode usar o mesmo OrgID para assinar mais de uma edição do Citrix DaaS.)
2. Entre em contato com o Citrix Sales para comprar o Citrix DaaS Standard for Azure e o Citrix Azure Consumption Fund, usando o novo OrgID. (Você não precisa solicitar o fundo de consumo, mas sem ele, você não pode acessar todos os recursos do Citrix DaaS Standard for Azure.)
3. Faça login no Citrix Cloud. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
4. Adicione pelo menos uma de suas assinaturas do Azure ao Citrix DaaS Standard for Azure.
5. Importe uma ou mais imagens de suas assinaturas do Azure para o Citrix DaaS Standard for Azure.
6. Crie catálogosusando as imagens importadas de suas assinaturas do Azure.
7. Adicione usuários aos catálogos que você criou.
8. Se você quiser manter o mesmo URL do Workspace usado com o Citrix Virtual Apps Essentials ou o Citrix Virtual Desktops Essentials:

    a) Faça login no Citrix Cloud usando o OrgID que você usa com o serviço Essentials. Selecione **Configuração do espaço de trabalho** no menu superior esquerdo. Altere o URL do Workspace para algo diferente.

b) Faça login no Citrix Cloud usando o OrgID que você usa com o Citrix DaaS Standard for Azure. Selecione **Configuração do espaço de trabalho** no menu superior esquerdo. Altere o URL do Workspace para o que você usou anteriormente para o serviço Essentials.

9. Faça login no Azure e exclua todos os recursos que você usou com o serviço Essentials. Para obter orientação, consulte Cancelar o Virtual Apps Essentials. (O procedimento é equivalente para o Citrix Virtual Desktops Essentials.)
10. Interrompa o serviço Essentials excluindo seu recurso do Azure Marketplace no Azure.

Introdução

September 7, 2022

Este artigo resume as tarefas de configuração para a entrega de desktops e aplicativos usando o Citrix Daas Standard for Azure (antigo serviço Citrix Virtual Apps and Desktops Standard for Azure). Recomendamos que você revise cada procedimento antes de realmente fazê-lo, para saber o que esperar.

Para tarefas de configuração do Acesso ao PC remoto, consulte Acesso ao PC remoto.

> **Importante:**
>
> Para garantir que você obtenha informações importantes sobre o Citrix Cloud e os serviços Citrix que você assina, procure receber todas as notificações por e-mail. Por exemplo, a Citrix envia emails de notificação informativos mensais detalhando seu consumo (uso) do Azure.
>
> No canto superior direito do console do Citrix Cloud, expanda o menu à direita do nome do cliente e dos campos OrgID. Selecione **Configurações de conta**. Na guia **Meu perfil**, selecione todas as entradas na seção **Notificações por e-mail**.

Resumo da tarefa de configuração

As seções a seguir deste artigo orientam você nas tarefas de configuração:

1. Prepare-se para a configuração.
2. Configure uma implantação, seguindo as orientações em um dos seguintes:
   - Implantação rápida de prova de conceito
   - Implementação
3. Forneça o URL do espaço de trabalho para seus usuários.

Preparar

- Se você não estiver familiarizado com catálogos, imagens, conexões de rede ou assinaturas do Azure, analise os conceitos introdutórios e as informações de terminologia.
- Leia a visão geral de segurança para saber e entender pelo que você (o cliente) e a Citrix são responsáveis.
- Se você ainda não tiver uma conta do Citrix Cloud que possa ser usada para esse serviço, adquira uma e, em seguida, inscreva-se no serviço.
- Analise os requisitos do sistema.
- Revise as etapas de configuração: prova de conceito ou produção.

Configure uma implantação rápida de prova de conceito

Esse procedimento requer uma assinatura do Citrix Managed Azure.

1. Criar um catálogo usando a criação rápida.
2. Adicionar seus usuários ao Managed Azure AD.
3. Adicionar seus usuários ao catálogo.
4. Notificar seus usuários sobre a URL do espaço de trabalho.

Configurar uma implantação de produção

1. Se você estiver usando seu próprio Active Directory ou Azure Active Directory para autenticar usuários, conecte-se e defina esse método no Citrix Cloud.
2. Se você estiver usando máquinas ingressadas no domínio, verifique se você tem entradas de servidor DNS válidas.
3. Se você estiver usando sua própria assinatura do Azure (em vez de uma assinatura do Citrix Managed Azure), importe sua assinatura do Azure.
4. Crie ou importe uma imagem. Embora você possa usar uma das imagens preparadas pela Citrix no estado em que se encontram em um catálogo, elas se destinam principalmente a implantações de prova de conceito.
5. Se você estiver usando uma assinatura do Citrix Managed Azure e quiser que seus usuários possam acessar itens em sua rede (como servidores de arquivos), configure um emparelhamento VNet do Azure ou uma conexão Citrix SD-WAN.
6. Criar um catálogo usando a criação personalizada.
7. Se você estiver criando um catálogo de máquinas com várias sessões, adicionar aplicativos ao catálogo, se necessário.
8. Se você estiver usando o Citrix Managed Azure AD para autenticar seus usuários, adicionar usuários ao diretório.
9. Adicione usuários ao catálogo.

10. Notifique seus usuários sobre o URL do Workspace.

Depois de configurar a implantação, use o painel **Monitor** no Citrix DaaS for Azure para ver o uso da área de trabalho, as sessõese as máquinas.

Requisitos do sistema

Para todas as implantações:

- **Citrix Cloud:** Este serviço é entregue por meio do Citrix Cloud e requer uma conta do Citrix Cloud para concluir o processo de integração. Para obter detalhes, consulte Obter uma conta do Citrix Cloud.
- **Licenciamento do Windows:** verifique se você está devidamente licenciado para que os Serviços de Área de Trabalho Remota executem cargas de trabalho do Windows Server ou Licenciamento de Área de Trabalho Virtual do Azure para Windows 10.

Se você estiver usando uma assinatura do Citrix Managed Azure:

- **Assinaturas do Azure ao usar o emparelhamento de VNet do Azure (opcional):** Se você planeja acessar recursos (como AD e outros compartilhamentos de arquivos) em sua própria rede do Azure usando conexões de mesmo ponto do Azure VNet, você deve ter uma assinatura do Azure.
- **Associando VDAs ao Azure Active Directory (opcional):** Para associar VDAs a um domínio usando a Política de Grupo do Active Directory, você deve ser um administrador com permissão para executar essa ação no Active Directory. Para obter detalhes, consulte Responsabilidade do cliente.

Configurar conexões com sua rede local corporativa tem requisitos extras.

- Qualquer conexão (Azure VNet peering ou SD-WAN): Requisitos para todas as conexões.
- Conexões de peering do Azure VNet: requisitos e preparação de peering do VNet.
- Conexões SD-WAN: requisitos e preparação de conexão SD-WAN.

Se você quiser usar suas próprias imagens do Azure ao criar um catálogo, essas imagens devem atender a determinados requisitos antes de importá-las para o Citrix DaaS for Azure.

Informações adicionais:

- Requisitos de conectividade com a Internet: requisitos de sistema e conectividade.
- Limites de recursos em uma implantação de serviço: Limites.

Sistemas operacionais compatíveis

Ao usar uma assinatura do Citrix Managed Azure:

- Windows 7 (o VDA deve ser 7.15 LTSR com a atualização cumulativa mais recente)
- Windows 10 de sessão única
- Windows 10 multissessão
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (requer o mínimo de VDA 2106)
- Red Hat Enterprise Linux e Ubuntu

Ao usar uma assinatura do Azure gerenciada pelo cliente:

- Windows 7 (o VDA deve ser 7.15 LTSR com a atualização cumulativa mais recente)
- Windows 10 Enterprise de sessão única
- Área de trabalho virtual do Windows 10 Enterprise multissessão
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (requer o mínimo de VDA 2106)
- Red Hat Enterprise Linux e Ubuntu

URL do espaço de trabalho

Depois de criar catálogos e atribuir usuários, notifique os usuários sobre onde encontrar suas áreas de trabalho e aplicativos: a URL do espaço de trabalho. A URL do espaço de trabalho é a mesma para todos os catálogos e usuários.

No painel **Gerenciar > Implantação Rápida do Azure**, visualize a URL expandindo **Acesso e Autenticação do Usuário** à direita.

Você pode alterar a primeira parte do URL do Workspace no Citrix Cloud. Para obter instruções, consulte Personalizar o URL do espaço de trabalho.

Obter ajuda

Leia o artigo Solução de problemas.

Se você ainda tiver problemas com o serviço, abra um ticket seguindo as instruções em Como obter ajuda e suporte.

Criar catálogos

October 7, 2022

Quando usado para áreas de trabalho e aplicativos publicados, um catálogo é um grupo de máquinas virtuais idênticas. Quando você implanta áreas de trabalho, as máquinas no catálogo são compartilhadas com os usuários selecionados. Quando você publica aplicativos, máquinas com várias sessões hospedam aplicativos que são compartilhados com usuários selecionados.

> **Nota:**
>
> Para obter informações sobre a criação de catálogos de Acesso ao PC remoto, consulte Acesso ao PC remoto.

Tipos de máquinas

Um catálogo pode conter um dos seguintes tipos de máquinas:

- **Estático:** O catálogo contém máquinas estáticas de sessão única (também conhecidas como áreas de trabalho pessoais, dedicadas ou persistentes). Static significa que, quando um usuário inicia uma área de trabalho, essa área de trabalho "pertence"a esse usuário. Todas as alterações feitas pelo usuário na área de trabalho são mantidas no logoff. Mais tarde, quando esse usuário retornar ao Citrix Workspace e iniciar uma área de trabalho, ela será a mesma área de trabalho.
- **Random:** o catálogo contém máquinas aleatórias de sessão única (também conhecidas como desktops não persistentes). Aleatório significa que quando um usuário inicia uma área de trabalho, todas as alterações feitas por ele nessa área de trabalho são descartadas após o logoff. Mais tarde, quando esse usuário retornar ao Citrix Workspace e iniciar uma área de trabalho, ela pode ou não ser a mesma área de trabalho.
- **Multi-session:** o catálogo contém máquinas com aplicativos e desktops. Mais de um usuário pode acessar cada uma dessas máquinas simultaneamente. Os usuários podem iniciar uma área de trabalho ou aplicativos em seu espaço de trabalho. As sessões do aplicativo podem ser compartilhadas. O compartilhamento de sessão não é permitido entre um aplicativo e um desktop.
  - Ao criar um catálogo de várias sessões, você seleciona a carga de trabalho: leve (como entrada de dados), média (como aplicativos de escritório), pesada (como engenharia) ou personalizada. Cada opção representa um número específico de máquinas e sessões por máquina, o que gera o número total de sessões que o catálogo suporta.
  - Se você selecionar a carga de trabalho personalizada, selecione entre as combinações disponíveis de CPUs, RAM e armazenamento. Digite o número de máquinas e sessões por máquina, o que gera o número total de sessões que o catálogo suporta.

Ao implantar áreas de trabalho, os tipos de máquina estática e aleatória às vezes são chamados de "tipos de desktop".

Formas de criar um catálogo

Existem várias maneiras de criar e configurar um catálogo:

- A **criação rápida** é a maneira mais rápida de começar. Você fornece informações mínimas e o Citrix DaaS for Azure cuida do resto. Um catálogo de criação rápida é ótimo para um ambiente de teste ou prova de conceito.
- A **criação personalizada** permite mais opções de configuração do que a criação rápida. É mais adequada para um ambiente de produção do que um catálogo de criação rápida.
- Os catálogos **Remote PC Access** contêm máquinas existentes (geralmente físicas) que os usuários acessam remotamente. Para obter detalhes e instruções sobre esses catálogos, consulte Acesso ao PC remoto.

Aqui está uma comparação entre criação rápida e criação personalizada:

Criação rápida	Criação personalizada
Menos informações para fornecer.	Mais informações para fornecer.
Menos opções para alguns recursos.	Mais opções para alguns recursos.
Autenticação de usuário do Azure Active Directory gerenciada pela Citrix.	Opções: Azure Active Directory gerenciado pela Citrix ou seu Active Directory/Azure Active Directory.
Sem conexão com sua rede local.	Opções: Sem conexão com sua rede local, emparelhamento de VNet do Azure e SD-WAN.
Usa uma imagem do Windows 10 preparada pela Citrix. Essa imagem contém um VDA de desktop atual.	Escolha de: imagens preparadas pela Citrix, suas imagens que você importa do Azure ou imagens que você criou no Citrix DaaS for Azure a partir de uma imagem preparada ou importada da Citrix.
Cada área de trabalho tem armazenamento em disco padrão (HDD) do Azure.	Várias opções de armazenamento estão disponíveis.
Somente desktops estáticos.	Desktops estáticos, aleatórios ou com várias sessões.

Criação rápida	Criação personalizada
Um cronograma de gerenciamento de energia não pode ser configurado durante a criação. A máquina que hospeda a área de trabalho é desligada quando a sessão termina. (Você pode alterar essa configuração mais tarde.)	Um cronograma de gerenciamento de energia pode ser configurado durante a criação.
É necessário usar uma assinatura do Citrix Managed Azure.	Pode usar o Citrix Managed Azure ou sua própria assinatura do Azure.

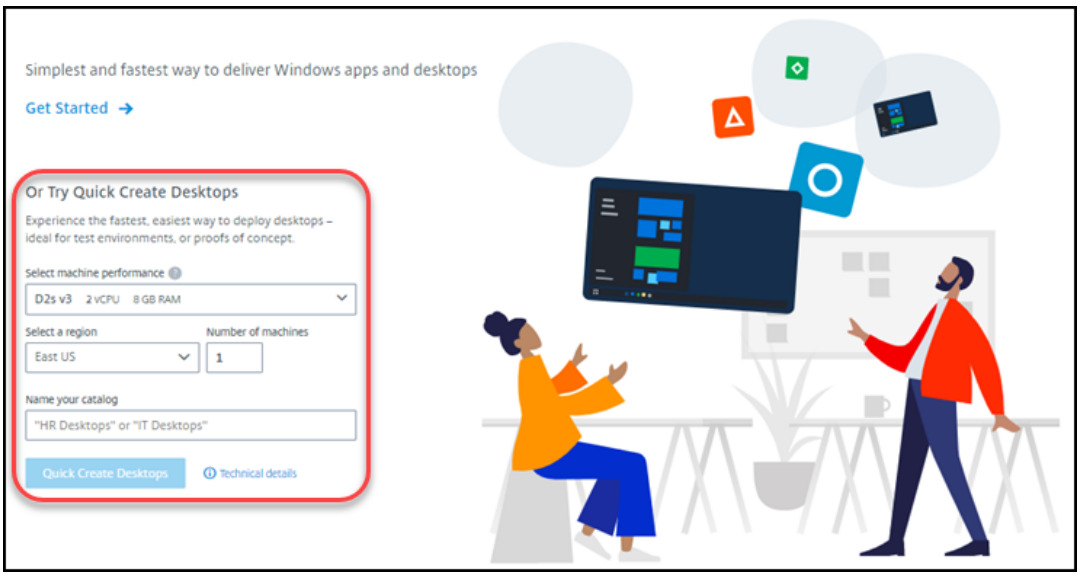
Para obter detalhes, consulte:

- Crie um catálogo usando a criação rápida
- Crie um catálogo usando a criação personalizada

Crie um catálogo usando a criação rápida

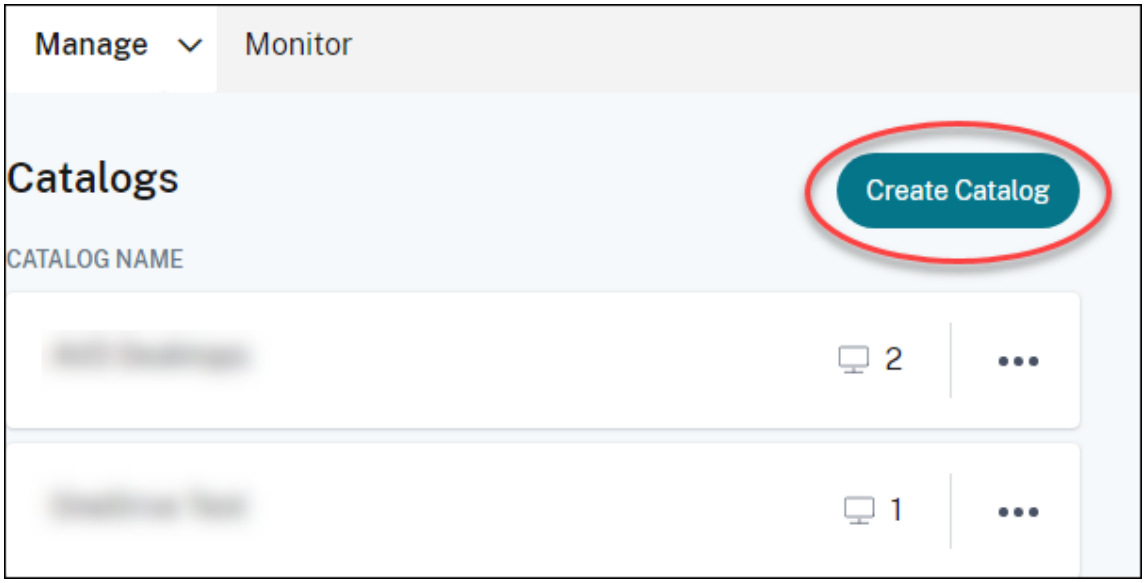
Esse método de criação de catálogo sempre usa uma assinatura do Citrix Managed Azure.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
3. Se um catálogo ainda não tiver sido criado, você será direcionado para a página de **boas-vindas** de implantação rápida. Escolha um dos seguintes:
   - Configure o catálogo nesta página. Continue com as etapas 6 a 10.

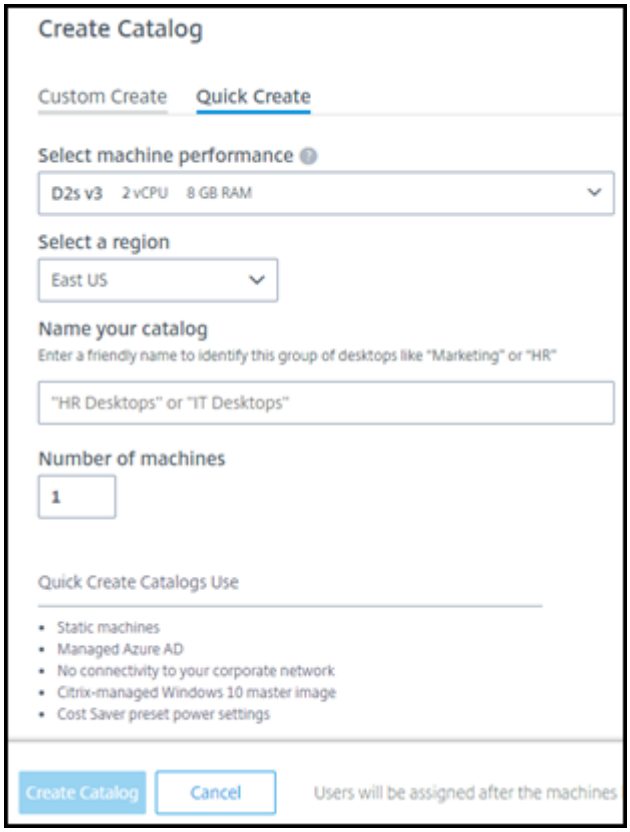


- Clique em **Começar**. Você é levado ao painel **Gerenciar > Implantação Rápida do Azure** . Clique em **Create Catalog**.

4. Se um catálogo já tiver sido criado (e você estiver criando outro), você será levado ao painel **Gerenciar > Implantação Rápida do Azure** . Clique em **Create Catalog**.



5. Clique em **Criação rápida** na parte superior da página, se ela ainda não estiver selecionada.



- **Machine performance:** Selecione o tipo de máquina. Cada opção tem uma combinação exclusiva de CPUs, RAM e armazenamento. Máquinas de alto desempenho têm custos mensais mais altos.
- **Region:** Selecione uma região onde você deseja que as máquinas sejam criadas. Você pode selecionar uma região próxima aos seus usuários.
- **Name:** digite um nome para o catálogo. Esse campo é obrigatório e não há valor padrão.
- **Número de máquinas:** Digite o número de máquinas que você deseja.

6. Quando terminar, clique em **Criar catálogo**. (Se você estiver criando o primeiro catálogo na página de **boas-vindas** de implantação rápida, clique em **Criação rápida de áreas de trabalho**.)

Você é levado automaticamente para o painel **Gerenciar > Implantação Rápida do Azure** . Enquanto o catálogo está sendo criado, o nome do catálogo é adicionado à lista de catálogos, indicando seu progresso na criação.

O Citrix DaaS for Azure também cria automaticamente um local de recurso e adiciona dois Cloud Connectors.

O que fazer a seguir:

- Se você estiver usando o Citrix Managed Azure AD para autenticação de usuário, poderá adicionar usuários ao diretório enquanto o catálogo está sendo criado.
- Independentemente do método de autenticação de usuário usado, depois que o catálogo for criado, adicione usuários ao catálogo.

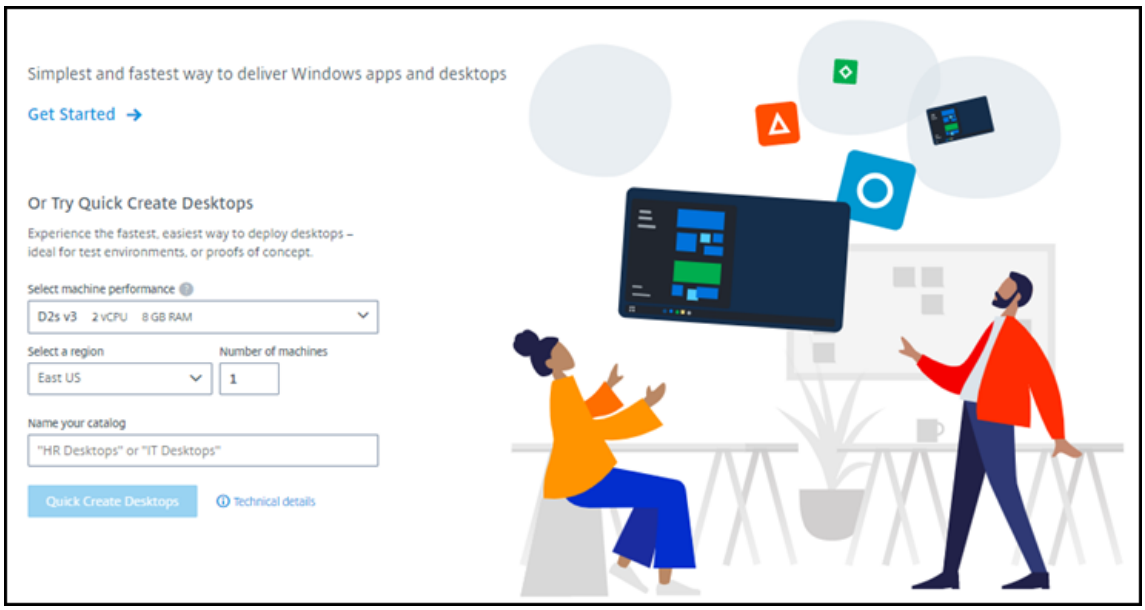
Crie um catálogo usando a criação personalizada

Se você estiver usando uma assinatura do Citrix Managed Azure e planeja usar uma conexão com seus recursos de rede locais, crie essa conexão de rede antes de criar o catálogo. Para permitir que seus usuários acessem seus recursos locais ou outros recursos de rede, você também precisa de informações do Active Directory para esse local.

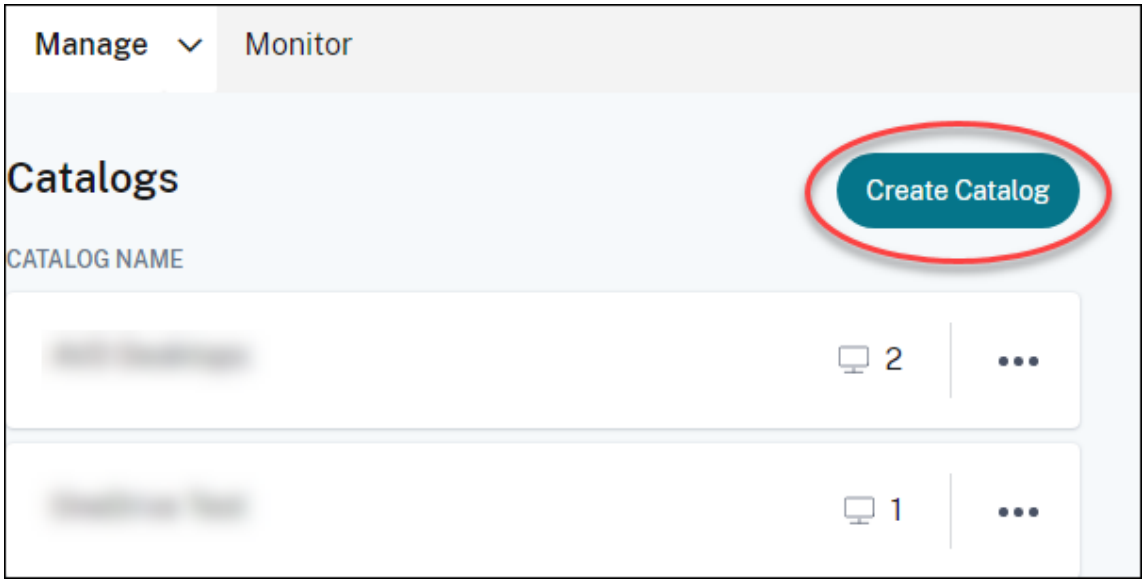
Se você não tiver uma assinatura do Citrix Managed Azure, deverá importar (adicionar) pelo menos uma de suas próprias assinaturas do Azure para o Citrix DaaS for Azure antes de criar um catálogo.

Para criar um catálogo:

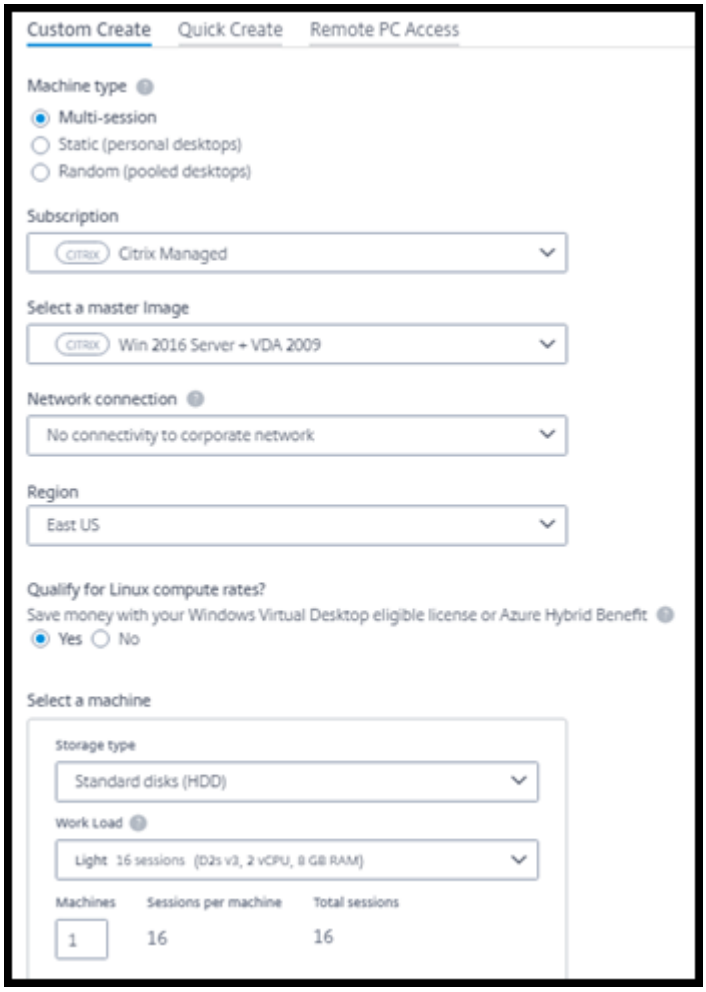
1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
3. Se um catálogo ainda não tiver sido criado, você será direcionado para a página de **boas-vindas** de implantação rápida. Clique em **Começar**. No final da página de introdução, você é direcionado para o painel **Gerenciar > Azure Quick Deploy** . Clique em **Create Catalog**.



Se um catálogo já tiver sido criado, você será levado ao painel **Gerenciar > Implantação Rápida do Azure** . Clique em **Create Catalog**.



4. Selecione **Criar personalizado** na parte superior da página, se ainda não estiver selecionado.



5. Preencha os campos a seguir. (Alguns campos são válidos somente para determinados tipos de máquinas. A ordem dos campos pode ser diferente.)

   - **Machine type**. Selecione um tipo de máquina. Para obter detalhes, consulte Tipos de máquina.
   - **Subscription**. Selecione uma assinatura do Azure. Para obter detalhes, consulte Assinaturas do Azure.
   - **Imagem mestre:** Selecione uma imagem do sistema operacional. Para obter detalhes, consulte Imagens.
   - **Conexão de rede:** selecione a conexão a ser usada para acessar recursos em sua rede. Para obter detalhes, consulte Conexões de rede.
     - Para uma assinatura do Citrix Managed Azure, as opções são:
       - **Sem conectividade:** os usuários não podem acessar locais e recursos em sua rede corporativa local.

    * *Conexões:* Selecione uma conexão, como emparelhamento VNet ou conexão SD-WAN.

  - Para uma assinatura do Azure gerenciada pelo cliente, selecione o grupo de recursos, a rede virtual e a sub-rede apropriados.

- **Região:** (Disponível somente se você tiver selecionado **Sem Conectividade** na **Conexão de Rede**.) Selecione uma região na qual deseja que as áreas de trabalho sejam criadas. Você pode selecionar uma região próxima aos seus usuários.

  Se você selecionou um nome de conexão em **Conexão de rede**, o catálogo usará a região dessa rede.

- **Qualificar-se para as taxas de computação do Linux?** (Disponível somente se você selecionou uma imagem do Windows.) Você pode economizar dinheiro ao usar sua licença qualificada ou o Azure Hybrid Benefit.

  Benefício Azure Virtual Desktop: licenças qualificadas do Windows 10 ou Windows 7 por usuário para:

  - Microsoft 365 E3/ES
  - Benefícios de uso do Microsoft 365 A3/AS/Student
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Enterprise E3/E5
  - Windows 10 Education A3/A5
  - Windows 10 VDA por usuário

  Licença por usuário ou por dispositivo da RDS CAL com Software Assurance para cargas de trabalho do Windows Server.

  Azure Hybrid benefit: licenças do Windows Server com o Software Assurance ativo ou as licenças de assinatura qualificadas equivalentes. Veja https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine:**

  - **Tipo de armazenamento**. Disco padrão (HDD), SSD padrão ou SSD premium.

  - **Desempenho da máquina** (para o tipo de máquina **estática** ou **aleatória**) ou **Carga de trabalho** (para o tipo de máquina com várias sessões). As opções incluem somente opções que correspondem ao tipo de geração (gen1 ou gen2) da imagem selecionada.

    Se você selecionar a carga de trabalho personalizada, digite o número de máquinas e sessões por máquina no campo **Machine Performance**.

  - **Machines**. Quantas máquinas você deseja neste catálogo.

- **Esquema de nomeação de máquina:** consulte Esquema de nomeação de máquina.

- **Nome:** Digite um nome para o catálogo. Esse nome aparece no painel **Manage**.
- **Programação de energia:** Por padrão, a caixa de seleção **I'll configure this later** está marcada. Para obter detalhes, consulte Programações de gerenciamento de energia.

6. Quando terminar, clique em **Criar catálogo**.

O painel **Gerenciar > Implantação Rápida do Azure** indica quando seu catálogo é criado. O Citrix DaaS for Azure também cria automaticamente um local de recurso e adiciona dois Cloud Connectors.

O que fazer a seguir:

- Se você ainda não fez isso, configure o método de autenticação para que seus usuários se autentiquem no Citrix Workspace.
- Depois que o catálogo for criado, adicione usuários ao catálogo.
- Se você criou um catálogo de várias sessões, adicione aplicativos (antes ou depois de adicionar usuários).

Criação de catálogos de máquinas associadas ao domínio do Azure AD

Você pode usar a criação personalizada para criar catálogos de máquinas associadas ao seu Azure Active Directory.

Requisitos

Sua implantação deve incluir conectores do Citrix Cloud. O Machine Creation Services implanta seus conectores de nuvem com base nas informações que você fornece sobre seu domínio do Azure AD ao criar um catálogo.

Esse tipo de catálogo só pode ser usado para provisionar máquinas estáticas ou aleatórias. O provisionamento de máquinas com várias sessões não é suportado no momento.

Não junte a imagem mestre ao Azure AD antes de criar um catálogo. O Citrix MCS une a imagem mestre ao Azure AD quando o catálogo é criado.

Use o VDA versão 2203 ou superior.

No portal do Azure, atribua a função IAM de Login de Usuário da Máquina Virtual às máquinas virtuais no catálogo. Você pode fazer isso de várias maneiras:

- Mais seguro: se você estiver criando máquinas estáticas, atribua a função à atribuição do usuário à máquina.
- Método alternativo: atribua a função nos grupos de recursos que contêm as máquinas virtuais a todos os usuários com acesso ao catálogo.

- Menos seguro: atribua a função nas assinaturas a todos os usuários com acesso ao catálogo.

Defina a autenticação do Workspace para usar o Azure AD ao qual você está ingressando nas máquinas no catálogo. Para obter instruções, consulte Configurar a autenticação do usuário no Citrix Cloud.

Para obter mais informações sobre requisitos, problemas conhecidos e considerações, consulte as informações sobre configurações puras de VDA ingressadas no Azure AD na configuração de VDA ingressada e não associada ao domínio do Azure Active Directory.

Para criar um catálogo

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
3. Selecione **Gerenciar > Implantação rápida do Azure**.
4. Se um catálogo ainda não tiver sido criado, você será direcionado para a página de **boas-vindas** . Selecione **Get Started**. No final da página de introdução, você será levado ao painel **Gerenciar > Implantação Rápida do Azure** . Selecione **Create Catalog**. Se um catálogo já tiver sido criado, você será levado ao painel **Gerenciar > Implantação Rápida do Azure** . Selecione **Create Catalog**.
5. Selecione **Criar personalizado** na parte superior da página, se ainda não estiver selecionado.
6. Preencha os campos a seguir.
   - **Tipo de máquina.** Selecione **Estático (desktops pessoais)** ou **Aleatório (áreas de trabalho agrupadas)**.
   - **Assinatura**. Selecione sua assinatura do Azure.
   - **Imagem principal.** Selecione uma imagem do sistema operacional a ser usada para as máquinas nos catálogos.
   - **Conexão de rede.** Selecione o grupo de recursos, a rede virtual e a sub-rede apropriados.
   - **Configuração do domínio**. Selecione **Azure Active Directory** como seu tipo de domínio. Um aviso pode aparecer lembrando você de definir a autenticação do Workspace para usar este Azure AD.
7. Conclua o restante do assistente para criar o catálogo.

Configurações de localização de recursos ao criar um catálogo

Ao criar um catálogo, você pode, opcionalmente, definir várias configurações de localização de recursos.

Quando você clica em **Configurações avançadas** na caixa de diálogo de criação do catálogo Quick Deploy, o Citrix DaaS for Azure recupera informações de localização do recurso.

- Se você já tiver um local de recurso para o domínio e a conexão de rede selecionados para o catálogo, poderá salvá-lo para uso pelo catálogo que você está criando.

  Se esse local de recurso tiver apenas um Cloud Connector, outro será instalado automaticamente. Opcionalmente, você pode especificar configurações avançadas para o Cloud Connector que está adicionando.

- Se você não tiver um local de recurso configurado para o domínio e a conexão de rede selecionados para o catálogo, será solicitado que você configure um.

Defina as configurações avançadas:

- (Obrigatório somente quando o local do recurso já está configurado.) Um nome para o local do recurso.
- Tipo de conectividade externa: por meio do serviço Citrix Gateway ou de dentro de sua rede corporativa.
- Configurações do Cloud Connector:
  - (Disponível somente ao usar uma assinatura do Azure gerenciada pelo cliente) Machine performance. Essa seleção é usada para os Cloud Connectors no local do recurso.
  - (Disponível somente ao usar uma assinatura do Azure gerenciada pelo cliente) Azure resource group. Essa seleção é usada para os Cloud Connectors no local do recurso. O padrão é o último grupo de recursos usado pelo local do recurso (se aplicável).
  - Organizational Unit (OU). O padrão é a UO usada pela última vez pelo local do recurso (se aplicável).

Ao concluir as configurações avançadas, clique em **Salvar** para retornar à caixa de diálogo de criação de catálogo de Implantação rápida.

Depois de criar um catálogo, várias ações de localização de recursos estarão disponíveis. Para obter detalhes, consulte Resource location actions.

Esquema de nomeação de máquinas

Para especificar um esquema de nomeação de máquina ao criar um catálogo usando a Implantação Rápida, selecione **Especificar esquema de nomeação de máquina**. Use de 1 a 4 caracteres curinga (marcas de hash) para indicar onde números ou letras sequenciais aparecem no nome. Regras:

- O esquema de nomenclatura deve conter pelo menos um curinga, mas não mais do que quatro curingas. Todos os curingas devem estar juntos.
- O nome inteiro, incluindo curingas, deve ter entre 2 e 15 caracteres.
- Um nome não pode incluir espaços em branco (espaços), barras, barras invertidas, dois-pontos, asteriscos, colchetes angulares, barras verticais, vírgulas, sinais de til, pontos de exclamação,

símbolos de arroba, cifrões, sinais de porcentagem, sinais de circunflexo, parênteses, chaves ou sublinhados.
- Um nome não pode começar com um ponto final.
- Um nome não pode conter somente números.
- Não use as seguintes letras no final de um nome: `-GATEWAY`, `-GW` e `-TAC`.

Indique se os valores sequenciais são números (0-9) ou letras (A-Z):

Por exemplo, um esquema de nomenclatura de `PC-Sales-##` (com **0-9** selecionado) resulta em contas de computador nomeadas `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03` e assim por diante.

Deixe espaço suficiente para a expansão.

- Por exemplo, um esquema de nomeação com 2 curingas e 13 outros caracteres (por exemplo, `MachineSales-##`) usa o número máximo de caracteres (15).
- Quando o catálogo contiver 99 máquinas, a próxima criação da máquina falhará. O serviço tenta criar uma máquina com três dígitos (100), mas isso criaria um nome com 16 caracteres. O máximo é 15.
- Então, neste exemplo, um nome mais curto (por exemplo, `PC-Sales-##`) permite escalar além de 99 máquinas.

Se você não especificar um esquema de nomenclatura de máquina, o Citrix DaaS for Azure usará o esquema de nomenclatura padrão `DAS%%%%%-**-###`.

- `%%%%%` = cinco caracteres alfanuméricos aleatórios correspondentes ao prefixo de localização do recurso
- `**` = dois caracteres alfanuméricos aleatórios para o catálogo
- `###` = três dígitos.

Informações correlatas

- Máquinas unidas ao domínio e não unidas ao domínio.
- Catálogos de Acesso ao PC remoto.
- Crie um catálogo em uma rede que usa um servidor proxy.
- Exibir informações do catálogo.

Remote PC Access

September 7, 2022

Introdução

> **Nota:**
>
> Este artigo descreve como configurar o Acesso Remoto ao PC ao usar a interface de gerenciamento Quick Deploy no Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure service). Para obter informações sobre como configurar o Acesso ao PC remoto ao usar a interface de gerenciamento Configuração completa, consulte Acesso ao PC remoto.

O Acesso ao PC remoto da Citrix permite que os usuários usem remotamente máquinas físicas Windows ou Linux localizadas no escritório. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

O Acesso ao PC remoto é compatível com máquinas ingressadas no domínio.

Diferenças em relação ao fornecimento de desktops e aplicativos virtuais

Se você estiver familiarizado com o fornecimento de áreas de trabalho e aplicativos virtuais, o recurso Remote PC Access tem várias diferenças:

- Um catálogo de acesso ao PC remoto geralmente contém máquinas físicas existentes. Portanto, você não precisa preparar uma imagem ou provisionar máquinas para usar o Remote PC Access. A entrega de áreas de trabalho e aplicativos geralmente usa máquinas virtuais (VMs), e uma imagem é usada como modelo para provisionar as VMs.
- Quando uma máquina em um catálogo aleatório de acesso ao PC remoto é desligada, ela não é redefinida para o estado original da imagem.
- Para catálogos estáticos de atribuição de usuário do Remote PC Access, a atribuição ocorre depois que um usuário faz login (na máquina ou via RDP). Ao fornecer áreas de trabalho e aplicativos, um usuário é atribuído se uma máquina estiver disponível.

Resumo da instalação e configuração

Leia esta seção antes de iniciar as tarefas.

1. Antes de começar:
   a) Leia os Requisitos e considerações.
   b) Conclua as tarefas de preparação.
2. Do Citrix Cloud:
   a) Configure uma conta do Citrix Cloud e assine o serviço Citrix DaaS Standard for Azure.

b) Configure um local de recurso que possa acessar os recursos do Active Directory. Instale pelo menos dois Cloud Connectors no local de recursos. Os Cloud Connectors se comunicam com o Citrix Cloud.

   Siga as orientações para criar um local de recursos e instalar Cloud Connectors nele. As informações incluem requisitos do sistema, preparação e procedimentos.

c) Conecte seu Active Directory ao Citrix Cloud.

3. Instale um Citrix Virtual Delivery Agent (VDA) em cada máquina que os usuários acessarão remotamente. Os VDAs se comunicam com o Citrix Cloud por meio dos Cloud Connectors no local do recurso.

4. Na interface de gerenciamento do Citrix DaaS for Azure Quick Deploy:

   a) Crie um catálogo de Acesso ao PC remoto. Nesse procedimento, você especifica a localização do seu local de recursos e seleciona o método de atribuição de usuário.
   b) Adicione assinantes (usuários) ao catálogo, se necessário. Adicione usuários a um catálogo se o catálogo usar o método de atribuição de usuário estático atribuído automaticamente ou aleatório de um pool. Você não precisa adicionar usuários a um catálogo estático pré-atribuído.

5. Envie o URL do espaço de trabalho para os usuários. No espaço de trabalho, os usuários podem fazer logon em suas máquinas no escritório.

Requisitos e considerações

As referências a máquinas nesta seção referem-se às máquinas que os usuários acessam remotamente.

Geral:

- As máquinas devem estar executando um sistema operacional Windows 10 ou Linux (Red Hat Enterprise Linux e Ubuntu) de sessão única.
- A máquina deve estar associada a um domínio dos Serviços de Domínio do Active Directory.
- Se você estiver familiarizado com o uso do Acesso Remoto ao PC com o Citrix Virtual Apps and Desktops, o recurso Wake-on-LAN não está disponível no Citrix DaaS para Azure.

Rede:

- A máquina 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:
  - Defina as configurações de energia para deixar o adaptador sem fio ligado.

  - 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. A máquina não fica disponível para acesso remoto até que um usuário faça logon.
  - Verifique se os Cloud Connectors podem ser acessados pela rede Wi-Fi.

Dispositivos e periféricos:

- Os seguintes dispositivos não são compatíveis:
  - 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 à máquina. 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.
- Para laptops e dispositivos Surface Pro: certifique-se de que o laptop está conectado a uma fonte de alimentação em vez de estar funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de uma máquina desktop. Por exemplo:
  - Desative o recurso de hibernação.
  - Desative o recurso de suspensão.
  - Defina a ação de fechar a tampa como **Não fazer nada**.
  - Defina a ação *pressionar o botão liga/desliga* para **Desligar**.
  - Desative os recursos de economia de energia da placa de vídeo e da NIC.

  Quando estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixar o laptop, o VDA se registra novamente com os Cloud Connectors via Wi-Fi. No entanto, quando você reencaixar o laptop, o VDA não muda para usar a conexão com fio até que você desconecte o adaptador sem fio. Alguns dispositivos fornecem funcionalidade interna para desconectar o adaptador de conexão sem fio ao estabelecer uma conexão com fio. 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.

  Para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

  - Em **Iniciar > Configurações > Sistema > Energia e suspensão**, defina **Suspender** como **Nunca**.
  - 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**. Certifique-se de que **Permitir que este dispositivo desperte o computador** esteja selecionado.

Linux VDA:

- Use o Linux VDA em máquinas físicas somente no modo não 3D. Devido a limitações no driver da NVIDIA, a tela local do PC não pode ser apagada e exibe atividades de sessão quando o modo HDX 3D está ativado. Mostrar essa tela é um risco de segurança.
- Catálogos com máquinas Linux devem usar o método de atribuição de usuário estático pré-atribuído. Os catálogos com máquinas Linux não podem usar os métodos de atribuição estática atribuída automaticamente ou aleatória.

Considerações sobre o espaço de trabalho:

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz login no Citrix Workspace, a máquina aparece como indisponível se já estiver em uso por outro usuário.

Preparar

- Decida como instalar o VDA nas máquinas. Há vários métodos disponíveis:
  - Manualmente, instale o VDA em cada máquina.
  - Envie a instalação do VDA usando a Política de grupo, usando um script.
  - Envie a instalação do VDA usando uma ferramenta de Distribuição Eletrônica de Software (ESD), como o Microsoft System Center Configuration Manager (SCCM). Para obter detalhes, consulte Instalar VDAs usando SCCM.
- Saiba mais sobre os métodos de atribuição de usuário e decida qual método você usará. Você especifica o método ao criar um catálogo do Remote PC Access.
- Decida como as máquinas (na verdade, os VDAs que você instala nas máquinas) serão registradas no Citrix Cloud. Um VDA deve se registrar para estabelecer comunicação com o agente de sessão no Citrix Cloud.

  Os VDAs se registram por meio dos Cloud Connectors em seus locais de recursos. Você pode especificar endereços de Cloud Connectors ao instalar um VDA ou posteriormente.

  Para o primeiro registro (inicial) de um VDA, a Citrix recomenda o uso de LGPO ou GPO baseado em políticas. Após o registro inicial, a Citrix recomenda o uso da atualização automática, que é ativada por padrão. Saiba mais sobre o registro do VDA.

Instale um VDA

Baixe e instale um VDA em cada máquina física que os usuários acessarão remotamente.

Download de um VDA

- Para baixar um Windows VDA:
  1. Usando suas credenciais de conta do Citrix Cloud, navegue até a página de download do Citrix DaaS.
  2. Baixe o VDA mais recente. Há dois tipos de pacotes de instalação disponíveis. Os valores de ano e mês no título do VDA variam.
- Para baixar um Linux VDA para acesso ao PC remoto, siga as orientações na documentação do Linux VDA.

Tipos de pacotes de instalação do Windows VDA O site de download da Citrix fornece dois tipos de pacotes de instalação do Windows VDA que podem ser usados para máquinas no Remote PC Access:

- Instalador de VDA básico de sessão única (a *versão* é *aamm*): `VDAWorkstationCoreSetup_release.exe`

  O instalador de VDA básico de sessão única é adaptado especificamente para o Remote PC Access. Ele é leve e mais fácil de implantar (do que outros instaladores de VDA) pela rede em todas as máquinas. Ele não inclui componentes que normalmente não são necessários nessas implantações, como o Citrix Profile Management, o Machine Identity Service e a camada de personalização do usuário.

  No entanto, sem o Citrix Profile Management instalado, os displays do Citrix Analytics for Performance e alguns detalhes do Monitor não estarão disponíveis. Para obter detalhes sobre essas limitações, consulte a publicação do blog Monitorar e solucionar problemas em máquinas no Remote PC Access.

  Se você quiser exibições completas de análise e monitoramento, use o instalador de VDA completo de sessão única.

- Instalador de VDA completo de sessão única (a *versão* é *aamm*): `VDAWorkstationSetup_release.exe`

  Embora o instalador de VDA completo de sessão única seja um pacote maior do que o instalador de VDA básico de sessão única, você pode adaptá-lo para instalar apenas os componentes necessários. Por exemplo, você pode instalar os componentes que oferecem suporte ao Profile Management.

Instalar um Windows VDA para acesso ao PC remoto de forma interativa

1. Clique duas vezes no arquivo de instalação do VDA que você baixou.

2. Na página **Environment**, selecione **Enable Remote PC Access** e clique em **Next**.
3. Na página **Delivery Controller**, selecione uma das seguintes opções:
   - Se você souber o endereço dos seus Cloud Connectors, selecione **Do it manually**. Insira o FQDN de um Cloud Connector e clique em **Add**. Repita o procedimento para os outros Cloud Connectors no seu local de recursos.
   - Se você souber onde instalou os Cloud Connectors na sua estrutura do AD, selecione **Choose locations from Active Directory** e navegue até o local. Repita o procedimento para os outros Cloud Connectors.
   - Se você quiser especificar o endereço dos Cloud Connectors na Política de Grupo Citrix, selecione **Do it later (Advanced)** e confirme a seleção quando solicitado.

   Quando terminar, clique em **Next**.
4. Se você estiver usando o instalador VDA completo de sessão única, na página **Additional Components**, selecione os componentes que deseja instalar, como o Profile Management. (Essa página não aparece se você estiver usando o instalador de VDA básico de sessão única.)
5. Na página **Features**, clique em **Next**.
6. Na página **Firewall**, selecione **Automatically** (se ainda não estiver). Clique em **Next**.
7. Na página **Summary**, clique em **Install**.
8. Na página **Diagnosticar**, clique em **Conectar**. Verifique se a caixa de seleção está marcada. Quando solicitado, insira as credenciais da sua conta da Citrix. Depois que suas credenciais forem validadas, clique em **Next**.
9. Na página **Finish**, clique em **Finish**.

Para obter informações completas sobre a instalação, consulte Instalar VDAs.

Instalar um Windows VDA para acesso ao PC remoto usando uma linha de comando

- Se você estiver usando o instalador de VDA básico de sessão única: execute `VDAWorkstationCoreSetup.exe` e inclua as opções `/quiet`, `/enable_hdx_ports` e `/enable_hdx_udp_ports`. Para especificar endereços do Cloud Connector, use a opção `/controllers`.

  Por exemplo, o comando a seguir instala um VDA básico de sessão única. O aplicativo Citrix Workspace e outros serviços não principais não são instalados. O FQDN dos dois Cloud Connectors é especificado e as portas no Serviço do Firewall do Windows serão abertas automaticamente. O administrador lidará com as reinicializações.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```


- Se você estiver usando o instalador VDA completo de sessão única e quiser incluir o Profile Management (ou outros componentes opcionais): Execute `VDAWorkstationSetup.exe` e inclua `/remotepc` `/includeadditional` as opções e. A `/remotepc` opção impede a instalação da maioria dos componentes opcionais. A `/includeadditional` opção especifica exatamente quais componentes você deseja instalar.

  Por exemplo, o comando a seguir impede a instalação de todos os componentes adicionais opcionais, exceto o Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "
  Citrix User Profile Manager","Citrix User Profile Manager WMI
  Plugin" /controllers "connector.domain.com" "connector2.domain.com
  " /enable_hdx_ports /noresume /noreboot
  ```

Para obter detalhes, consulte Opções de linha de comando para instalar um VDA.

Instalar um Linux VDA

Siga as orientações na documentação do Linux para instalar um Linux VDA interativamente ou usando a linha de comando.

Criar um catálogo de acesso ao PC remoto

Um local de recursos contendo pelo menos dois Cloud Connectors deve existir antes que você possa criar um catálogo com êxito.

> **Importante:**
>
> Uma máquina só pode pertencer a um catálogo por vez. Essa restrição não é imposta quando você especifica as máquinas a serem adicionadas a um catálogo. No entanto, ignorar a restrição pode causar problemas posteriormente.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
3. Se você ainda não criou nenhum catálogo, clique em **Primeiros passos** na página de **boas-vindas** de implantação rápida. Se você criou um catálogo, clique em **Criar catálogo** no painel **Gerenciar > Implantação Rápida do Azure** .
4. Na guia **Remote PC Access**, selecione um método para atribuir usuários às máquinas.
5. Insira um nome para o catálogo e selecione o local de recursos que você criou.
6. Adicione máquinas.

7. Clique em **Create Catalog**.
8. Na página **Seu catálogo de Acesso ao PC remoto está sendo criado**, clique em **Concluído**.
9. Uma entrada para o novo catálogo aparece no painel **Gerenciar**.

   Depois que o catálogo for criado com êxito, clique em um dos links para adicionar assinantes (usuários) ao catálogo. Esta etapa se aplica se o catálogo usar o método de atribuição de usuário estático autoatribuído ou aleatório de um pool não atribuído.

Depois de criar um catálogo e adicionar usuários (se necessário), envie a URL do espaço de trabalho para os seus usuários.

Métodos de atribuição do usuário

O método de atribuição do usuário escolhido ao criar um catálogo indica como os usuários são atribuídos às máquinas.

- **Atribuição automática estática:** a atribuição do usuário ocorre quando um usuário faz logon na máquina (sem usar o Citrix, por exemplo, pessoalmente ou por RDP), depois que um VDA é instalado na máquina. Posteriormente, se outros usuários fizerem logon nessa máquina (sem usar o Citrix), eles também serão atribuídos. Somente um usuário pode usar a máquina por vez. Essa é uma configuração típica para funcionários de escritório ou que trabalham por turnos e que compartilham um computador.

  Esse método é aceito com máquinas Windows. Ele não pode ser usado com máquinas Linux.

- **Pré-atribuído estático:** os usuários são pré-atribuídos às máquinas. (Isso geralmente é configurado fazendo o upload de um arquivo CSV contendo o mapeamento usuário-máquina.) Não há necessidade de logon do usuário para estabelecer a atribuição após a instalação do VDA. Também não há necessidade de atribuir usuários ao catálogo depois que ele é criado. Esse é o melhor para funcionários de escritório.

  Esse método é aceito com máquinas Windows e Linux.

- **Aleatório de um pool não atribuído:** os usuários são atribuídos aleatoriamente a uma máquina disponível. Somente um usuário pode usar a máquina por vez. Ideal para laboratórios de computação em escolas.

  Esse método é aceito com máquinas Windows. Ele não pode ser usado com máquinas Linux.

Métodos para adicionar máquinas a um catálogo

Lembre-se: toda máquina deve ter um VDA instalado nela.

Ao criar ou editar um catálogo, há três maneiras de adicionar máquinas a ele:

- Selecionar contas de máquina uma a uma.
- Selecionar unidades organizacionais (UO).
- Adicionar em massa usando um arquivo CSV. Há um modelo disponível do arquivo CSV para você usar.

Adicionar nomes de máquinas

Esse método adiciona contas de máquina uma a uma.

1. Selecione seu domínio.
2. Procure a conta da máquina.
3. Clique em **Add**.
4. Repita para adicionar mais máquinas.
5. Quando terminar de adicionar máquinas, clique em **Done**.

Adicionar UOs

Este método adiciona contas de máquina de acordo com a Unidade Organizacional em que elas residem.
Ao selecionar UOs, escolha UOs de nível inferior para obter maior granularidade. Se a granularidade não for necessária, você pode escolher UOs de nível superior.

Por exemplo, no caso de `Bank`/`Officers`/`Tellers`, selecione `Tellers` para obter maior granularidade. Caso contrário, você pode selecionar `Officers` ou `Bank` de acordo com as exigências.

Mover ou excluir UOs depois que forem atribuídas a um catálogo Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Certifique-se de que seu plano de alteração do AD contabilize as atualizações de atribuição de UO para catálogos.

Para adicionar UOs:

1. Selecione seu domínio.
2. Selecione as UOs que contêm as contas de máquinas que você deseja adicionar.
3. Indique na caixa de seleção se deseja incluir as subpastas incluídas em suas seleções.
4. Quando terminar de selecionar as UOs, clique em **Done**.

Adicionar em massa

1. Clique em **Download CSV Template**.
2. No modelo, adicione as informações da conta da máquina (até 100 entradas). O arquivo CSV também pode conter o nome dos usuários atribuídos a cada máquina.
3. Salve o arquivo.

4. Arraste o arquivo para a página **Add machines in bulk** ou navegue até o arquivo.
5. É exibida uma pré-visualização do conteúdo do arquivo. Se esse não for o arquivo desejado, você pode criar outro arquivo e arrastá-lo ou navegar até ele.
6. Quando terminar, clique em **Done**.

Gerenciar catálogos de acesso ao PC remoto

Para exibir ou alterar as informações de configuração de um catálogo de Acesso Remoto ao PC, selecione o catálogo no painel **Gerenciar > Implantação Rápida do Azure** (clique em qualquer lugar em sua entrada).

- Na guia **Details**, você pode adicionar ou remover máquinas.
- Na guia **Subscribers**, você pode adicionar ou remover usuários.
- Na guia **Machines**, você pode:
  - Adicionar ou remover máquinas: botão **Add or remove machines**.
  - Alterar atribuições do usuário: ícone de lixeira **Remove assignment**, **Edit machine assignment** no menu de reticências.
  - Ver quais máquinas estão registradas e colocar as máquinas dentro ou fora do modo de manutenção.

Assinaturas do Azure

December 28, 2023

Introdução

O Citrix DaaS Standard for Azure (antigo serviço Citrix Virtual Apps and Desktops Standard for Azure) é compatível com assinaturas do Citrix Managed Azure e suas próprias assinaturas do Azure gerenciadas pelo cliente.

- Para usar suas próprias assinaturas do Azure, primeiro importe (adicione) uma ou mais dessas assinaturas ao Citrix DaaS for Azure. Essa ação permite que o Citrix DaaS for Azure acesse suas assinaturas do Azure.
- O uso de uma assinatura do Citrix Managed Azure não requer configuração de assinatura. No entanto, para ter uma assinatura do Citrix Managed Azure disponível, você deve ter solicitado o Citrix Azure Consumption Fund (além do Citrix DaaS Standard for Azure).

Ao criar um catálogo ou criar uma imagem, você escolhe entre as assinaturas disponíveis do Azure.

Alguns recursos de serviço diferem, dependendo se as máquinas estão em uma assinatura do Citrix Managed Azure ou em sua própria assinatura do Azure.

Assinatura do Citrix Managed Azure	Sua própria assinatura do Azure
Oferece suporte a máquinas ingressadas no domínio ou não ingressadas no domínio.	Oferece suporte somente a máquinas ingressadas no domínio.
Oferece suporte à criação rápida e criação personalizada de catálogos.	Suporta apenas catálogos de criação personalizados.
Sempre disponível (e é a seleção de assinatura padrão) ao criar catálogos e imagens.	É necessário adicionar a assinatura do Azure ao Citrix DaaS for Azure antes de criar um catálogo.
Para autenticação de usuário, oferece suporte ao Citrix Managed Azure Active Directory ou ao seu próprio Active Directory.	Pode conectar seu próprio Active Directory e Azure Active Directory.
As opções de conexão de rede incluem **No connectivity**.	As opções de conexão de rede incluem apenas suas próprias redes virtuais.
Ao usar o emparelhamento de VNet do Azure para se conectar aos seus recursos, você deve criar uma conexão de mesmo nível VNet no Citrix DaaS para Azure.	Selecione uma rede virtual existente.
Ao importar uma imagem do Azure, você especifica o URI da imagem.	Ao importar uma imagem, você pode selecionar um VHD ou navegar pelo armazenamento na assinatura do Azure.
Pode criar uma máquina bastion assinatura do Azure do cliente para solucionar problemas de máquinas.	Não há necessidade de criar uma máquina bastion porque você já pode acessar as máquinas em sua assinatura.

Exibir assinaturas

Para visualizar os detalhes da assinatura, no painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Assinaturas de nuvem** à direita. Em seguida, clique em uma entrada de assinatura.

- A página **Detalhes** inclui o número de máquinas, além dos números e nomes de catálogos e imagens na assinatura.
- A página **Locais de recursos** lista os locais de recursos em que a assinatura é usada.

Adicionar assinaturas do Azure gerenciadas pelo cliente

Para usar uma assinatura do Azure gerenciada pelo cliente, você deve adicioná-la ao Citrix DaaS Standard for Azure antes de criar um catálogo ou imagem que use essa assinatura. Você tem duas opções ao adicionar suas assinaturas do Azure:

- **Se você for administrador global do diretório e tiver privilégios de proprietário para a assinatura:** basta se autenticar na sua conta do Azure.
- **Se você não for um administrador global e tiver privilégios de proprietário na assinatura:** antes de adicionar a assinatura ao Citrix DaaS for Azure, crie um aplicativo do Azure no seu Azure AD e adicione esse aplicativo como colaborador da assinatura. Ao adicionar essa assinatura ao Citrix DaaS para Azure, você fornece informações relevantes sobre o aplicativo.

Adicione assinaturas do Azure gerenciadas pelo cliente se você for um Administrador Global

Essa tarefa exige privilégios de administrador global para o diretório e privilégios de proprietário para a assinatura.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Assinaturas de nuvem** à direita.
2. Clique em **Adicionar assinatura do Azure**.
3. Na página **Adicionar assinaturas**, clique em **Adicionar sua assinatura do Azure**.
4. Selecione o botão que permite que o Citrix DaaS for Azure acesse suas assinaturas do Azure em seu nome.
5. Clique em **Autenticar conta do Azure**. Você é direcionado para a página de login do Azure.
6. Insira suas credenciais do Azure.
7. Você retorna automaticamente ao Citrix DaaS para Azure. A página **Adicionar assinatura** lista as assinaturas do Azure descobertas. Use a caixa de pesquisa para filtrar a lista, se necessário. Selecione uma ou mais assinaturas. Quando terminar, clique em **Adicionar assinaturas**.
8. Confirme se você deseja adicionar as assinaturas selecionadas.

As assinaturas do Azure selecionadas são listadas quando você expande **Assinaturas**. As assinaturas adicionadas estão disponíveis para seleção ao criar um catálogo ou uma imagem.

Adicione assinaturas do Azure gerenciadas pelo cliente se você não for um administrador global

Adicionar uma assinatura do Azure quando você não é um administrador global é um processo de duas partes:

- Antes de adicionar uma assinatura ao Citrix DaaS for Azure, crie um aplicativo no Azure AD e adicione esse aplicativo como colaborador da assinatura.

- Adicione a assinatura ao Citrix DaaS for Azure, usando informações sobre o aplicativo que você criou no Azure.

Crie um aplicativo no Azure AD e adicione-o como colaborador

1. Registre um novo aplicativo no Azure AD:
   a) Em um navegador, navegue até https://portal.azure.com.
   b) No menu superior esquerdo, selecione **Azure Active Directory**.
   c) Na lista **Gerenciar**, clique em **Registros de aplicativos**.
   d) Clique em **+ Novo registro**.
   e) Na página **Registrar um aplicativo**, forneça as seguintes informações:
      - **Name:** Insira o nome da conexão
      - **Application type:** Selecione **Web app / API**
      - **URI de redirecionamento:** deixe em branco
   f) Clique em **Create**.
2. Crie a chave de acesso secreta do aplicativo e adicione a atribuição de função:
   a) No procedimento anterior, selecione **App Registration** para ver os detalhes.
   b) Anote o ID do **aplicativo e o IDdo diretório**. Você usará isso mais tarde ao adicionar sua assinatura ao Citrix DaaS para Azure.
   c) Em **Gerenciar**, selecione **Certificados e segredos**.
   d) Na página **Client secrets**, selecione **+ New client secret**.
   e) Na página **Adicionar segredo do cliente**, forneça uma descrição e selecione um intervalo de expiração. Em seguida, clique em **Add**.
   f) Anote o valor do segredo do cliente. Você usará isso mais tarde ao adicionar sua assinatura ao Citrix DaaS para Azure.
   g) Selecione a assinatura do Azure que você deseja vincular (adicionar) ao Citrix DaaS for Azure e clique em **Controle de acesso (IAM)**.
   h) Na caixa **Adicionar uma atribuição de função**, clique em **Adicionar**.
   i) Na guia **Adicionar atribuição de função**, selecione o seguinte:
      - **Role:** Colaborador
      - **Assign access to:** usuário, grupo ou entidade de serviço do Azure AD
      - **Selecione:** O nome do aplicativo do Azure que você criou anteriormente.
   j) Clique em **Save**.

Adicione sua assinatura ao Citrix DaaS for Azure Você precisará do ID do aplicativo, do ID do diretório e do valor do segredo do cliente do aplicativo criado no Azure AD.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Assinaturas de nuvem** à direita.
2. Clique em **Adicionar assinatura do Azure**.
3. Na página **Adicionar assinaturas**, clique em **Adicionar suas assinaturas do Azure**.
4. Selecione **Eu tenho um aplicativo do Azure com função de colaborador para a assinatura**.
5. Insira o ID do locatário (ID do diretório), o ID do cliente (ID do aplicativo) e o segredo do cliente para o aplicativo que você criou no Azure.
6. Clique em **Selecionar sua assinatura** e, em seguida, selecione a assinatura desejada.

Posteriormente, na página **Detalhes** da assinatura no painel do Citrix DaaS para Azure, você pode atualizar o segredo do cliente ou substituir o aplicativo do Azure no menu de reticências.

Se o Citrix DaaS for Azure não puder acessar uma assinatura do Azure depois que ela for adicionada, não serão permitidas várias ações de gerenciamento de energia do catálogo e de máquinas individuais. Uma mensagem oferece a opção de adicionar a assinatura novamente. Se a assinatura foi originalmente adicionada usando um aplicativo do Azure, você pode substituir o aplicativo do Azure.

Adicionar assinaturas do Citrix Managed Azure

Uma assinatura do Citrix Managed Azure suporta o número de máquinas indicado em Limites. (Nesse contexto, *as máquinas* se referem a VMs que têm um Citrix VDA instalado. Essas máquinas fornecem aplicativos e desktops aos usuários. A expressão não inclui outras máquinas em um local de recurso, como Cloud Connectors.)

Se sua assinatura do Citrix Managed Azure provavelmente atingirá seu limite em breve e você tiver licenças Citrix suficientes, poderá solicitar outra assinatura do Citrix Managed Azure. O painel contém uma notificação quando você está perto do limite.

Você não pode criar um catálogo (ou adicionar máquinas a um catálogo) se o número total de máquinas para todos os catálogos que usam essa assinatura do Citrix Managed Azure exceder o valor indicado em Limites.

Por exemplo, suponha um limite hipotético de 1.000 máquinas por assinatura do Citrix Managed Azure.

- Digamos que você tenha dois catálogos (`Cat1` e `Cat2`) que usam a mesma assinatura do Citrix Managed Azure. `Cat1` atualmente contém 500 máquinas e `Cat2` tem 250.
- Ao planejar as necessidades futuras de capacidade, você adiciona 200 máquinas a `Cat2`. A assinatura do Citrix Managed Azure agora oferece suporte a 950 máquinas (500 em `Cat 1` e 450 em `Cat 2`). O painel indica que a assinatura está perto do limite.

- Quando você precisar de mais 75 máquinas, não poderá usar essa assinatura para criar um catálogo com 75 máquinas (ou adicionar 75 máquinas a um catálogo existente). Isso excederia o limite de assinatura. Em vez disso, você solicita outra assinatura do Citrix Managed Azure. Em seguida, você pode criar um catálogo usando essa assinatura.

Quando você tiver mais de uma assinatura do Citrix Managed Azure:

- Nada é compartilhado entre essas assinaturas.
- Cada assinatura tem um nome exclusivo.
- Você pode escolher entre as assinaturas do Citrix Managed Azure (e todas as assinaturas do Azure gerenciadas pelo cliente que você adicionou) quando:
  - Criação de um catálogo.
  - Construindo ou importando uma imagem.
  - Criação de um emparelhamento VNet ou conexão SD-WAN.

Requisito:

- Você deve ter licenças Citrix suficientes para garantir a adição de outra assinatura do Citrix Managed Azure. Usando o exemplo hipotético anterior, se você tiver 2.000 licenças Citrix anteriormente à implantação de pelo menos 1.500 máquinas por meio de assinaturas do Citrix Managed, poderá adicionar outra assinatura do Citrix Managed Azure.

Para adicionar uma assinatura do Citrix Managed Azure:

1. Entre em contato com seu representante Citrix para solicitar outra assinatura do Citrix Managed Azure. Você será notificado quando puder continuar.
2. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Assinaturas de nuvem** à direita.
3. Clique em **Adicionar assinatura do Azure**.
4. Na página **Adicionar assinaturas**, clique em **Adicionar uma assinatura do Citrix Managed Azure**.
5. Na página **Adicionar uma assinatura gerenciada Citrix**, clique em **Adicionar assinatura** na parte inferior da página.

Se você for notificado de que ocorreu um erro durante a criação de uma assinatura do Citrix Managed Azure, entre em contato com o Suporte da Citrix.

Remover assinaturas do Azure

Para remover uma assinatura do Azure, você deve primeiro excluir todos os catálogos e imagens que a usam.

Se você tiver uma ou mais assinaturas do Citrix Managed Azure, não poderá remover todas elas. Pelo menos uma deve permanecer.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Assinaturas de nuvem** à direita.
2. Clique na entrada de assinatura.
3. Na guia **Detalhes**, clique em **Remover assinatura**.
4. Clique em **Autenticar conta do Azure**. Você é direcionado para a página de login do Azure.
5. Insira suas credenciais do Azure.
6. Você retorna automaticamente ao Citrix DaaS para Azure. Confirme a exclusão nas caixas de seleção e clique em **Sim, Excluir assinatura**.

Conexões de rede

May 11, 2023

Introdução

Este artigo fornece detalhes sobre vários cenários de implantação ao usar uma assinatura do Citrix Managed Azure.

Ao criar um catálogo, você indica se e como os usuários acessam locais e recursos em sua rede local corporativa a partir de seus desktops e aplicativos Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure).

Ao usar uma assinatura do Citrix Managed Azure, as opções são:

- Sem conectividade
- Emparelhamento do Azure VNet
- SD-WAN

Ao usar uma de suas próprias assinaturas do Azure gerenciadas pelo cliente, não há necessidade de criar uma conexão com o Citrix DaaS for Azure. Você acabou de adicionar a assinatura do Azure ao Citrix DaaS for Azure.

Você não pode alterar o tipo de conexão de um catálogo após a criação do catálogo.

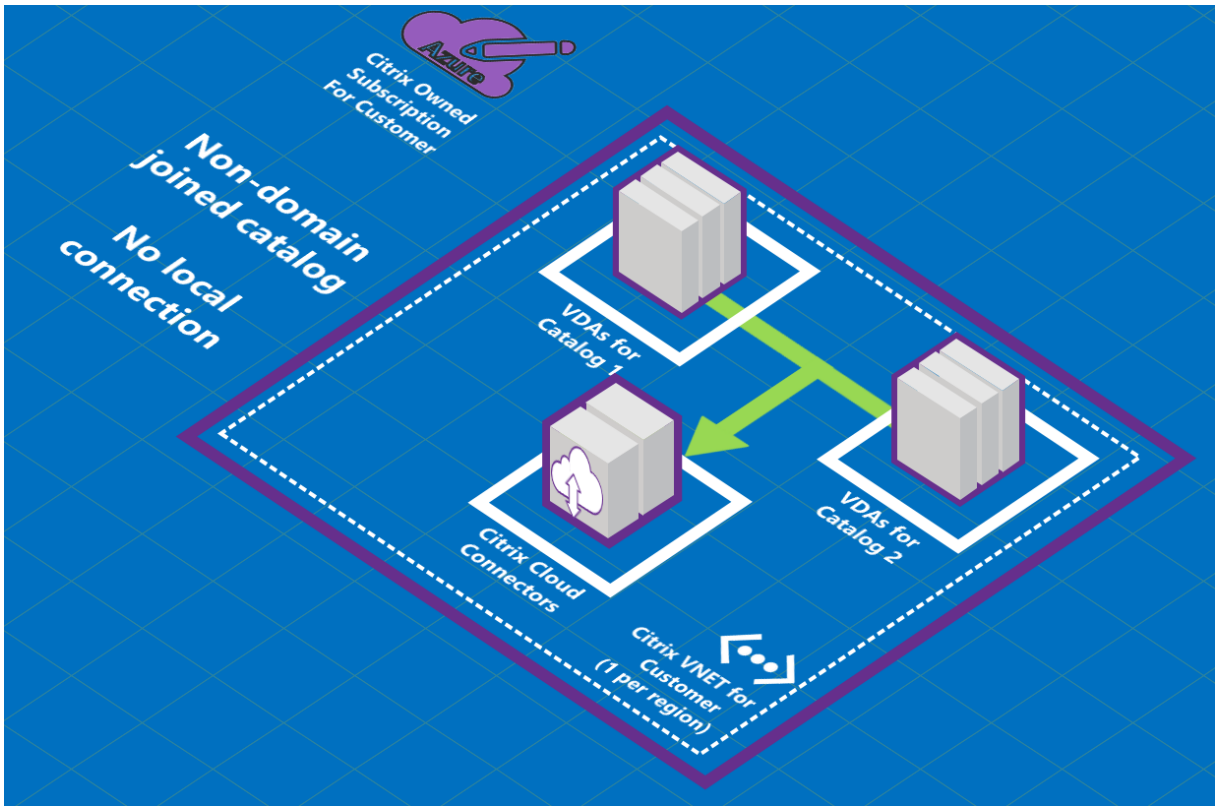
Requisitos para todas as conexões de rede

- Ao criar uma conexão, você deve ter entradas de servidor DNS válidas.

- Ao usar o Secure DNS ou um provedor de DNS de terceiros, você deve adicionar o intervalo de endereços alocado para uso pelo Citrix DaaS for Azure aos endereços IP do provedor de DNS na lista de permissões. Esse intervalo de endereços é especificado quando você cria uma conexão.
- Todos os recursos de serviço que usam a conexão (máquinas ingressadas no domínio) devem ser capazes de acessar seu servidor NTP (Network Time Protocol), para garantir a sincronização de horário.

Sem conectividade

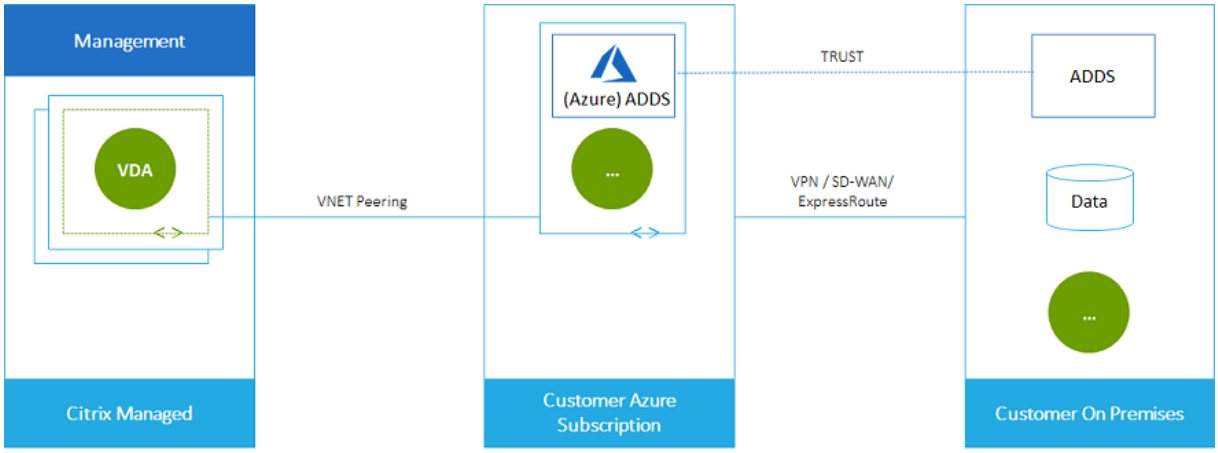
Quando um catálogo é configurado com **Sem conectividade**, os usuários não podem acessar recursos em suas redes locais ou em outras redes. Essa é a única opção ao criar um catálogo usando a criação rápida.



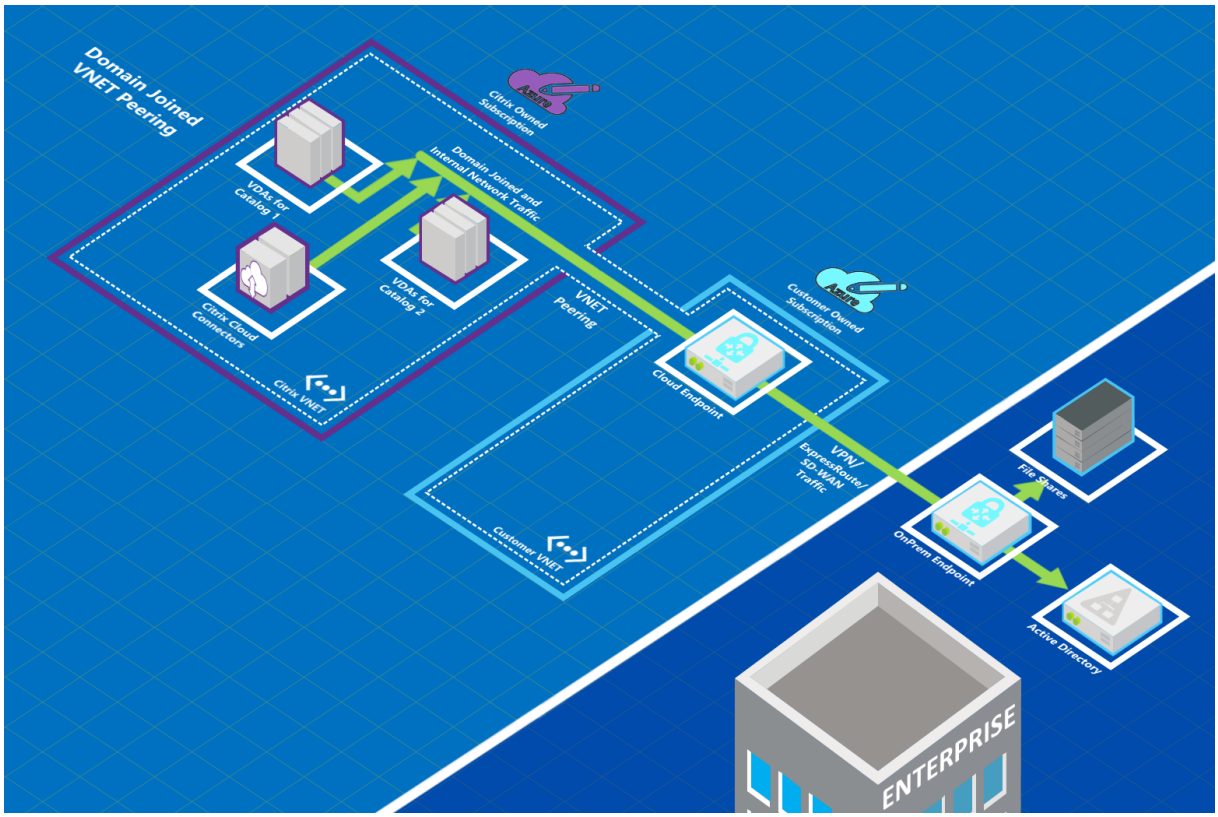
Sobre as conexões de emparelhamento do Azure VNet

O peering de rede virtual conecta perfeitamente duas redes virtuais do Azure (VNETs): a sua e o Citrix DaaS para Azure VNet. O emparelhamento também ajuda a permitir que os usuários acessem arquivos e outros itens de suas redes locais.

Conforme mostrado no gráfico a seguir, você cria uma conexão usando o emparelhamento VNet do Azure da assinatura do Citrix Managed Azure para o VNet na assinatura do Azure da sua empresa.



Aqui está outra ilustração do emparelhamento VNet.



Os usuários podem acessar seus recursos de rede locais (como servidores de arquivos) ingressando no domínio local quando você cria um catálogo. (Ou seja, você ingressará no domínio do AD onde residem os compartilhamentos de arquivos e outros recursos necessários.) Sua assinatura do Azure se conecta a esses recursos (nos gráficos, usando uma VPN ou o Azure ExpressRoute). Ao criar o catálogo, você fornece o domínio, a UO e as credenciais da conta.

> **Importante:**
>
> - Saiba mais sobre o emparelhamento de VNet antes de usá-lo no Citrix DaaS para Azure.

> • Crie uma conexão de emparelhamento VNet antes de criar um catálogo que a use.

Rotas personalizadas de peering do Azure VNet

As rotas personalizadas ou definidas pelo usuário substituem as rotas de sistema padrão do Azure para direcionar o tráfego entre máquinas virtuais em um emparelhamento VNet, redes locais e a Internet. Você pode usar rotas personalizadas se houver redes que os recursos do Citrix DaaS para Azure devem acessar, mas não estão diretamente conectadas por meio do emparelhamento VNet. Por exemplo, você pode criar uma rota personalizada que force o tráfego por meio de um dispositivo de rede para a Internet ou para uma sub-rede de rede local.

Para usar rotas personalizadas:

- Você deve ter um gateway de rede virtual do Azure existente ou um dispositivo de rede, como o Citrix SD-WAN, em seu ambiente Citrix DaaS para Azure.
- Ao adicionar rotas personalizadas, você deve atualizar as tabelas de rotas da sua empresa com as informações de VNet de destino do Citrix DaaS para Azure para garantir a conectividade de ponta a ponta.
- As rotas personalizadas são exibidas no Citrix DaaS for Azure na ordem em que são inseridas. Essa ordem de exibição não afeta a ordem na qual o Azure seleciona as rotas.

Antes de usar rotas personalizadas, consulte o artigo da Microsoft Roteamento de tráfego de rede virtual para saber mais sobre como usar rotas personalizadas, tipos de próximo salto e como o Azure seleciona rotas para tráfego de saída.

Você pode adicionar rotas personalizadas ao criar uma conexão emparelhada do Azure VNet ou a rotas existentes em seu ambiente Citrix DaaS para Azure. Quando você estiver pronto para usar rotas personalizadas com seu emparelhamento VNet, consulte as seções a seguir neste artigo:

- Para rotas personalizadas com novos peerings do Azure VNet: Create an Azure VNet peering connection
- Para rotas personalizadas com peerings de VNet do Azure existentes: Manage custom routes for existing Azure VNet peer connections

Requisitos e preparação de emparelhamento do Azure VNet

- Credenciais de um proprietário de assinatura do Azure Resource Manager. Essa deve ser uma conta do Azure Active Directory. O Citrix DaaS para Azure não oferece suporte a outros tipos de conta, como live.com ou contas externas do Azure AD (em um locatário diferente).
- Uma assinatura do Azure, um grupo de recursos e uma rede virtual (VNet).

- Configure as rotas de rede do Azure para que os VDAs na assinatura do Citrix Managed Azure possam se comunicar com seus locais de rede.
- Abra os grupos de segurança de rede do Azure da sua VNet para o intervalo de IP especificado.
- **Active Directory:** em cenários de ingresso em domínios, recomendamos que você tenha alguma forma de serviços do Active Directory em execução na VNet emparelhada. Isso aproveita as características de baixa latência da tecnologia de emparelhamento VNet do Azure.

  Por exemplo, a configuração pode incluir os Serviços de Domínio do Azure Active Directory (AADDS), uma VM de controlador de domínio na VNet ou o Azure AD Connect ao Active Directory local.

  Depois de habilitar o AADDS, você não poderá mover seu domínio gerenciado para uma VNet diferente sem excluir o domínio gerenciado. Portanto, é importante selecionar a VNet correta para habilitar seu domínio gerenciado. Antes de continuar, leia o artigo da Microsoft Networking considerations for Azure AD Domain Services.
- **Intervalo de IP VNet:** Ao criar a conexão, você deve fornecer um espaço de endereço CIDR disponível (endereço IP e prefixo de rede) exclusivo entre os recursos de rede e as VNets do Azure que estão sendo conectadas. Esse é o intervalo de IP atribuído às VMs dentro do Citrix DaaS for Azure peering VNet.

  Certifique-se de especificar um intervalo de IP que não se sobreponha a nenhum endereço usado nas redes Azure e no local.

  - Por exemplo, se sua VNet do Azure tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão emparelhada VNet no Citrix DaaS para Azure como algo como 192.168.0.0 /24.
  - Neste exemplo, criar uma conexão de emparelhamento com um intervalo de IP 10.0.0.0 /24 seria considerado um intervalo de endereços sobreposto.

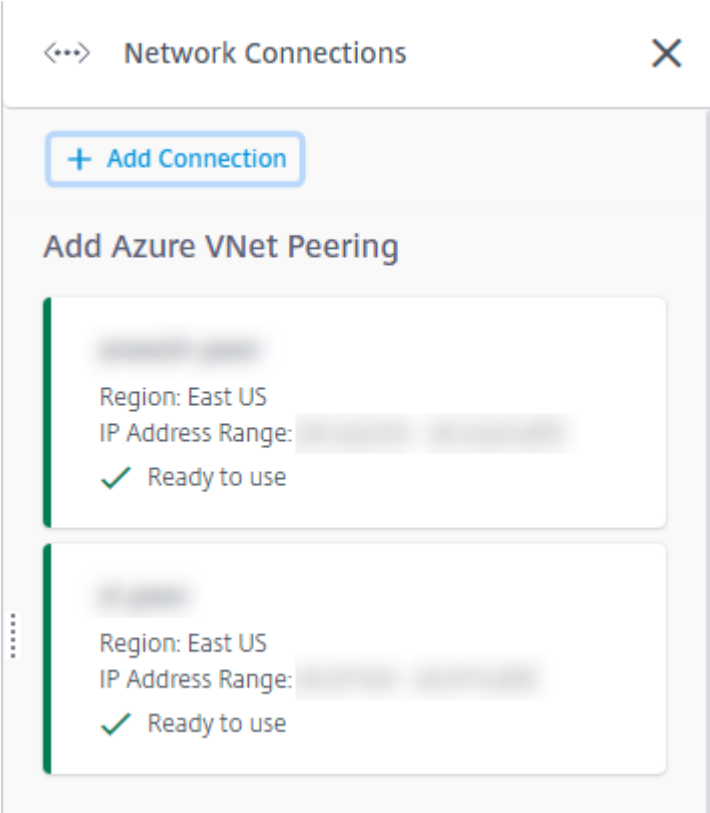
  Se os endereços se sobrepuserem, poderá não ser possível criar a conexão de emparelhamento VNet. Também não funciona corretamente para tarefas de administração do site.

Para saber mais sobre o emparelhamento de VNet, consulte os seguintes artigos da Microsoft.

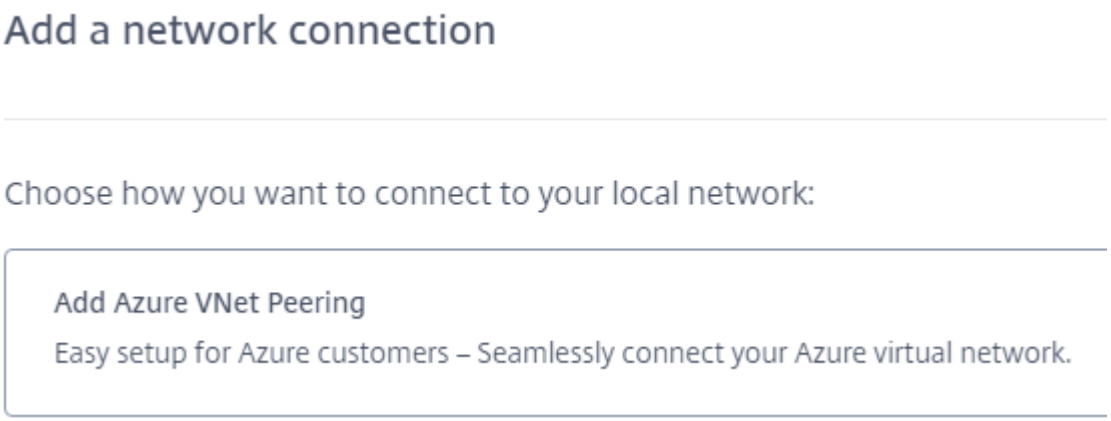
- Virtual network peering
- Azure VPN Gateway
- Create a Site-to-Site connection in the Azure portal
- VPN Gateway FAQ (procure por “overlap”)

Criar uma conexão emparelhada do Azure VNet

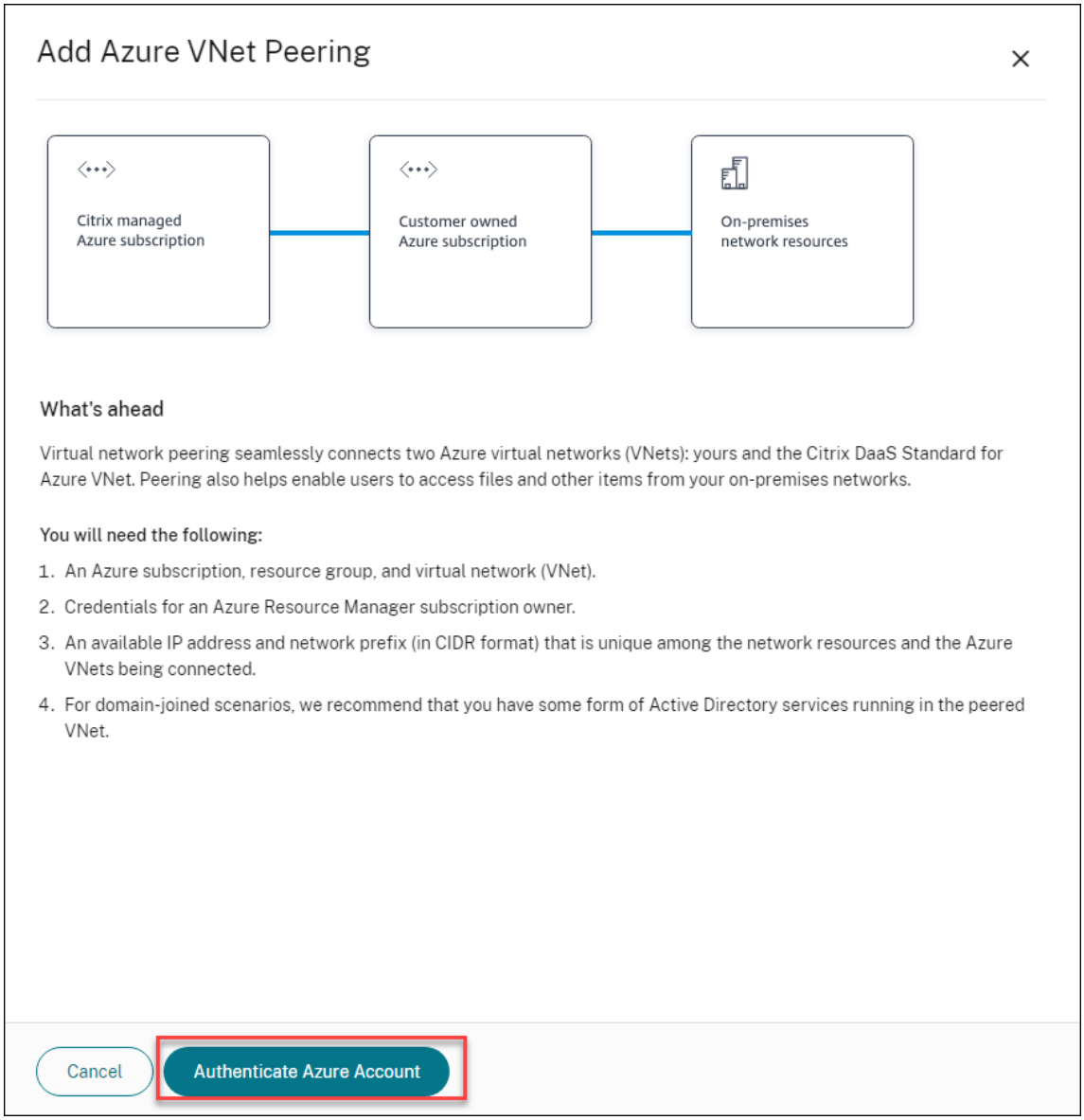
1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita. Se você já tiver configurado conexões, elas estão listadas.



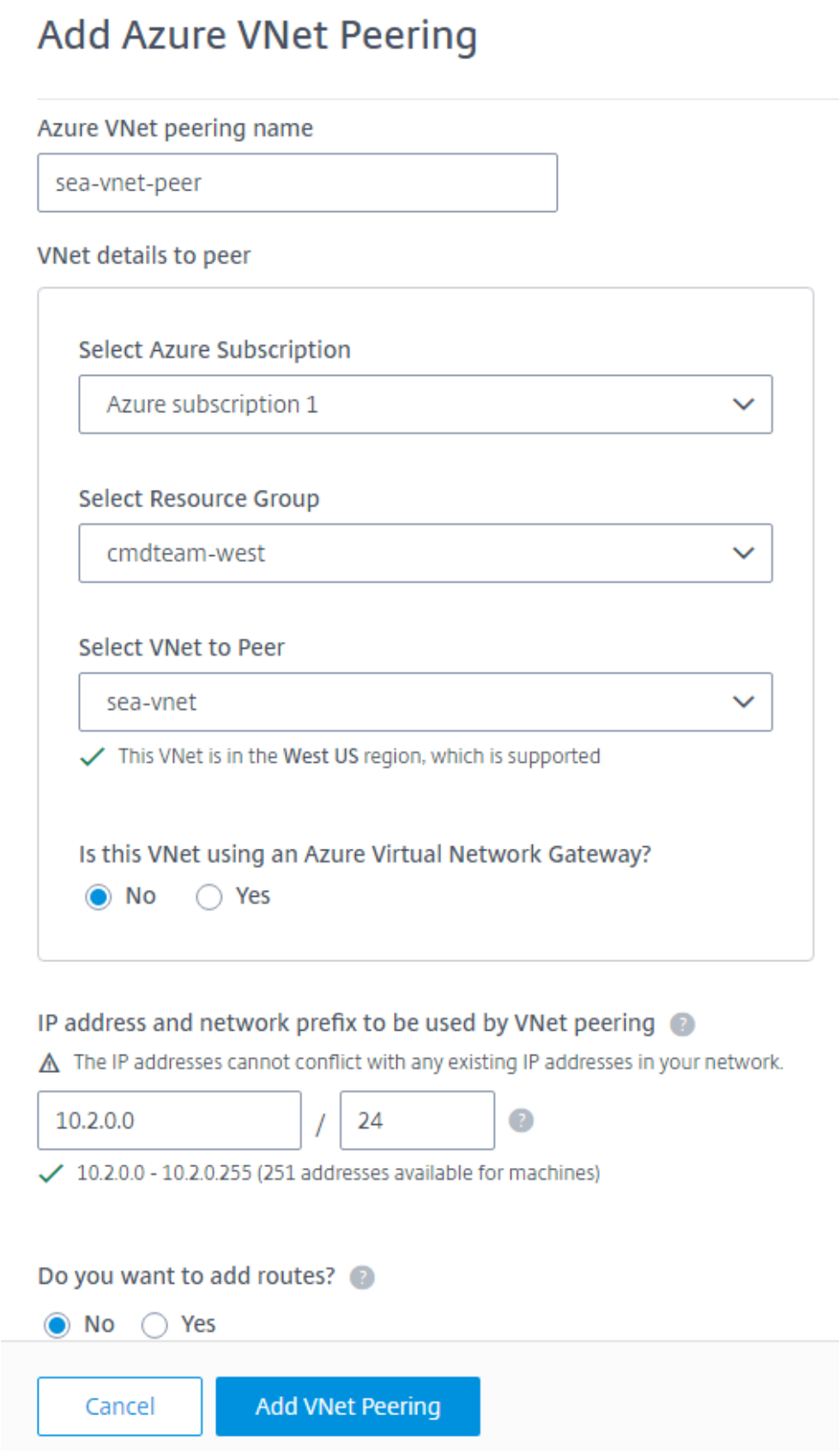
2. Clique em **Adicionar conexão**.
3. Clique em qualquer lugar na caixa **Adicionar emparelhamento de VNet do Azure**.



4. Clique em **Autenticar conta do Azure**.



5. O Citrix DaaS for Azure leva você automaticamente para a página de login do Azure para autenticar suas assinaturas do Azure. Depois de entrar no Azure (com as credenciais da conta de administrador global) e aceitar os termos, você retornará à caixa de diálogo de detalhes da criação da conexão.



6. Digite um nome para o par VNet do Azure.
7. Selecione a assinatura do Azure, o grupo de recursos e o VNet to peer.
8. Indique se a VNet selecionada usa um Gateway de Rede Virtual do Azure. Para obter informações, consulte o artigo da Microsoft Azure VPN Gateway.
9. Se você respondeu **Sim** na etapa anterior (a VNet selecionada usa um gateway de rede virtual do Azure), indique se deseja habilitar a propagação de rota do gateway de rede virtual. Quando habilitado, o Azure aprende automaticamente (adiciona) todas as rotas por meio do gateway.

   Você pode alterar essa configuração posteriormente na página **Details** da conexão. No entanto, alterá-lo pode causar alterações no padrão de rota e interrupções no tráfego VDA. Além disso, se você desativá-lo mais tarde, deverá adicionar manualmente rotas às redes que os VDAs usarão.
10. Digite um endereço IP e selecione uma máscara de rede. O intervalo de endereços a ser usado é exibido, além de quantos endereços o intervalo suporta. Certifique-se de que o intervalo de IP não se sobreponha a nenhum endereço que você usa nas redes Azure e no local.

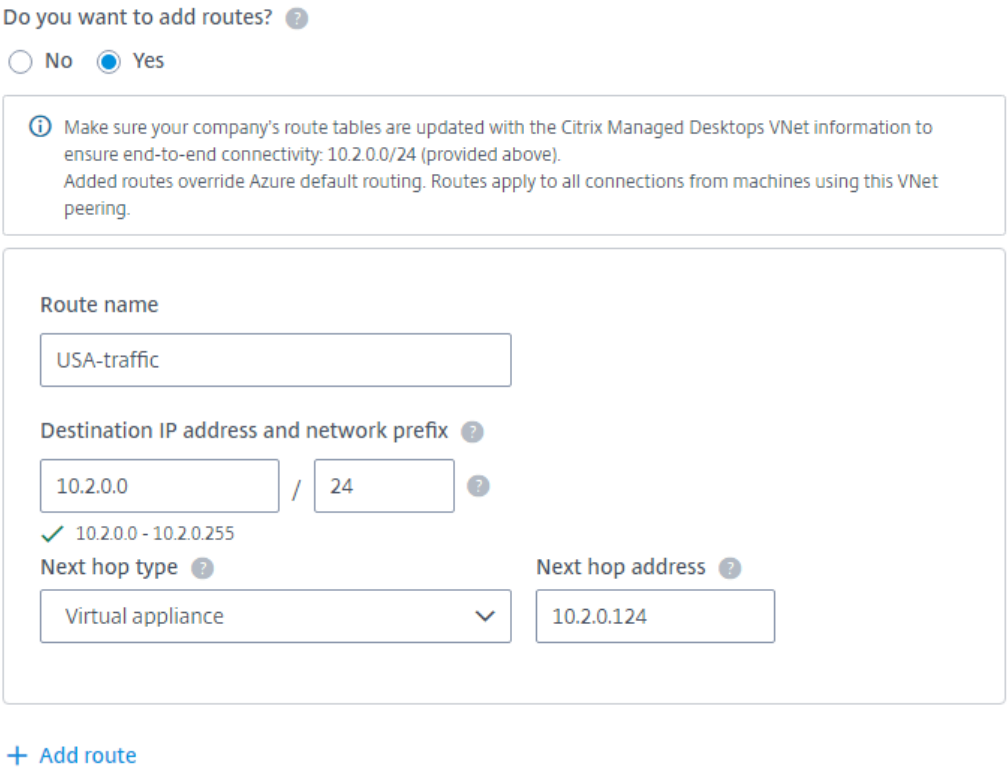
    - Por exemplo, se o Azure VNet tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão de emparelhamento VNet no Citrix Virtual Apps and Desktops Standard como algo como 192.168.0.0 /24.
    - Neste exemplo, criar uma conexão de emparelhamento VNet com um intervalo de IP 10.0.0.0 /24 seria considerado um intervalo de endereços sobreposto.

    Se os endereços se sobrepõem, a conexão de emparelhamento VNet pode não ser criada com êxito. Também não funciona corretamente para tarefas de administração do site.
11. Indique se você deseja adicionar rotas personalizadas à conexão de emparelhamento VNet. Se selecionar **Yes**, insira as seguintes informações:

    a) Digite um nome amigável para a rota personalizada.

    b) Insira o endereço IP de destino e o prefixo da rede. O prefixo da rede deve estar entre 16 e 24.

    c) Selecione um tipo de próximo salto para onde você deseja que o tráfego seja roteado. Se você selecionar **Virtual appliance**, digite o endereço IP interno do equipamento.



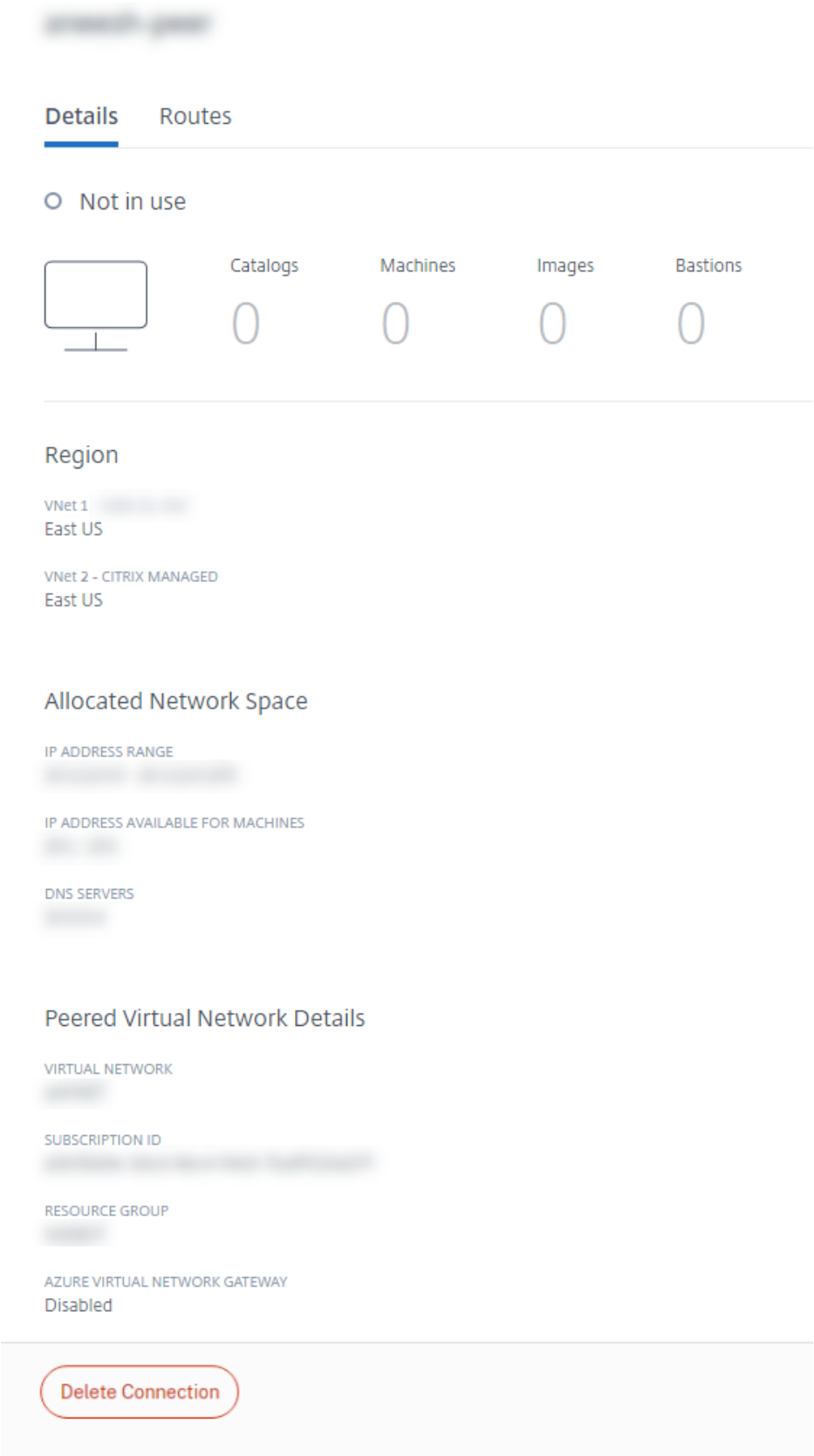
Para obter mais informações sobre os próximos tipos de salto, consulte Rotas personalizadas no artigo da Microsoft Roteamento de tráfego de rede virtual.

d) Clique em **Adicionar rota** para criar outra rota personalizada para a conexão.

12. Clique em **Adicionar emparelhamento VNet**.

Depois que a conexão é criada, ela é listada em **Conexões de Rede > Pares VNet do Azure** no lado direito do painel **Gerenciar > Implantação Rápida do Azure** . Quando você cria um catálogo, essa conexão é incluída na lista de conexões de rede disponíveis.

Veja os detalhes da conexão de peering do Azure VNet



1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Selecione a conexão emparelhada do Azure VNet que você deseja exibir.

Os detalhes incluem:

- O número de catálogos, máquinas, imagens e bastions que usam essa conexão.
- A região, o espaço de rede alocado e as VNets emparelhadas.
- As rotas atualmente configuradas para a conexão de emparelhamento VNet.

Gerenciar rotas personalizadas para conexões de mesmo nível existentes do Azure VNet

Você pode adicionar novas rotas personalizadas a uma conexão existente ou modificar rotas personalizadas existentes, inclusive a desativação ou exclusão de rotas personalizadas.

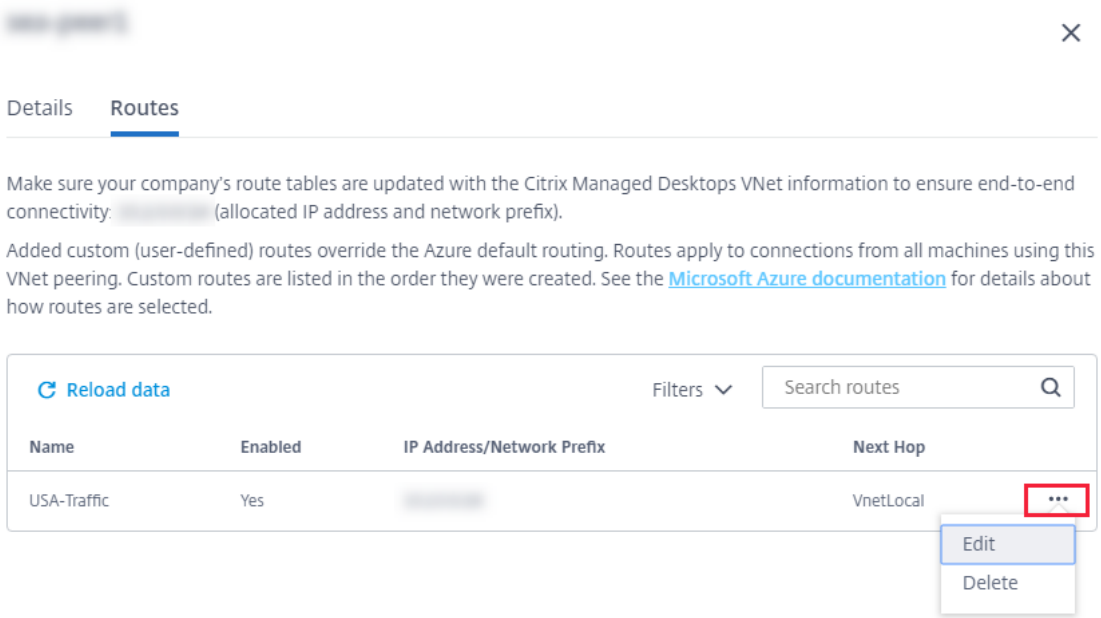
> **Importante:**
>
> A modificação, desativação ou exclusão de rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper qualquer sessão de usuário que possa estar ativa.

Para adicionar uma rota personalizada:

1. Nos detalhes da conexão de emparelhamento VNet, selecione **Rotas** e clique em **Adicionar Rota**.
2. Digite um nome amigável, o endereço IP de destino e o prefixo e o próximo tipo de salto que você deseja usar. Se você selecionar **Virtual Appliance** como o tipo de salto seguinte, digite o endereço IP interno do equipamento.
3. Indique se você deseja ativar a rota personalizada. Por padrão, a rota personalizada está ativada.
4. Clique em **Adicionar rota**.

Para modificar ou desativar uma rota personalizada:

1. Nos detalhes da conexão de emparelhamento VNet, selecione **Rotas** e, em seguida, localize a rota personalizada que você deseja gerenciar.
2. No menu de reticências, selecione **Editar**.



3. Faça as alterações necessárias no endereço IP e prefixo de destino ou no tipo de próximo salto, conforme necessário.
4. Para habilitar ou desabilitar uma rota personalizada, em **Habilitar esta rota?**, selecione **Sim** ou **Não**.
5. Clique em **Save**.

Para excluir uma rota personalizada:

1. Nos detalhes da conexão de emparelhamento VNet, selecione **Rotas** e, em seguida, localize a rota personalizada que você deseja gerenciar.
2. No menu de reticências, selecione **Excluir**.
3. Selecione **Excluir uma rota pode interromper as sessões ativas** para reconhecer o impacto da exclusão da rota personalizada.
4. Clique em **Excluir rota**.

Excluir uma conexão de emparelhamento Azure VNet

Antes de excluir um peer VNet do Azure, remova todos os catálogos associados a ele. Consulte Delete a catalog.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, clique em **Excluir conexão**.

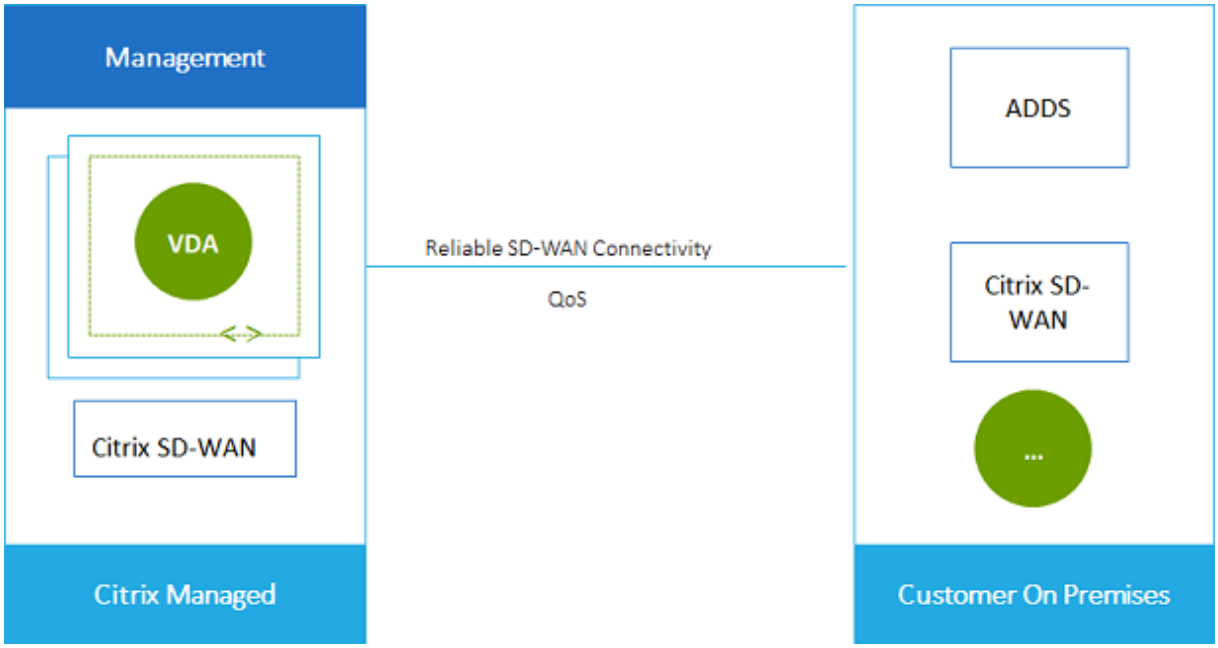
Sobre as conexões SD-WAN

> **Importante:**
>
> O Citrix SD-WAN foi preterido e todo o conteúdo relacionado será removido da documentação em uma versão futura. Recomendamos que você mude para soluções de rede alternativas para garantir acesso ininterrupto aos serviços Citrix.

O Citrix SD-WAN otimiza todas as conexões de rede necessárias para o Citrix Virtual Apps and Desktops Standard for Azure. Trabalhando em conjunto com as tecnologias HDX, o Citrix SD-WAN fornece qualidade de serviço e confiabilidade de conexão para tráfego padrão ICA e Citrix Virtual Apps and Desktops fora de banda. O Citrix SD-WAN oferece suporte às seguintes conexões de rede:

- Conexão ICA multi-stream entre usuários e seus desktops virtuais
- Acesso à Internet da área de trabalho virtual para sites, aplicativos SaaS e outras propriedades de nuvem
- Acesso da área de trabalho virtual de volta aos recursos locais, como Active Directory, servidores de arquivos e servidores de banco de dados
- Tráfego interativo/em tempo real transportado pelo RTP do mecanismo de mídia no aplicativo Workspace para serviços de Unified Communications hospedados na nuvem, como o Microsoft Teams
- Busca do lado do cliente de vídeos de sites como YouTube e Vimeo

Conforme mostrado no gráfico a seguir, você cria uma conexão SD-WAN a partir da assinatura do Citrix Managed Azure para seus sites. Durante a criação da conexão, os dispositivos SD-WAN VPX são criados na assinatura do Citrix Managed Azure. Do ponto de vista da SD-WAN, esse local é tratado como uma ramificação.



Requisitos e preparação da conexão SD-WAN

- Se os requisitos a seguir não forem atendidos, a opção de conexão de rede SD-WAN não estará disponível.
  - Direitos do Citrix Cloud: Citrix Virtual Apps and Desktops Standard para Azure e SD-WAN Orchestrator.
  - Uma implantação de SD-WAN instalada e configurada. A implantação deve incluir um Master Control Node (MCN), seja na nuvem ou no local, e ser gerenciada com o SD-WAN Orchestrator.
- Intervalo de IP VNet: forneça um espaço de endereço CIDR disponível (endereço IP e prefixo de rede) exclusivo entre os recursos de rede que estão sendo conectados. Esse é o intervalo de IP atribuído às VMs no Citrix Virtual Apps and Desktops Standard VNet.

  Certifique-se de especificar um intervalo de IP que não se sobreponha a nenhum endereço usado na nuvem e nas redes locais.

  - Por exemplo, se sua rede tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão no Citrix Virtual Apps and Desktops Standard como algo como 192.168.0.0 /24.
  - Neste exemplo, criar uma conexão com um intervalo de IP 10.0.0.0 /24 seria considerado um intervalo de endereços sobreposto.

  Se os endereços se sobrepuserem, poderá não ser possível criar a conexão. Ele também não funciona corretamente para tarefas de administração do site.
- O processo de configuração de conexão inclui tarefas que você (o administrador do Citrix DaaS for Azure) e o administrador do SD-WAN Orchestrator devem concluir. Além disso, para concluir suas tarefas, você precisa de informações fornecidas pelo administrador do SD-WAN Orchestrator.

  Recomendamos que você revise a orientação neste documento, além da documentação da SD-WAN, antes de criar uma conexão de fato.

Criar uma conexão SD-WAN

> **Importante:**
>
> Para obter detalhes sobre a configuração da SD-WAN, consulte Configuração da SD-WAN para integração do Citrix Virtual Apps and Desktops Standard for Azure.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Clique em **Adicionar conexão**.

3. Na página **Adicionar uma conexão de rede**, clique em qualquer lugar na caixa SD-WAN.
4. A próxima página resume o que está por vir. Quando terminar de ler, clique em **Iniciar configuração da SD-WAN**.
5. Na página **Configurar SD-WAN**, insira as informações fornecidas pelo administrador do SD-WAN Orchestrator.
   - **Deployment mode:** se você selecionar **High availability**, dois dispositivos VPX serão criados (recomendado para ambientes de produção). Se você selecionar **Standalone**, será criado um equipamento. Você não pode alterar essa configuração posteriormente. Para mudar para o modo de implantação, você terá que excluir e recriar o branch e todos os catálogos associados.
   - **Name:** digite um nome para o site da SD-WAN.
   - **Throughput and number of offices:** essas informações são fornecidas pelo administrador do SD-WAN Orchestrator.
   - **Region:** a região onde os dispositivos VPX serão criados.
   - **VDA subnet and SD-WAN subnet:** essas informações são fornecidas pelo administrador do SD-WAN Orchestrator. Consulte Requisitos de conexão SD-WAN e preparação para obter informações sobre como evitar conflitos.
6. Quando terminar, clique em **Criar ramificação**.
7. A próxima página resume o que procurar no painel **Gerenciar > Implantação Rápida do Azure** . Quando terminar de ler, clique em **Entendi**.
8. No painel **Gerenciar > Implantação Rápida do Azure**, a nova entrada SD-WAN em **Conexões de Rede** mostra o andamento do processo de configuração. Quando a entrada ficar laranja com a mensagem **Aguardando ativação pelo administrador da SD-WAN**, notifique o administrador do SD-WAN Orchestrator.
9. Para tarefas de administrador do SD-WAN Orchestrator, consulte a documentação do produtoSD-WAN Orchestrator.
10. Quando o administrador do SD-WAN Orchestrator terminar, a entrada SD-WAN em **Conexões de rede** fica verde, com a mensagem **Você pode criar catálogos usando essa conexão.**

Exibir detalhes da conexão SD-WAN

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Selecione **SD-WAN** se essa não for a única seleção.
3. Clique na conexão que você deseja exibir.

A tela inclui:

- **Details tab:** Informações que você especificou ao configurar a conexão.
- **Branch Connectivity tab:** nome, conectividade de nuvem, disponibilidade, camada de largura de banda, função e local para cada filial e MCN.

Excluir uma conexão SD-WAN

Antes de excluir uma conexão SD-WAN, remova todos os catálogos associados a ela. Consulte Delete a catalog.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Selecione SD-WAN se essa não for a única seleção.
3. Clique na conexão que você deseja excluir para expandir seus detalhes.
4. Na guia **Detalhes**, clique em **Excluir conexão**.
5. Confirme a exclusão.

Prévia técnica do Azure VPN

O recurso de VPN do Azure está disponível para visualização técnica.

Sobre as conexões de gateway VPN do Azure

Uma conexão de gateway VPN do Azure fornece um link de comunicação entre seus VDAs (desktops e aplicativos) do Azure gerenciados pela Citrix e os recursos da sua empresa, como redes locais ou recursos em outros locais de nuvem. Isso é semelhante à configuração e à conexão com uma filial remota.

A conectividade segura usa os protocolos padrão do setor Internet Protocol Security (IPsec) e Internet Key Exchange (IKE).

Durante o processo de criação da conexão:

- Você fornece informações que a Citrix usa para criar o gateway e a conexão.
- A Citrix cria um gateway de VPN do Azure baseado em rota site a site. O gateway VPN forma um túnel IPsec (Internet Protocol Security) direto entre a assinatura do Azure gerenciada pela Citrix e o dispositivo host da VPN.
- Depois que a Citrix cria o gateway e a conexão VPN do Azure, você atualiza a configuração, as regras de firewall e as tabelas de rotas da sua VPN. Para esse processo, você usa um endereço IP público fornecido pela Citrix e uma chave pré-compartilhada (PSK) fornecida para criar a conexão.

Um exemplo de conexão é ilustrado em Criar uma conexão de gateway VPN do Azure.

Você não precisa de sua própria assinatura do Azure para criar esse tipo de conexão.

Opcionalmente, você também pode usar rotas personalizadas com esse tipo de conexão.

Rotas personalizadas do gateway VPN do Azure

As rotas personalizadas ou definidas pelo usuário substituem as rotas padrão do sistema para direcionar o tráfego entre máquinas virtuais em suas redes e a Internet. Você pode usar rotas personalizadas se houver redes às quais se espera que os recursos do Citrix Virtual Apps and Desktops Standard acessem, mas não estejam diretamente conectadas por meio de um gateway VPN do Azure. Por exemplo, você pode criar uma rota personalizada que force o tráfego por meio de um dispositivo de rede para a Internet ou para uma sub-rede de rede local.

Quando você adiciona rotas personalizadas a uma conexão, essas rotas se aplicam a todas as máquinas que usam essa conexão.

Para usar rotas personalizadas:

- Você deve ter um gateway de rede virtual existente ou um dispositivo de rede, como o Citrix SD-WAN, em seu ambiente Citrix Virtual Apps and Desktops Standard.
- Ao adicionar rotas personalizadas, você deve atualizar as tabelas de rotas da sua empresa com as informações da VPN de destino para garantir a conectividade de ponta a ponta.
- As rotas personalizadas são exibidas na guia **Conexão > Rotas** na ordem em que são inseridas. Essa ordem de exibição não afeta a ordem em que as rotas são selecionadas.

Antes de usar rotas personalizadas, consulte o artigo da Microsoft Roteamento de tráfego de rede virtual para saber mais sobre como usar rotas personalizadas, tipos de próximo salto e como o Azure seleciona rotas para tráfego de saída.

Você pode adicionar rotas personalizadas ao criar uma conexão de gateway VPN do Azure ou a conexões existentes em seu ambiente de serviço.

Requisitos e preparação da conexão do gateway VPN do Azure

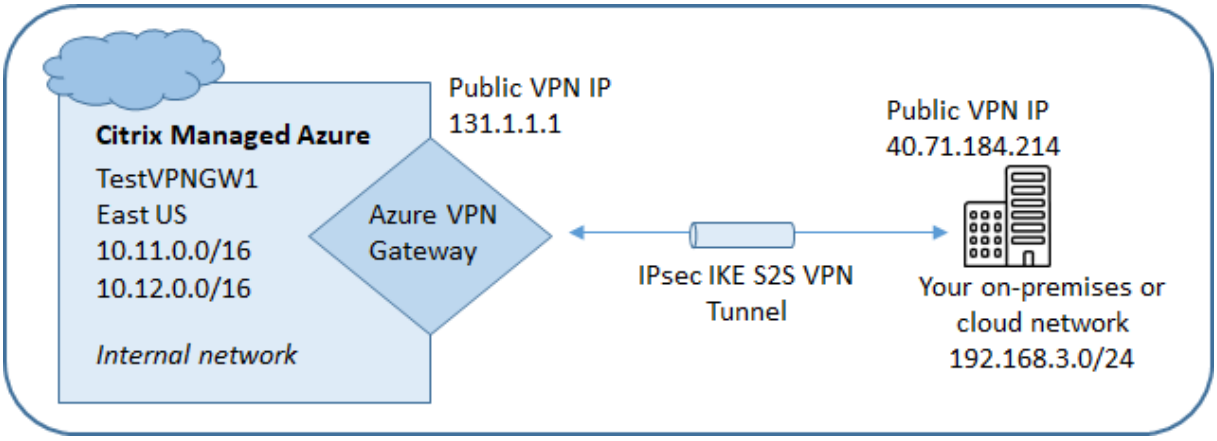
- Para saber mais sobre o Gateway VPN do Azure, consulte o artigo da Microsoft O que é o VPN Gateway?
- Analise os requisitos para todas as conexões de rede.
- Você deve ter uma VPN configurada. A rede virtual deve ser capaz de enviar e receber tráfego por meio do gateway VPN. Uma rede virtual não pode ser associada a mais de um gateway de rede virtual.

- Você deve ter um dispositivo IPsec que tenha um endereço IP público. Para saber mais sobre dispositivos VPN validados, consulte o artigo da Microsoft Sobre dispositivos VPN.
- Revise o procedimento Criar uma conexão do Gateway VPN do Azure antes de iniciá-lo, para que você possa coletar as informações de que precisa. Por exemplo, você precisará de endereços permitidos em sua rede, intervalos de IP para os VDAs e gateway, taxa de transferência e nível de desempenho desejados e endereços de servidor DNS.

Crie uma conexão de gateway VPN do Azure

Certifique-se de revisar esse procedimento antes de iniciá-lo.

O diagrama a seguir mostra um exemplo de configuração de uma conexão de gateway VPN do Azure. Geralmente, a Citrix gerencia os recursos no lado esquerdo do diagrama e você gerencia os recursos no lado direito. Algumas descrições no procedimento a seguir incluem referências aos exemplos do diagrama.



1. No painel **Gerenciar** no Citrix DaaS for Azure, expanda **Conexões de rede** à direita.
2. Clique em **Adicionar conexão**.
3. Clique em qualquer lugar na caixa **Gateway de VPN do Azure** .
4. Revise as informações na página **Adicionar conexão VPN** e clique em **Iniciar configuração de VPN**.
5. Na página **Adicionar uma conexão**, forneça as seguintes informações.
   - **Nome:** Um nome para a conexão. (No diagrama, o nome é TestVPNGW1.)
   - **Endereço IP da VPN:** Seu endereço IP voltado para o público.

     No diagrama, o endereço é 40.71.184.214.

- **Redes permitidas:** um ou mais intervalos de endereços que o serviço Citrix tem permissão para acessar em sua rede. Normalmente, esse intervalo de endereços contém os recursos que os usuários precisam acessar, como servidores de arquivos.

  Para adicionar mais de um intervalo, clique em **Adicionar mais endereços IP** e insira um valor. Repita conforme necessário.

  No diagrama, o intervalo de endereços é 192.168.3.0/24.

- **Chave pré-compartilhada:** um valor usado por ambas as extremidades da VPN para autenticação (semelhante a uma senha). Você decide qual é esse valor. Certifique-se de anotar o valor. Você precisará dele mais tarde quando configurar sua VPN com as informações de conexão.

- **Desempenho e taxa de transferência:** o nível de largura de banda a ser usado quando os usuários acessam recursos em sua rede.

  Todas as opções não suportam necessariamente o Border Gateway Protocol (BGP). Nesses casos, os campos de **configurações do BCP** não estão disponíveis.

- **Região: região** do Azure em que a Citrix implanta máquinas que fornecem áreas de trabalho e aplicativos (VDAs), quando você cria catálogos que usam essa conexão. Você não pode alterar essa seleção depois de criar a conexão. Se você decidir usar uma região diferente posteriormente, deverá criar ou usar outra conexão que especifique a região desejada.

  No diagrama, a região é EastUS.

- **Modo ativo-ativo (alta disponibilidade):** se dois gateways VPN são criados para alta disponibilidade. Quando esse modo está ativado, somente um gateway fica ativo por vez. Saiba mais sobre o gateway VPN do Azure ativo-ativo no documento da Microsoft Highly Available Cross-Premises Connectivity.

- **Configurações de BGP:** (Disponível somente se o **desempenho e a taxa de transferência** selecionados suportarem BGP.) Se usar o Border Gateway Protocol (BGP). Saiba mais sobre o BGP no documento da Microsoft: Sobre o BGP com o Gateway VPN do Azure. Se você habilitar o BGP, forneça as seguintes informações:

  - **Número de sistema autônomo (ASN):** os gateways de rede virtual do Azure recebem um ASN padrão de 65515. Uma conexão habilitada para BGP entre dois gateways de rede requer que seus ASNs sejam diferentes. Se necessário, você pode alterar o ASN agora ou depois que o gateway for criado.

  - **Endereço IP de peering de IP BGP:** o Azure oferece suporte a IP BGP no intervalo 169.254.21.*x* para 169.254.22.*x*.

- **Sub-rede VDA:** o intervalo de endereços em que os Citrix VDAs (máquinas que fornecem desktops e aplicativos) e os Cloud Connectors residirão quando você criar um catálogo

que usa essa conexão. Depois de inserir um endereço IP e selecionar uma máscara de rede, o intervalo de endereços é exibido, além de quantos endereços o intervalo suporta.

Embora esse intervalo de endereços seja mantido na assinatura do Azure gerenciada pela Citrix, ele funciona como se fosse uma extensão da sua rede.

- O intervalo de IP não deve sobrepor nenhum endereço que você usa em suas redes locais ou em outras redes de nuvem. Se os endereços se sobrepuserem, a conexão poderá não ser criada com êxito. Além disso, um endereço sobreposto não funcionará corretamente para tarefas de administração do site.
- O intervalo de sub-rede VDA deve ser diferente do endereço de sub-rede do gateway.
- Você não pode alterar esse valor depois de criar a conexão. Para usar um valor diferente, crie outra conexão.

No diagrama, a sub-rede VDA é 10.11.0.0/16.

- **Sub-rede do gateway:** o intervalo de endereços em que o gateway VPN do Azure residirá quando você criar um catálogo que usa essa conexão.
  - O intervalo de IP não deve sobrepor nenhum endereço que você usa em suas redes locais ou em outras redes de nuvem. Se os endereços se sobrepuserem, a conexão poderá não ser criada com êxito. Além disso, um endereço sobreposto não funcionará corretamente para tarefas de administração do site.
  - O intervalo de sub-rede do gateway deve ser diferente do endereço de sub-rede do VDA.
  - Você não pode alterar esse valor depois de criar a conexão. Para usar um valor diferente, crie outra conexão.

  No diagrama, a sub-rede do gateway é 10.12.0.9/16.
- **Rotas:** indique se você deseja adicionar rotas personalizadas à conexão. Se você quiser adicionar rotas personalizadas, forneça as seguintes informações:
  - Digite um nome amigável para a rota personalizada.
  - Insira o endereço IP de destino e o prefixo da rede. O prefixo da rede deve estar entre 16 e 24.
  - Selecione um tipo de próximo salto para onde você deseja que o tráfego seja roteado. Se você selecionar Equipamento **virtual, insira o endereço IP interno do equipamento. Para obter mais informações sobre os próximos tipos de salto, consulte Rotas personalizadas no artigo da Microsoft Roteamento de tráfego de rede virtual.

Para adicionar mais de uma rota, clique em **Adicionar rota** e insira as informações solicitadas.

- **Servidores DNS:** insira os endereços dos seus servidores DNS e indique o servidor preferido. Embora você possa alterar as entradas do servidor DNS posteriormente, lembre-se de que alterá-las pode causar problemas de conectividade para as máquinas em catálogos que usam essa conexão.

  Para adicionar mais de dois endereços de servidor DNS, clique em **Adicionar DNS alternativo** e insira as informações solicitadas.

6. Clique em **Criar conexão VPN**.

Depois que a Citrix cria a conexão, ela é listada em **Conexões de Rede > Gateway VPN do Azure** no painel **Gerenciar** no Citrix DaaS para Azure. A placa de conexão contém um endereço IP público. (No diagrama, o endereço é 131.1.1.1.)

- Use esse endereço (e a chave pré-compartilhada especificada ao criar a conexão) para configurar sua VPN e firewalls. Se você esqueceu sua chave pré-compartilhada, você pode alterá-la na página **Detalhes** da conexão. Você precisará da nova chave para configurar sua extremidade do gateway VPN.

  Por exemplo, permita exceções no firewall para os intervalos de endereços IP da sub-rede do VDA e do gateway que você configurou.

- Atualize as tabelas de rotas da sua empresa com as informações de conexão do gateway VPN do Azure para garantir a conectividade de ponta a ponta.

  No diagrama, novas rotas são necessárias para o tráfego que vai de 192.168.3.0/24 para 10.11.0.0/16 e 10.12.0.9/16 (as sub-redes VDA e gateway).

- Se você configurou rotas personalizadas, faça as atualizações apropriadas para elas também.

Quando ambas as extremidades da conexão são configuradas com êxito, a entrada da conexão em **Conexões de Rede > Gateway VPN do Azure** indica **Pronto para uso**.

Veja uma conexão de gateway VPN do Azure

1. No painel **Gerenciar** no Citrix DaaS for Azure, expanda **Conexões de rede** à direita.
2. Selecione a conexão que você deseja exibir.

   Monitores:

- A guia **Detalhes** mostra o número de catálogos, máquinas, imagens e bastiões que usam essa conexão. Ele também contém a maioria das informações que você configurou para essa conexão.
- A guia **Rotas** lista as informações de rota personalizadas para a conexão.

Gerenciar rotas personalizadas para uma conexão de gateway VPN do Azure

Em uma conexão de gateway VPN do Azure existente, você pode adicionar, modificar, desativar e excluir rotas personalizadas.

Para obter informações sobre como adicionar rotas personalizadas ao criar uma conexão, consulte Criar uma conexão de gateway VPN do Azure.

> **Importante:**
>
> modificar, desativar ou excluir rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper as sessões ativas do usuário.

1. No painel **Gerenciar** no Citrix DaaS for Azure, expanda **Conexões de rede** à direita.
2. Selecione a conexão que você deseja exibir.
   - Para adicionar uma rota personalizada:
     a) Na guia **Rotas** da conexão, clique em **Adicionar rota**.
     b) Digite um nome amigável, o endereço IP de destino e o prefixo e o próximo tipo de salto que você deseja usar. Se você selecionar **Virtual Appliance** como o tipo de salto seguinte, digite o endereço IP interno do equipamento.
     c) Indique se você deseja ativar a rota personalizada. Por padrão, a rota personalizada está ativada.
     d) Clique em **Adicionar rota**.
   - Para modificar ou ativar/desativar uma rota personalizada:
     a) Na guia **Rotas** da conexão, localize a rota personalizada que você deseja gerenciar.
     b) No menu de reticências, selecione **Editar**.
     c) Altere o endereço IP e o prefixo de destino ou o tipo de próximo salto, conforme necessário.
     d) Indique se você deseja ativar a rota.
     e) Clique em **Save**.
   - Para excluir uma rota personalizada:
     a) Na guia **Rotas** da conexão, localize a rota personalizada que você deseja gerenciar.
     b) No menu de reticências, selecione **Excluir**.
     c) Selecione **Excluir uma rota pode interromper as sessões ativas** para reconhecer o impacto da exclusão da rota personalizada.
     d) Clique em **Excluir rota**.

Redefinir ou excluir uma conexão de gateway VPN do Azure

> **Importante:**
>
> - A redefinição de uma conexão faz com que a conexão atual seja perdida e ambas as extremidades devem restabelecê-la. Uma redefinição interrompe as sessões ativas do usuário.
> - Antes de excluir uma conexão, exclua todos os catálogos que a utilizam. Consulte Delete a catalog.

Para redefinir ou excluir uma conexão:

1. No painel **Gerenciar** no Citrix DaaS for Azure, expanda **Conexões de rede** à direita.
2. Selecione a conexão que você deseja redefinir ou excluir.
3. Na guia **Detalhes** da conexão:
   - Para redefinir a conexão, clique em **Redefinir conexão**.
   - Para excluir a conexão, clique em **Excluir conexão**.
4. Se solicitado, confirme a ação.

Crie um endereço IP estático público

Se você quiser que todos os VDAs de máquinas em uma conexão usem um único endereço IP estático público de saída (gateway) para a Internet, habilite um gateway NAT. Você pode habilitar um gateway NAT para conexões com catálogos que ingressaram no domínio ou não ingressaram no domínio.

Para habilitar um gateway NAT para uma conexão:

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Em **Conexões de rede**, selecione uma conexão em **CITRIX MANAGED** ou **AZURE VNET PEERINGS**.
3. No cartão de detalhes da conexão, clique em **Ativar gateway NAT**.
4. Na página Ativar gateway NAT, mova o controle deslizante para **Sim** e configure um tempo ocioso.
5. Clique em **Confirmar alterações**.

Quando você ativa um gateway NAT:

- O Azure atribui um endereço IP estático público ao gateway automaticamente. (Você não pode especificar esse endereço.) Todos os VDAs em todos os catálogos que usam essa conexão usarão esse endereço para conectividade de saída.

- Você pode especificar um valor de tempo limite ocioso. Esse valor indica o número de minutos que uma conexão de saída aberta através do gateway NAT pode permanecer ociosa antes que a conexão seja fechada.
- Você deve permitir o endereço IP estático público em seu firewall.

Você pode voltar para a placa de detalhes da conexão para habilitar ou desabilitar o gateway NAT e alterar o valor do tempo limite.

Imagens

July 17, 2024

Quando você cria um catálogo para entregar áreas de trabalho ou aplicativos, uma imagem é usada (com outras configurações) como um modelo para criar as máquinas.

Imagens preparadas pela Citrix

O Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure) fornece várias imagens preparadas pela Citrix:

- Windows 11 Pro (sessão única)
- Área de trabalho virtual do Windows 11 Enterprise (multissessão)
- Área de trabalho virtual do Windows 11 Enterprise (várias sessões) com Office 365 ProPlus
- Windows 10 Pro (sessão única)
- Área de trabalho virtual do Windows 10 Enterprise (multissessão)
- Área de Trabalho Virtual do Windows 10 Enterprise (multissessão) com o Office 365 ProPlus
- Windows Server 2022 (várias sessões)
- Windows Server 2019 (várias sessões)
- Windows Server 2016 (várias sessões)
- Linux Ubuntu 22.04 LTS (sessão única)
- Linux Ubuntu 22.04 LTS (várias sessões)

As imagens preparadas pela Citrix têm um Citrix Virtual Delivery Agent (VDA) atual e ferramentas de solução de problemas instaladas. O VDA é o mecanismo de comunicação entre as máquinas dos seus usuários e a infraestrutura do Citrix Cloud que gerencia o Citrix DaaS para Azure. As imagens fornecidas pela Citrix são notadas como **CITRIX**.

Você também pode importar e usar sua própria imagem do Azure.

Formas de usar imagens

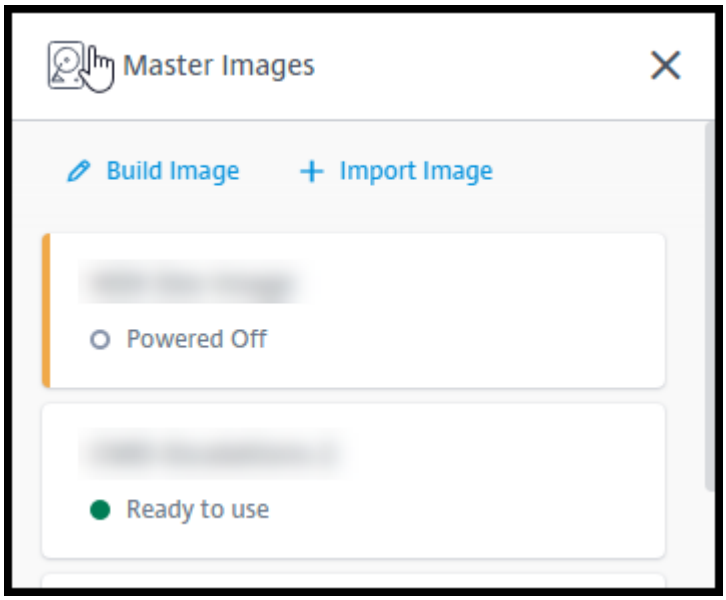
Você pode:

- **Use a Citrix prepared image when creating a catalog.** Essa opção é recomendada somente para implantações de prova de conceito.
- **Use a Citrix prepared image to create another image.** Depois que a nova imagem é criada, você a personaliza adicionando aplicativos e outros softwares de que seus usuários precisam. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.
- **Import an image from Azure.** Depois de importar uma imagem do Azure, você pode usar essa imagem ao criar um catálogo. Ou você pode usar essa imagem para criar uma nova imagem e personalizá-la adicionando aplicativos. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.

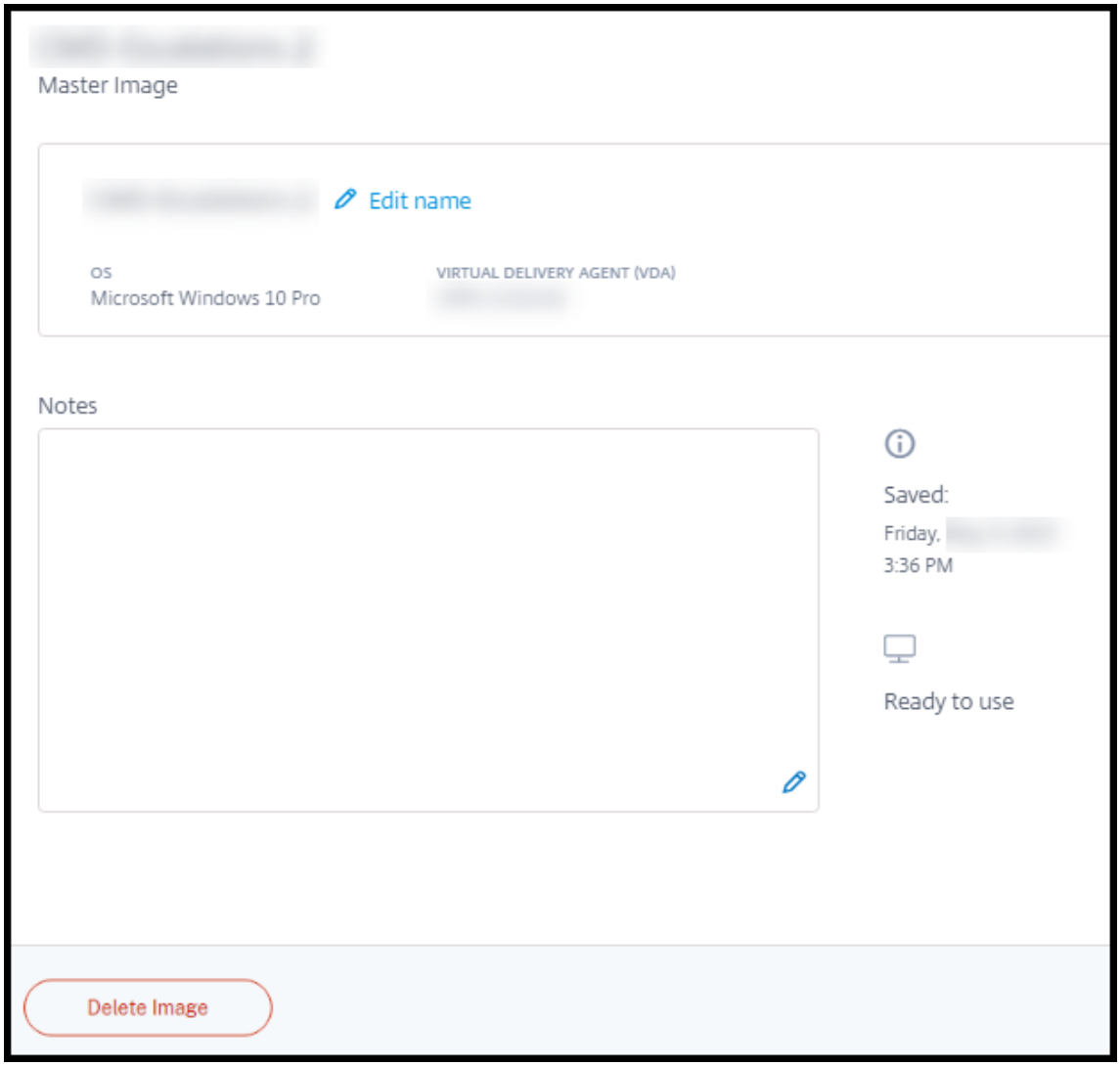
Quando você cria um catálogo, o Citrix DaaS for Azure verifica se a imagem usa um sistema operacional válido e tem um Citrix VDA e ferramentas de solução de problemas instalados (junto com outras verificações).

Exibir informações da imagem

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita. A tela lista as imagens que a Citrix fornece e as imagens que você criou e importou.



2. Clique em uma imagem para exibir seus detalhes.



No cartão de detalhes, você pode:

- Altere (edite) o nome da imagem.
- Adicione e edite notas (Disponível apenas para imagens que você preparou ou importou, não imagens fornecidas pela Citrix).
- Exclua a imagem.

Preparar uma nova imagem

Preparar uma nova imagem inclui a criação e personalização da imagem. Quando você cria uma imagem, uma nova VM é criada para carregar a nova imagem.

Requisitos:

- Conheça as características de desempenho de que as máquinas precisam. Por exemplo, a exe-

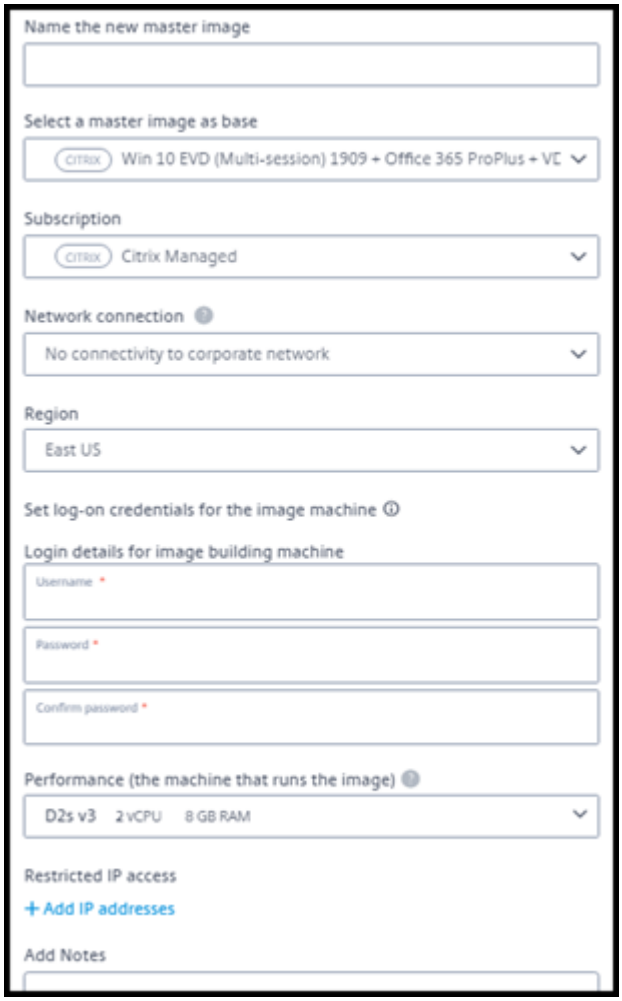
cução de aplicativos CAD pode exigir CPU, RAM e armazenamento diferentes dos outros aplicativos de escritório.
- Se você planeja usar uma conexão com seus recursos locais, configure essa conexão antes de criar a imagem e o catálogo. Para obter detalhes, consulte Network connections.

Ao usar uma imagem do Ubuntu preparada pela Citrix para criar uma nova imagem, é criada uma senha root para a nova imagem. Você pode alterar essa senha de root, mas somente durante o processo de criação e personalização da imagem. (Você não pode alterar a senha root depois que a imagem for usada em um catálogo.)

- Quando a imagem é criada, a conta de administrador que você especificou (**Login details for image building machine**) é adicionada ao grupo `sudoers`.
- Depois de fazer o RDP para a máquina que contém a nova imagem, inicie o aplicativo de terminal e digite `sudo passwd root`. Quando solicitado, forneça a senha especificada ao criar a imagem. Após a verificação, você será solicitado a inserir uma nova senha para o usuário root.

Para criar uma imagem:

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita.
2. Clique em **Criar imagem**.



3. Insira valores nos seguintes campos:

   - **Name:** insira um nome para a nova imagem.
   - **Master image:** selecione uma imagem existente. Essa é a imagem base usada para criar a nova imagem.
   - **Assinatura:** Selecione uma assinatura do Azure. Para obter detalhes, consulte Assinaturas do Azure.
   - **Conexão de rede:**
     - Se estiver usando uma assinatura do Citrix Managed Azure, selecione **No connectivity** ou uma conexão criada anteriormente.
     - Se estiver usando sua própria assinatura do Azure gerenciada pelo cliente, selecione seu grupo de recursos, rede virtual e sub-rede. Em seguida, adicione os detalhes do domínio: FQDN, OU, nome da conta de serviço e credenciais.
   - **Configuração do domínio:** selecione o tipo de domínio: Active Directory ou não ingressado no domínio.

  - Se você selecionar Active Directory, selecione ou adicione um domínio. Especifique uma OU (opcional), nome da conta de serviço e senha.
  - Se você selecionar não ingressado no domínio, nenhuma informação adicional será necessária.

- **Região:** (Disponível apenas para **Sem conectividade**.) Selecione uma região onde você deseja que a máquina que contém a imagem seja criada.
- **Logon credentials for image machine:** você usará essas credenciais mais tarde quando se conectar (RDP) à máquina que contém a nova imagem, para que você possa instalar aplicativos e outros softwares.
- **Machine performance:** são informações de CPU, RAM e armazenamento da máquina que executa a imagem. Selecione um desempenho de máquina que atenda aos requisitos dos seus aplicativos.
- **Acesso IP restrito:** Se você quiser restringir o acesso a endereços específicos, selecione **Adicionar endereços IP** e insira um ou mais endereços. Depois de adicionar os endereços, clique em **Concluído** para retornar ao cartão **Criar imagem**.
- **Notas:** Opcionalmente, adicione até 1024 caracteres de notas. Depois que a imagem é criada, você pode atualizar as notas na exibição de detalhes da imagem.
- **Ingresso no domínio local:** indique se você deseja ingressar no domínio local do Active Directory.
  - Se você selecionar **Sim**, insira as informações do Azure: FQDN, OU, nome da conta de serviço e credenciais.
  - Se você selecionar **Não**, insira as credenciais da máquina host.

4. Quando terminar, clique em **Criar imagem**.

Uma imagem pode levar até 30 minutos para ser criada. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita para ver o estado atual (como **Imagem de construção** ou **Pronto para personalizar**).

O que fazer a seguir: conectar-se a uma nova imagem e personalizá-la.

Conecte-se a uma nova imagem e personalize-a

Depois que uma nova imagem é criada, seu nome é adicionado à lista de imagens, com um status de **Pronto para personalizar** (ou palavras semelhantes). Para personalizar essa imagem, você primeiro faz o download de um arquivo RDP. Ao usar esse arquivo para se conectar à imagem, você pode adicionar aplicativos e outros softwares à imagem.

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita. Clique na imagem à qual você deseja se conectar.
2. Clique em **Baixar arquivo RDP**. Um cliente RDP faz o download.

   A máquina de imagem pode se desligar se você não fizer uma conexão por RDP a ela logo após sua criação. Isso economiza custos. Quando isso acontecer, clique em **Ligar**.
3. Clique duas vezes no cliente RDP baixado. Ele tenta se conectar automaticamente ao endereço da máquina que contém a nova imagem. Quando solicitado, insira as credenciais especificadas ao criar a imagem.
4. Depois de se conectar à máquina, adicione ou remova aplicativos, instale atualizações e conclua qualquer outro trabalho de personalização.

   NÃO use Sysprep na imagem.
5. Quando terminar de personalizar a nova imagem, volte para a caixa **Imagens mestras** e clique em **Concluir compilação**. A nova imagem passa automaticamente por testes de validação.

Mais tarde, quando você cria um catálogo, a nova imagem é incluída na lista de imagens que você pode selecionar.

No painel **Gerenciar > Implantação rápida**, as imagens exibidas à direita indicam quantos catálogos e máquinas usam cada imagem.

> **Nota:**
>
> Depois de finalizar uma imagem, você não poderá editá-la. Você deve criar uma nova imagem (usando a imagem anterior como ponto de partida) e, em seguida, atualizar a nova imagem.

Importar uma imagem do Azure

Ao importar uma imagem do Azure que tenha um Citrix VDA e aplicativos de que seus usuários precisam, você pode usá-la para criar um catálogo ou substituir a imagem em um catálogo existente.

Requisitos de imagem importada

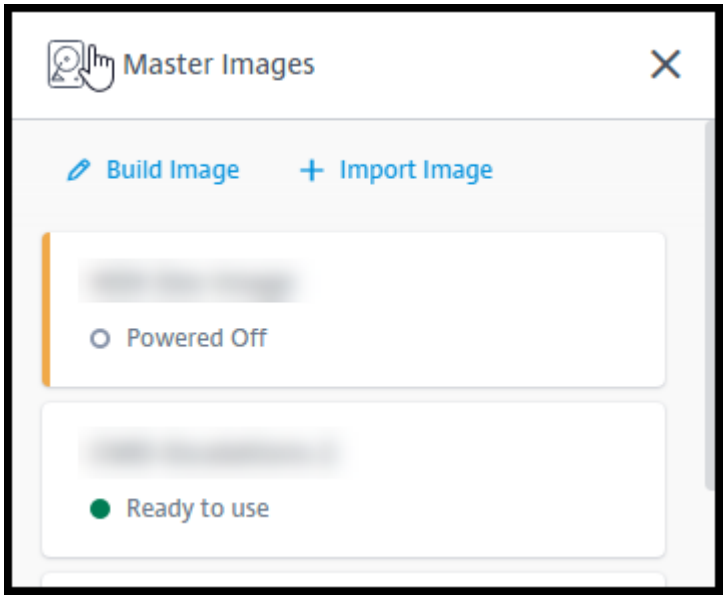
A Citrix executa testes de validação na imagem importada. Certifique-se de que os seguintes requisitos sejam atendidos ao preparar a imagem que você importará para o Citrix DaaS para Azure.

- **SO suportado:** A imagem deve ser um sistema operacional compatível. Para verificar uma versão do sistema operacional Windows, execute `Get-WmiObject Win32_OperatingSystem`.

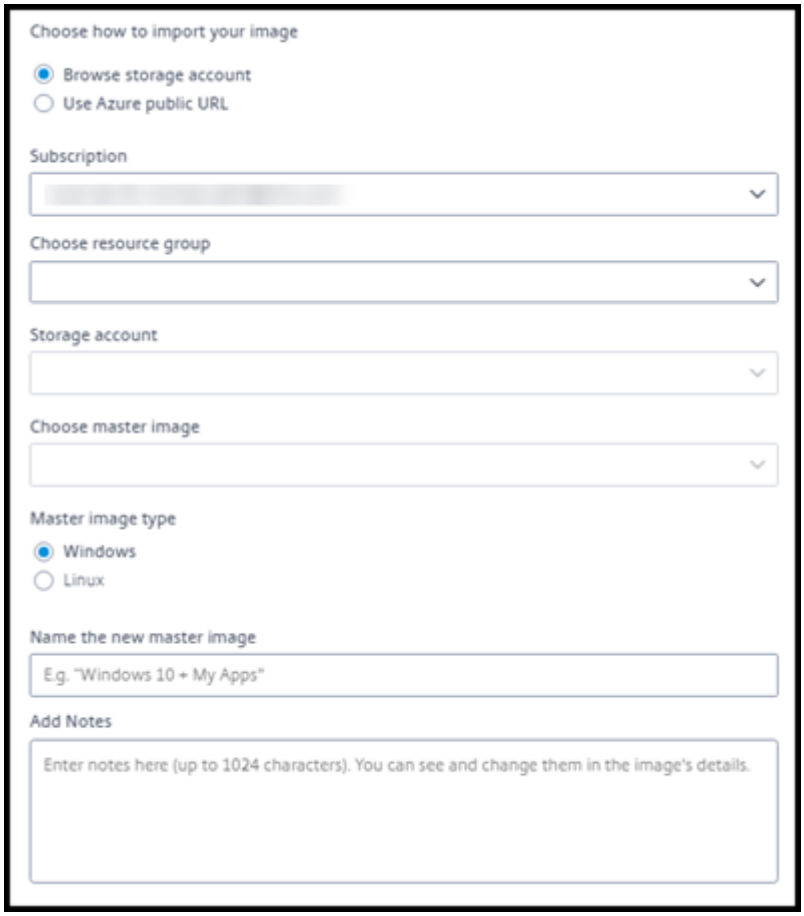
- **Supported generation:** as máquinas virtuais da geração 1 oferecem suporte à maioria dos sistemas operacionais convidados. As máquinas virtuais de segunda geração oferecem suporte à maioria das versões de 64 bits do Windows e à versão mais atual dos sistemas operacionais Linux.
- **Not generalized:** a imagem não deve ser generalizada.
- **No configured Delivery Controllers:** nenhum Citrix Delivery Controller deve estar configurado na imagem. As chaves de registro a seguir devem estar limpas.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini file:** o arquivo `personality.ini` deve existir na unidade do sistema.
- **Valid VDA:** a imagem deve ter um Citrix VDA mais recente que 7.11 instalado.
  - Windows: Para verificar, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Para obter orientações sobre instalação, consulte Instalar um VDA do Windows em uma imagem.
  - Red Hat Enterprise Linux e Ubuntu: Para obter orientações de instalação, consulte a documentação do produto.
- **Azure Virtual Machine Agent:** Antes de importar uma imagem, verifique se o Azure Virtual Machine Agent está instalado na imagem. Para obter mais informações, consulte o artigo da Microsoft Visão geral do Azure Virtual Machine Agent.

Importe a imagem

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita.



2. Clique em **Importar imagem**.



3. Escolha como importar a imagem.

   - No caso de discos gerenciados, use o recurso de exportação para gerar um URL de SAS.

Defina o tempo de expiração como 7200 segundos ou mais.

- No caso de VHDs em uma conta de armazenamento, escolha uma das seguintes opções:
  - Gerar um URL SAS para o arquivo VHD.
  - Atualizar o nível de acesso de um contêiner de armazenamento em bloco para blob ou contêiner. Em seguida, obtenha o URL do arquivo.

4. Se você selecionou **Browse storage account**:

   a) Selecione sequencialmente uma assinatura > grupo de recursos > conta de armazenamento > imagem.
   b) Dê um nome à imagem.

5. Se você selecionou a **Azure public URL**:

   a) Insira o URL gerado pelo Azure para o VHD. Para obter orientação, clique no link para o documento da Microsoft Baixar um VHD do Windows do Azure.
   b) Selecione uma assinatura. (Uma imagem do Linux só pode ser importada se você selecionar uma assinatura gerenciada pelo cliente.)
   c) Dê um nome à imagem.

6. Quando terminar, clique em **Importar imagem**.

Atualize um catálogo com uma nova imagem

O tipo de catálogo determina quais máquinas são atualizadas quando você atualiza o catálogo.

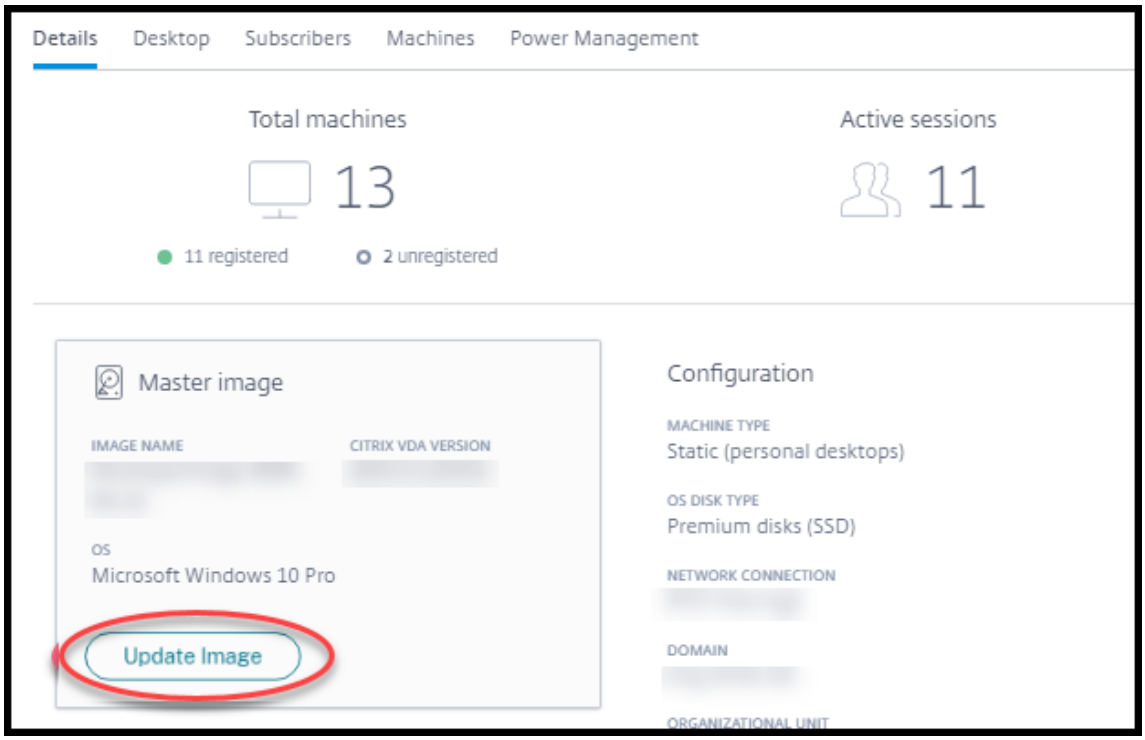
- No caso de um catálogo aleatório, todas as máquinas atualmente no catálogo são atualizadas com a imagem mais recente. Se você adicionar mais áreas de trabalho a esse catálogo, elas serão baseadas na imagem mais recente.
- No caso de um catálogo estático, as máquinas atualmente no catálogo não são atualizadas com a imagem mais recente. As máquinas atualmente contidas no catálogo continuam usando a imagem a partir da qual foram criadas. No entanto, se você adicionar mais máquinas a esse catálogo, elas serão baseadas na imagem mais recente.

Você pode atualizar um catálogo contendo máquinas com imagens gen1 com uma imagem gen2, se as máquinas do catálogo suportarem gen2. Da mesma forma, você pode atualizar um catálogo contendo máquinas gen2 com uma imagem gen1, se as máquinas do catálogo oferecerem suporte a gen1.

Para atualizar um catálogo com uma nova imagem:

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.

2. Na guia **Detalhes**, clique em **Atualizar imagem**.



3. Selecione uma imagem.
4. Para catálogos aleatórios ou com várias sessões: selecione um intervalo de logoff. Depois que o Citrix DaaS for Azure concluir o processamento inicial da imagem, os assinantes recebem um aviso para salvar seu trabalho e fazer logoff de seus desktops. O intervalo de logoff indica quanto tempo os assinantes têm depois de receber a mensagem até que a sessão termine automaticamente.
5. Clique em **Atualizar imagem**.

Excluir uma imagem

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Imagens Mestres** à direita.
2. Clique na imagem que você deseja excluir.
3. Clique em **Excluir imagem** na parte inferior do cartão. Confirme a exclusão.

Instale um Windows VDA em uma imagem

Use o procedimento a seguir ao preparar uma imagem do Windows que você planeja importar para o Citrix DaaS for Azure. Para obter orientações de instalação do Linux VDA, consulte a documentação do produto Linux VDA.

1. No seu ambiente do Azure, conecte-se à VM de imagem (se você ainda não estiver conectado).
2. Você pode baixar um VDA usando o link **Downloads** na barra de navegação do Citrix Cloud. Ou use um navegador para navegar até a página de download do Citrix DaaS for Azure.

   Baixe um VDA para a VM. Existem pacotes de download de VDA separados para um sistema operacional de desktop (sessão única) e um sistema operacional de servidor (multissessão).
3. Inicie o instalador do VDA clicando duas vezes no arquivo baixado. O assistente de instalação é iniciado.
4. Na página **Ambiente**, selecione a opção para criar uma imagem usando o MCS e clique em **Avançar**.
5. Na página **Componentes principais**, clique em **Avançar**.
6. Na página **Delivery Controller**, selecione **Permitir que os Serviços de Criação de Máquinas façam isso automaticamente** e clique em **Avançar**.
7. Deixe as configurações padrão nas páginas **Componentes adicionais**, **Recursos**e **Firewall**, a menos que a Citrix instrua o contrário. Clique em **Avançar** em cada página.
8. Na página **Resumo**, clique em **Instalar**. Os pré-requisitos começam a ser instalados. Quando solicitado a reiniciar, concorde.
9. A instalação do VDA é retomada automaticamente. A instalação de pré-requisito é concluída e, em seguida, os componentes e recursos são instalados. Na página **Call Home**, deixe a configuração padrão (a menos que a Citrix instrua o contrário). Depois de se conectar, clique em **Avançar**.
10. Clique em **Finish**. A máquina é reiniciada automaticamente.
11. Para garantir que a configuração esteja correta, inicie um ou mais dos aplicativos que você instalou na VM.
12. Desligue a VM. Não aplique Sysprep à imagem.

Para obter mais informações sobre a instalação de VDAs, consulte Install VDAs.

Usuários e autenticação

December 28, 2023

Métodos de autenticação do usuário

Os usuários devem se autenticar ao fazer login no Citrix Workspace para iniciar a área de trabalho ou os aplicativos.

O Citrix DaaS for Azure oferece suporte aos seguintes métodos de autenticação de usuário:

- **Azure AD gerenciado:** O Azure AD gerenciado é um Azure Active Directory (AAD) fornecido e gerenciado pela Citrix. Você não precisa fornecer sua própria estrutura do Active Directory. Basta adicionar seus usuários ao diretório.
- **Seu provedor de identidade:** você pode usar qualquer método de autenticação disponível no Citrix Cloud.

> **Nota:**
>
> - As implantações do Remote PC Access usam somente o Active Directory. Para obter detalhes, consulte Remote PC Access.
> - Se você usa o Azure AD Domain Services: os UPNs de logon do Workspace devem conter o nome de domínio que foi especificado ao habilitar o Azure AD Domain Services. Logons não podem usar UPNs em domínios que você personaliza, mesmo que o domínio personalizado seja designado como primário.

A configuração da autenticação do usuário inclui os seguintes procedimentos:

1. Configure o método de autenticação do usuário no Citrix Cloud e Workspace Configuration.
2. Se você estiver usando o Managed Azure AD para autenticação de usuário, adicione usuários ao diretório.
3. Adicione usuários a um catálogo.

Configurar a autenticação do usuário no Citrix Cloud

Para configurar a autenticação do usuário no Citrix Cloud:

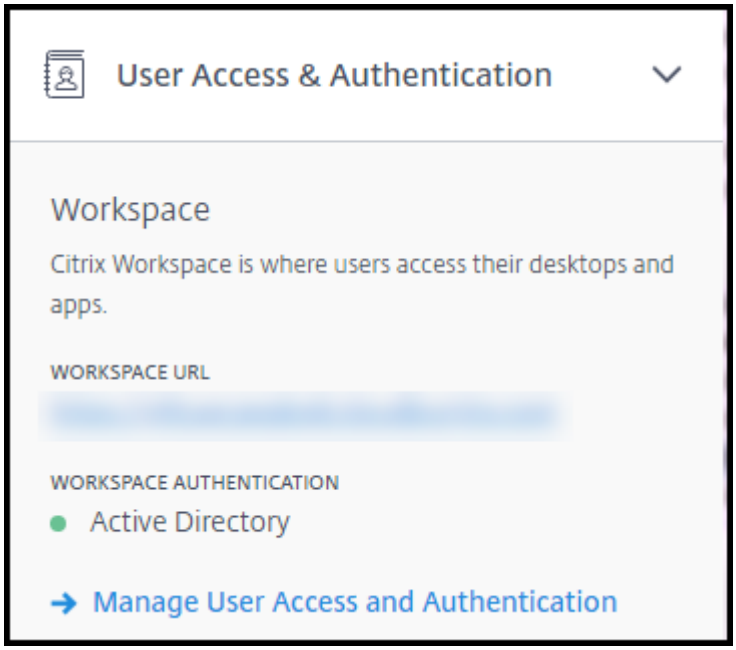
- Conecte-se ao método de autenticação do usuário que deseja usar. (No Citrix Cloud, você se “conecta”ou “desconecta”de um método de autenticação.)
- No Citrix Cloud, defina a autenticação do espaço de trabalho para usar o método conectado.

> **Nota:**
>
> O método de autenticação do Azure AD gerenciado é configurado por padrão. Ou seja, ele é conectado automaticamente no Citrix Cloud e a autenticação do Workspace é automaticamente definida para usar o Managed Azure AD for Citrix DaaS for Azure. Se você quiser usar esse método (e não tiver configurado um método diferente anteriormente), continue com Adicionar e excluir

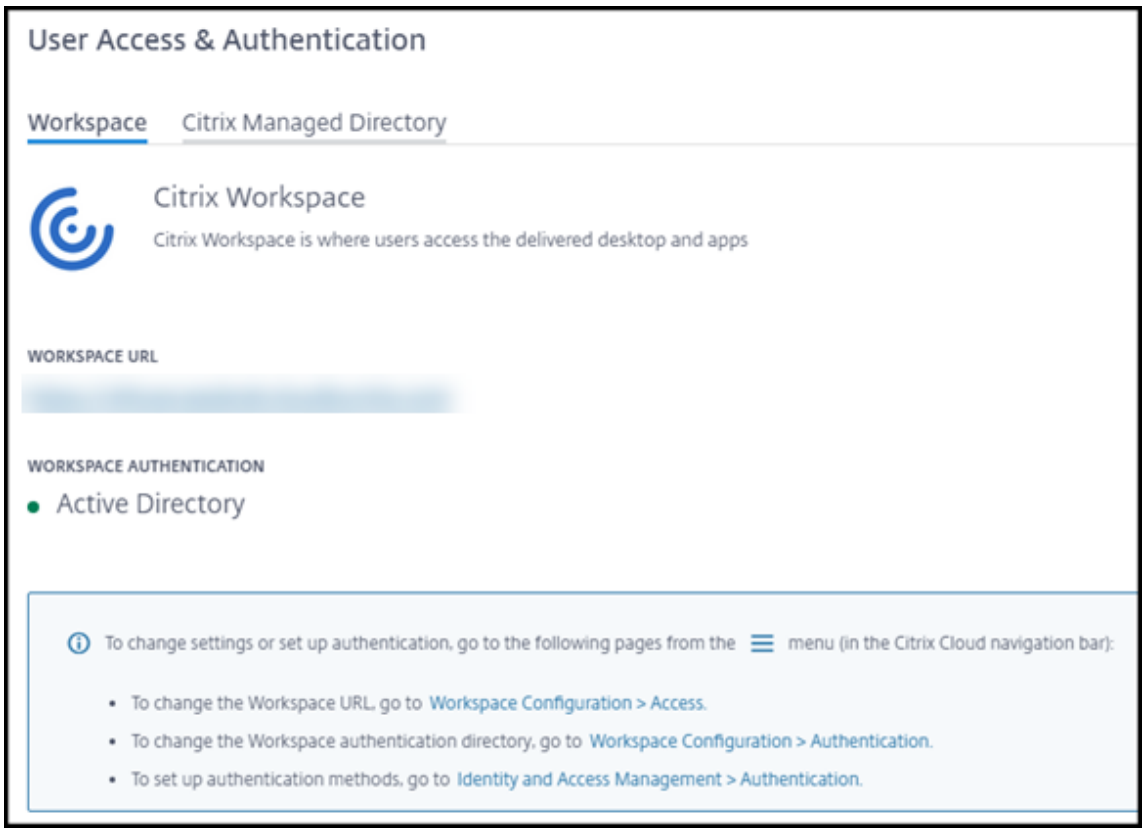
> usuários no Managed Azure AD.
> Se o Managed Azure AD for desconectado, a autenticação do Workspace será transferida para o Active Directory. Se você quiser usar um método de autenticação diferente, siga as etapas abaixo.

Para alterar o método de autenticação:

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, clique em **Acesso e Autenticação do Usuário** à direita.



2. Clique em **Gerenciar acesso e autenticação do usuário**. Selecione a guia **Espaço de trabalho**, se ela ainda não estiver selecionada. (A outra guia indica qual método de autenticação de usuário está configurado no momento.)



3. Siga o link **To set up authentication methods**. O link leva você ao Citrix Cloud. No menu de reticências, selecione **Connect** para o método desejado.
4. Enquanto ainda estiver no Citrix Cloud, selecione **Workspace Configuration** no menu superior esquerdo. Na guia **Authentication**, selecione o método desejado.

O que fazer a seguir:

- Se estiver usando o Managed Azure AD, adicione usuários ao diretório.
- Para todos os métodos de autenticação, adicione usuários ao catálogo.

Adicionar e excluir usuários no Managed Azure AD

Siga este procedimento somente se estiver usando o Managed Azure AD para autenticação do usuário no Citrix Workspace.

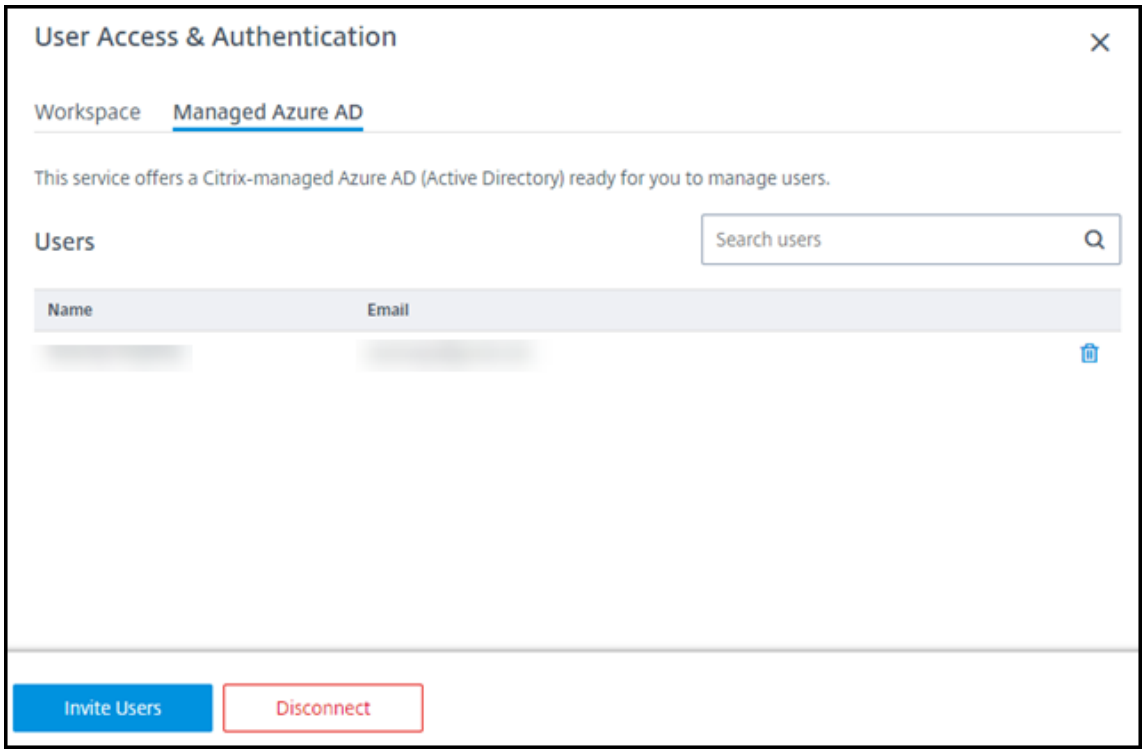
Você fornece o nome e o endereço de e-mail de seus usuários. Em seguida, a Citrix envia um convite por e-mail para cada um deles. O e-mail instrui os usuários a clicar em um link que os une ao Citrix Managed Azure AD.

- Se o usuário já tiver uma conta da Microsoft com o endereço de e-mail que você forneceu, essa conta será usada.

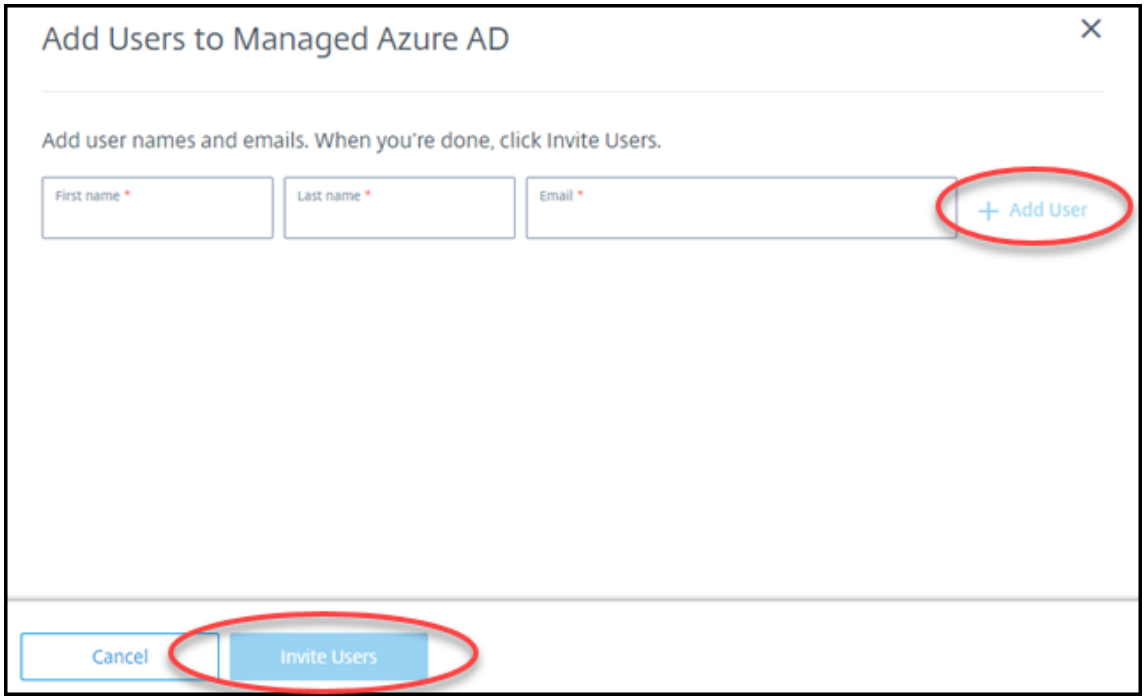
- Se o usuário não tiver uma conta da Microsoft com o endereço de e-mail, a Microsoft criará uma conta.

Para adicionar e convidar usuários para o Managed Azure AD:

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Acesso e Autenticação do Usuário** à direita. Clique em **Gerenciar acesso e autenticação do usuário**.
2. Clique na guia **Managed Azure AD**.
3. Clique em **Convidar usuários**.



4. Digite o nome e o endereço de e-mail de um usuário e clique em **Adicionar usuário**.



5. Repita a etapa anterior para adicionar outros usuários.
6. Quando terminar de adicionar as informações do usuário, clique em **Convidar usuários** na parte inferior do cartão.

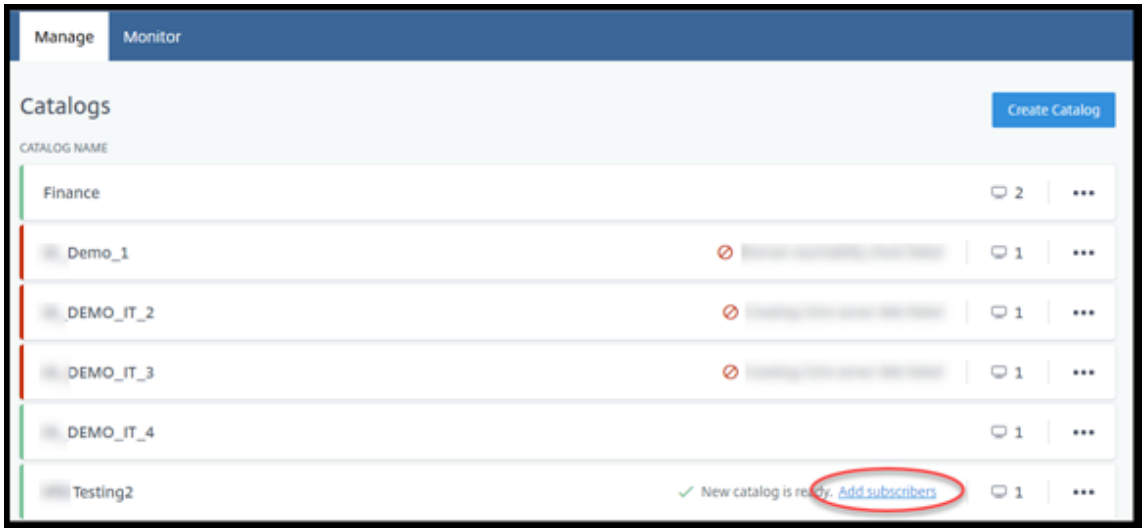
Para excluir um usuário do Managed Azure AD, clique no ícone de lixeira ao lado do nome do usuário que você deseja excluir do diretório. Confirme a exclusão.

O que fazer a seguir: Adicionar usuários ao catálogo

Adicionar ou remover usuários em um catálogo

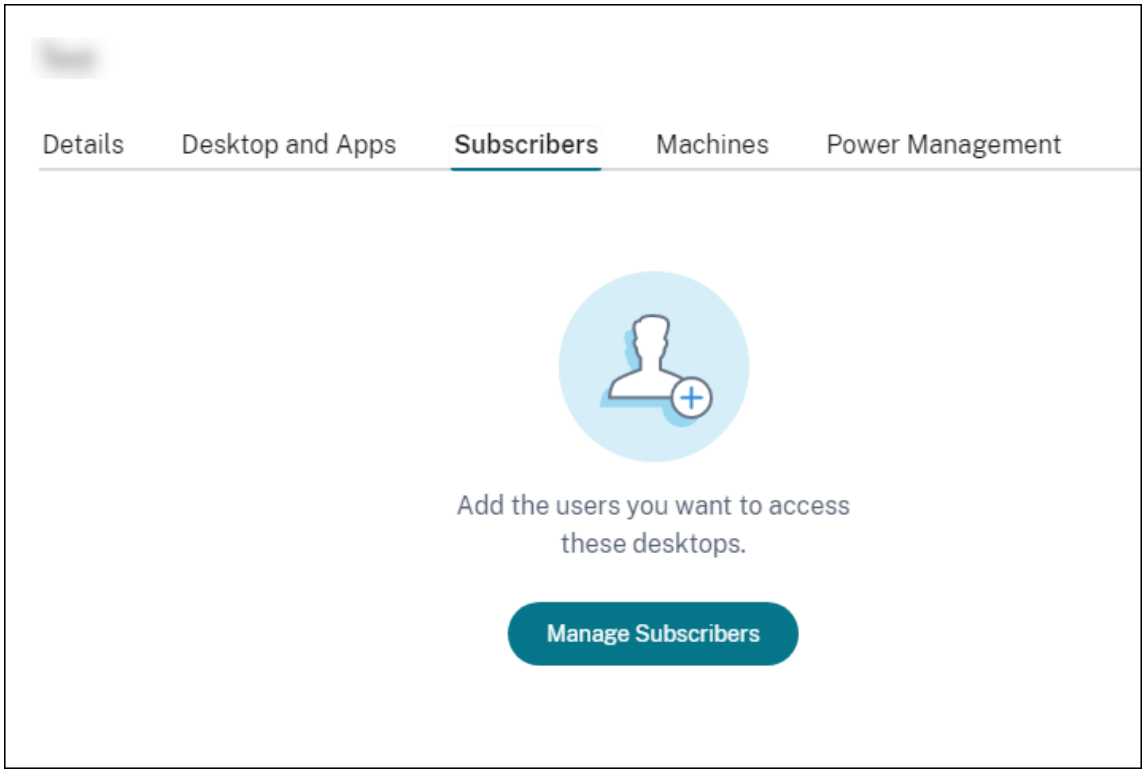
Conclua este procedimento independentemente do método de autenticação usado.

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, se você não tiver adicionado nenhum usuário a um catálogo, clique em **Adicionar assinantes**.

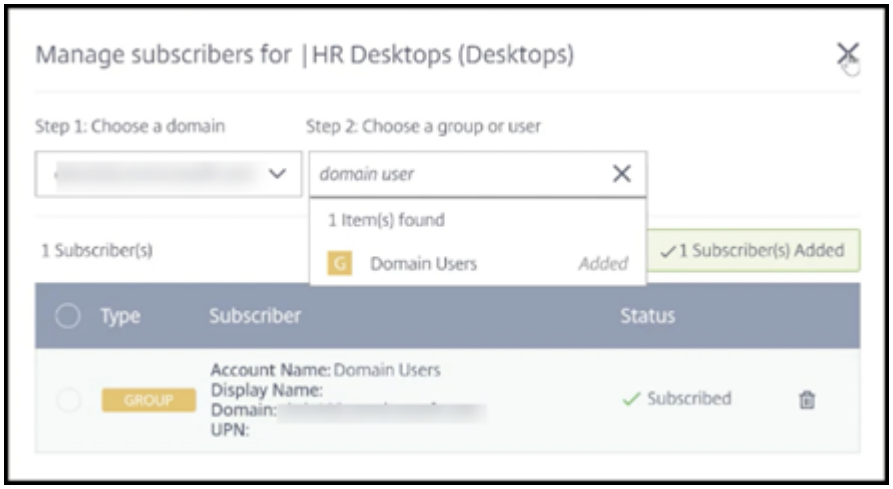


Para adicionar usuários a um catálogo que já tem usuários, clique em qualquer lugar na entrada do catálogo.

2. Na guia **Assinantes**, clique em **Gerenciar assinantes**.



3. Selecione um domínio. (Se você estiver usando o Managed Azure AD para autenticação de usuário, há apenas uma entrada no campo de domínio.) Em seguida, selecione um usuário.



4. Selecione outros usuários, conforme necessário. Quando terminar, clique no **X** no canto superior direito.

Para remover usuários de um catálogo, siga as etapas 1 e 2. Na etapa 3, clique no ícone da lixeira ao lado do nome que você deseja excluir (em vez de selecionar um domínio e um grupo/usuário). Essa ação remove o usuário do catálogo, não da origem (como o Managed Azure AD ou seu próprio AD ou AAD).

O que fazer a seguir:

- Para um catálogo com máquinas multissessão, adicione aplicativos, se ainda não o fez.
- Para todos os catálogos, envie o URL do Citrix Workspace para seus usuários.

Mais informações

Para obter mais informações sobre autenticação no Citrix Cloud, consulte Gerenciamento de identidade e acesso.

Gerenciar catálogos

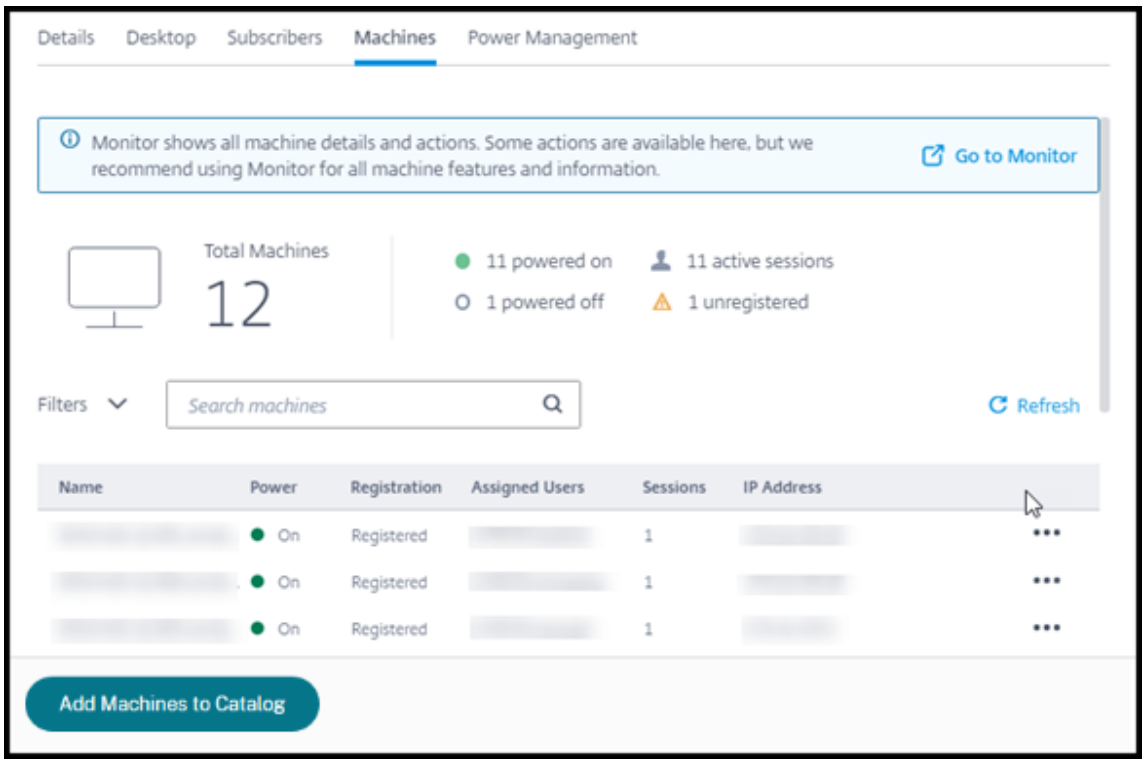
July 17, 2024

> **Nota:**
>
> Este artigo descreve as tarefas que você pode usar para gerenciar catálogos que foram criados na interface Quick Deploy. Para obter informações sobre o gerenciamento de catálogos usando a interface de gerenciamento Configuração Completa, consulte Gerenciar catálogos de máquinas.

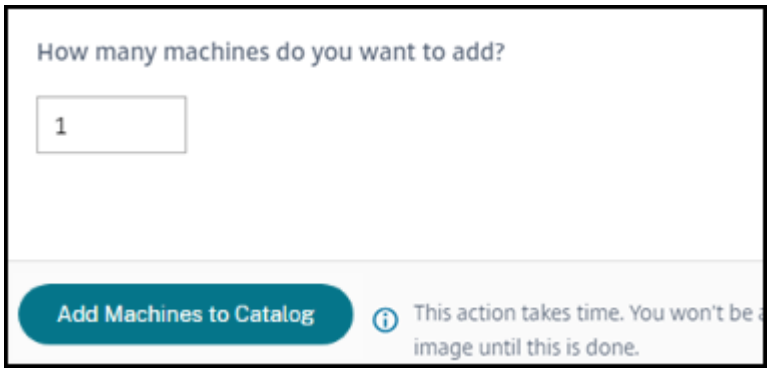
Adicionar máquinas a um catálogo

Enquanto as máquinas estão sendo adicionadas a um catálogo, você não pode fazer outras alterações nesse catálogo.

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Máquinas**, clique em **Adicionar máquinas ao catálogo**.



3. Insira o número de máquinas que você deseja adicionar ao catálogo.



4. (Válido somente se o catálogo for ingressado no domínio.) Digite o nome de usuário e a senha da conta de serviço.
5. Clique em **Adicionar máquinas ao catálogo**.

Você não pode reduzir a contagem de máquinas para um catálogo. No entanto, você pode usar as configurações de programação de gerenciamento de energia para controlar quantas máquinas estão ligadas ou excluir máquinas da guia **Machines**. Consulte Manage machines in a catalog para obter informações sobre como excluir máquinas na guia **Machines**.

Alterar o número de sessões por máquina

Alterar o número de sessões por máquina com várias sessões pode ter influência na experiência dos usuários. Aumentar esse valor pode reduzir os recursos computacionais alocados para sessões simultâneas. Recomendação: observe seus dados de uso para determinar o equilíbrio adequado entre a experiência do usuário e o custo.

1. No painel **Gerenciar > Implantação Rápida do Azure**, selecione um catálogo contendo máquinas com várias sessões.
2. Na guia **Detalhes**, clique em **Editar** ao lado de **Sessões por máquina**.
3. Insira um novo número de sessões por máquina.
4. Clique em **Atualizar número de sessões**.
5. Confirme sua solicitação.

Essa alteração não afeta as sessões atuais. Quando você altera o número máximo de sessões para um valor menor que o das sessões ativas atualmente de uma máquina, o novo valor é implementado por meio do atrito normal das sessões ativas.

Se ocorrer uma falha antes do início do processo de atualização, a exibição **Details** do catálogo manterá o número correto de sessões. Se ocorrer uma falha durante o processo de atualização, a exibição indicará o número de sessões desejadas.

Gerenciar máquinas em um catálogo

> **Nota:**
>
> Muitas das ações disponíveis no painel **Gerenciar > Implantação Rápida do Azure** também estão disponíveis no painel **Monitor** no Citrix DaaS Standard for Azure (antigo serviço Citrix Virtual Apps and Desktops Standard for Azure).

Para selecionar ações no painel **Gerenciar > Implantação Rápida do Azure** :

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada de um catálogo.
2. Na guia **Machines**, localize a máquina que você deseja gerenciar. No menu de reticências dessa máquina, selecione a ação desejada:

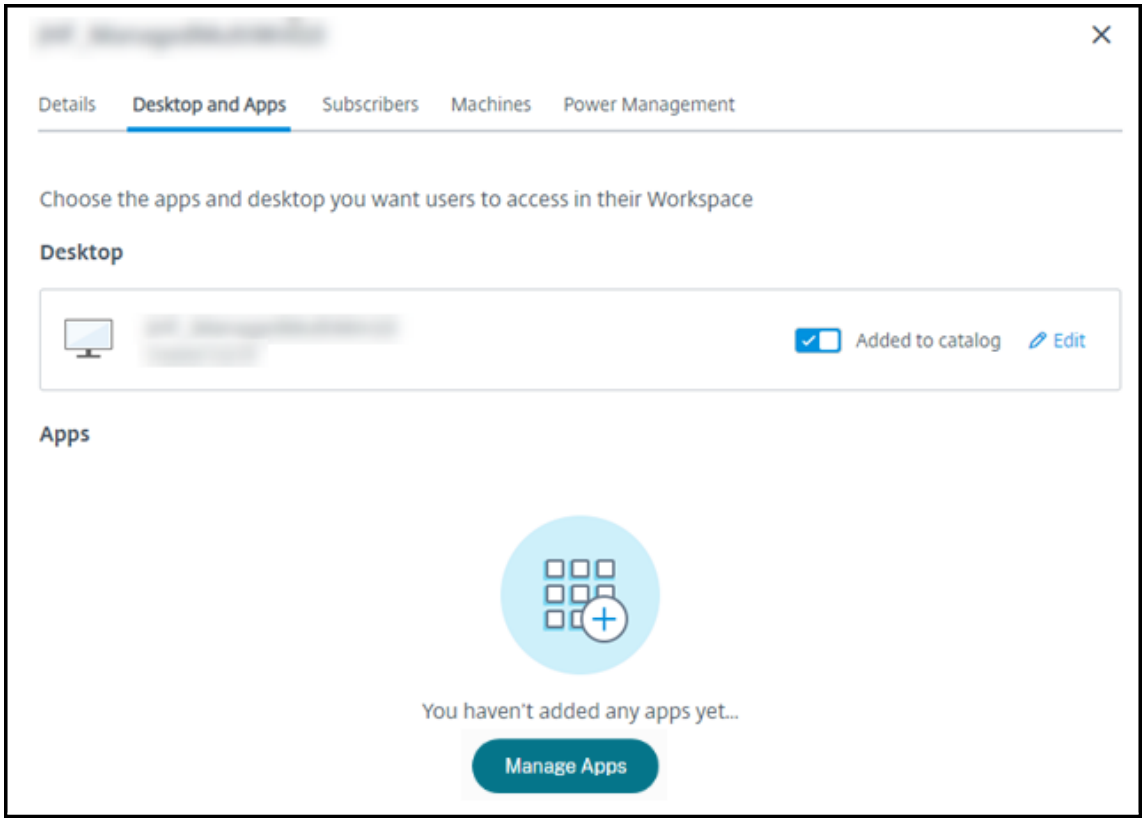
- **Reiniciar:** Reinicie o computador selecionado.
- **Iniciar:** Inicie a máquina selecionada. Essa ação estará disponível somente se a máquina estiver desligada.
- **Shutdown:** desliga a máquina selecionada. Essa ação estará disponível somente se a máquina estiver ligada.
- **Ativar/desativar o modo de manutenção:** Ative o modo de manutenção (se estiver desligado) ou desativado (se estiver ativado) para a máquina selecionada.

  Por padrão, o modo de manutenção está desativado para uma máquina. Ativar o modo de manutenção de uma máquina evita que novas conexões sejam feitas com essa máquina. Os usuários podem se conectar a sessões existentes nessa máquina, mas não podem iniciar novas sessões nessa máquina. Você pode colocar uma máquina no modo de manutenção antes de aplicar patches ou para solução de problemas.
- **Excluir:** Exclua a máquina selecionada. Essa ação está disponível somente quando a contagem de sessões da máquina for zero. Confirme a exclusão.

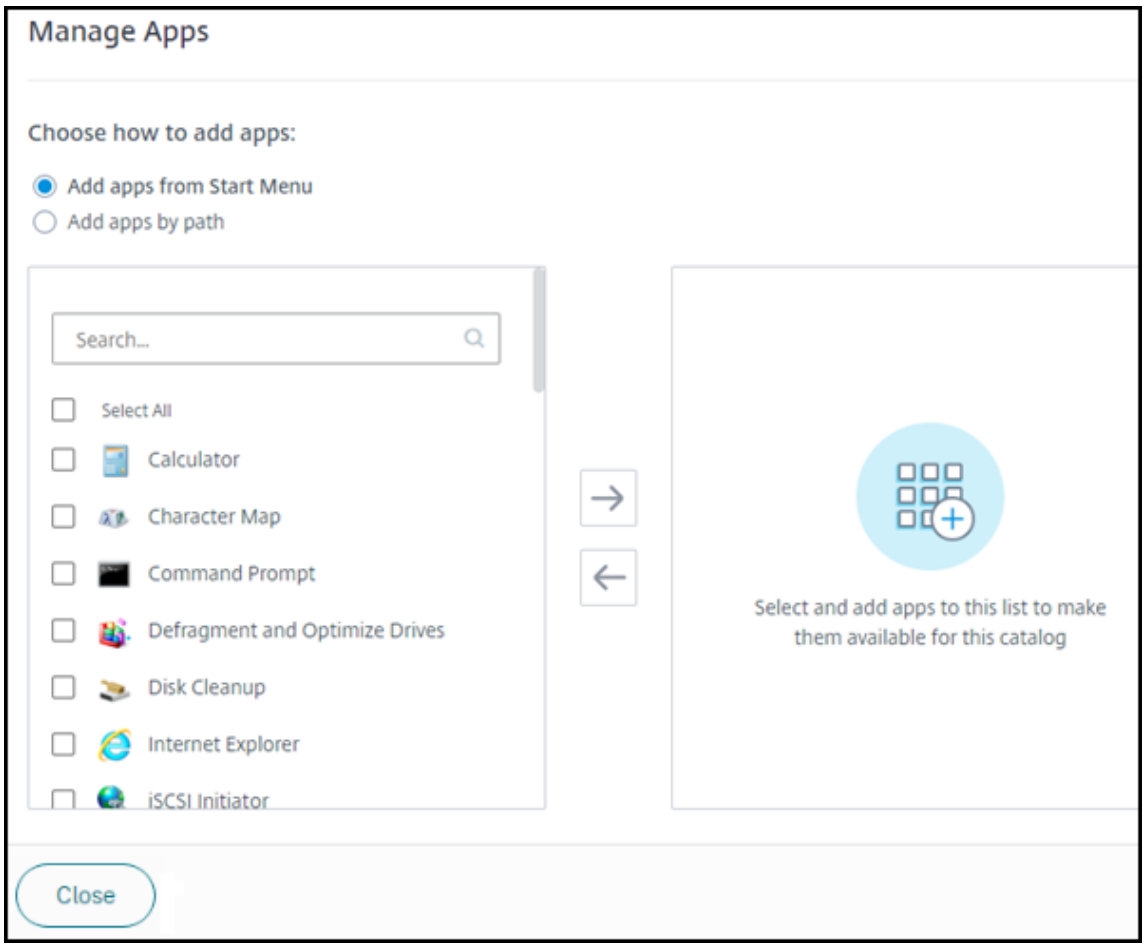
  Quando uma máquina é excluída, todos os dados da máquina são removidos.
- **Forçar reinicialização:** forçar a reinicialização do computador selecionado. Selecione essa ação somente se uma ação **Reiniciar** da máquina falhar.

Adicionar aplicativos a um catálogo

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Área de trabalho e aplicativos**, clique em **Gerenciar aplicativos**.

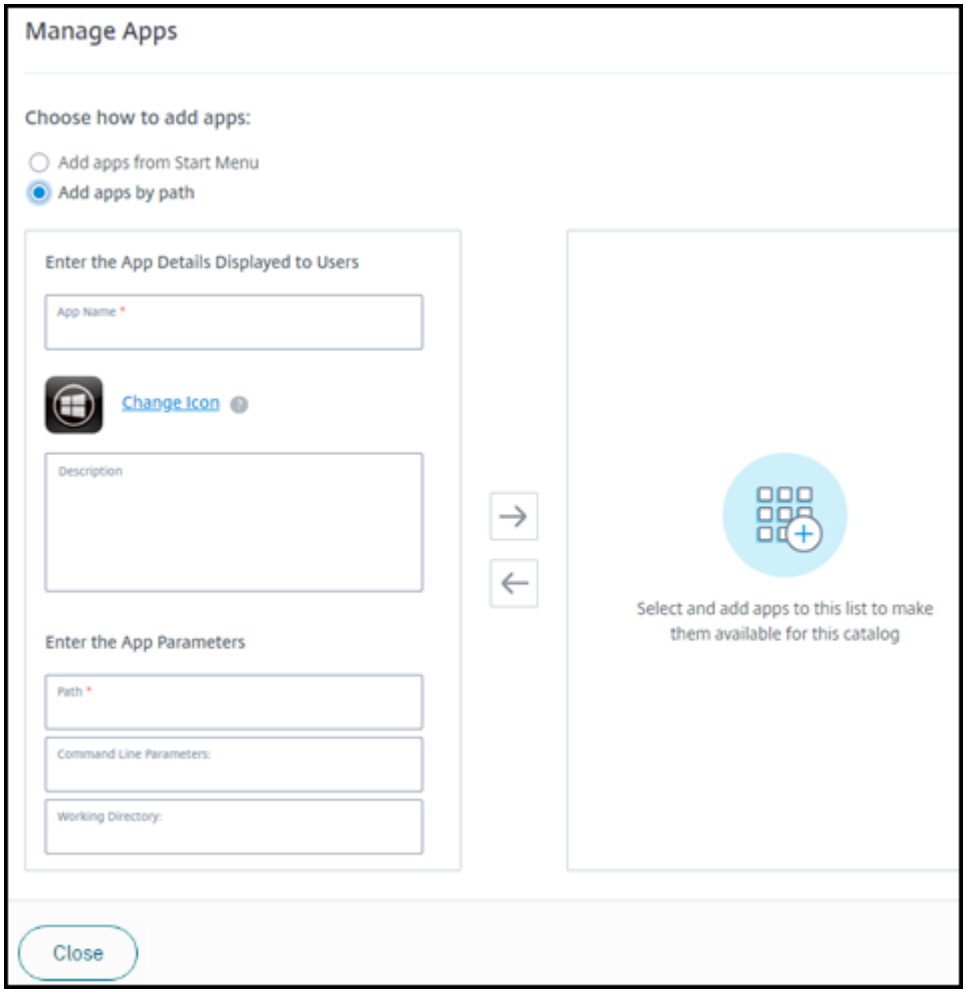


3. Selecione como você está adicionando aplicativos: no menu **Start** das máquinas no catálogo ou em um caminho diferente nas máquinas.
4. Para adicionar aplicativos do menu **Start** :



- Selecione os aplicativos disponíveis na coluna da esquerda. (Use a **Pesquisa** para personalizar a lista de aplicativos.) Clique na seta para a direita entre as colunas. Os aplicativos selecionados se movem para a coluna da direita.
- Da mesma forma, para remover aplicativos, selecione-os na coluna da direita. Clique na seta para a esquerda entre as colunas.
- Se o menu **Iniciar** tiver mais de uma versão do mesmo aplicativo, com o mesmo nome, você poderá adicionar apenas uma. Para adicionar outra versão desse aplicativo, edite essa versão para alterar seu nome. Em seguida, você pode adicionar essa versão do aplicativo.

5. Para adicionar aplicativos por caminho:



- Insira o nome do aplicativo. Esse é o nome que os usuários veem no Citrix Workspace.
- O ícone mostrado é o ícone que os usuários veem no Citrix Workspace. Para selecionar outro ícone, clique no **ícone Alterar** e navegue até o ícone que você deseja exibir.
- (Opcional) Insira uma descrição do aplicativo.
- Insira o caminho para o aplicativo. Esse campo é obrigatório. Opcionalmente, adicione parâmetros de linha de comando e o diretório de trabalho. Para obter detalhes sobre os parâmetros da linha de comando, consulte Passar parâmetros para aplicativos publicados.

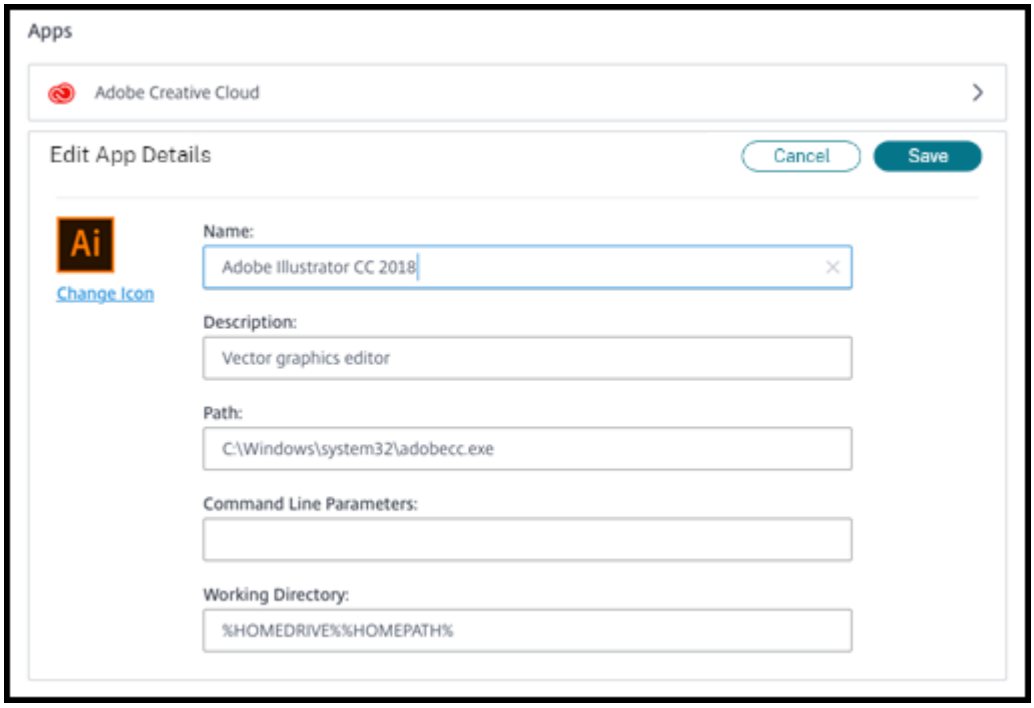
6. Ao terminar, clique em **Fechar**.

O que fazer a seguir (se você estiver concluindo o fluxo de criação e entrega do catálogo): Envie o URL do Citrix Workspace para seus usuários, se ainda não o fez.

Nos VDAs do Windows Server 2019, alguns ícones de aplicativos podem não aparecer corretamente durante a configuração e no espaço de trabalho dos usuários. Como solução alternativa, depois que o aplicativo for publicado, edite o aplicativo e use o recurso **Change icon** para atribuir um ícone diferente que seja exibido corretamente.

Editar um aplicativo em um catálogo

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, clique em qualquer lugar na linha que contém o aplicativo que você deseja editar.
3. Clique no ícone de lápis.



4. Digite as alterações em qualquer um dos seguintes campos:
   - **Name:** o nome que os usuários veem no Citrix Workspace.
   - **Descrição**
   - **Path:** o caminho para o executável.
   - **Command line parameters:** para obter detalhes, consulte Passar parâmetros para aplicativos publicados.
   - **Diretório de trabalho**
5. Para alterar o ícone que os usuários veem em seu Citrix Workspace, clique no **ícone Alterar** e navegue até o ícone que deseja exibir.
6. Quando terminar, clique em **Salvar**.

Passar parâmetros para aplicativos publicados

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos de percentual e estrela (entre aspas duplas) são acrescidos ao final da linha de comando. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos do usuário.

- Se um aplicativo publicado não for iniciado quando esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos do usuário são validados quando os símbolos são anexados.

  Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo do usuário, os símbolos são anexados à linha de comando para ignorar a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

- Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como "C:\Program Files"), inclua a linha de comando do aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas em torno dos símbolos de porcentagem e estrela. Adicione um espaço entre as aspas de fechamento para o caminho e as aspas de abertura para os símbolos de porcentagem e asterisco.

  Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é: `" C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

Remover aplicativos de um catálogo

Remover um aplicativo de um catálogo não o remove das máquinas. Isso apenas impede que ele apareça no Citrix Workspace.

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Área de trabalho e aplicativos**, clique no ícone da lixeira ao lado dos aplicativos que você deseja remover.

Excluir um catálogo

Quando você exclui um catálogo, todas as máquinas no catálogo são destruídas permanentemente. A exclusão de um catálogo não pode ser revertida.

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.

2. Na guia **Detalhes**, clique em **Excluir catálogo** na parte inferior da janela.
3. Confirme a exclusão marcando as caixas de seleção de confirmação e, em seguida, clicando no botão de confirmação.

Para ajudar a identificar contas de máquina residuais do Active Directory que você deve excluir, você pode baixar uma lista de nomes de máquina e do Cloud Connector.

Gerenciar programações de gerenciamento de energia

Um cronograma de gerenciamento de energia afeta todas as máquinas em um catálogo. Uma programação fornece:

- Experiência ideal para o usuário: as máquinas estão disponíveis para os usuários quando são necessárias.
- Segurança: as sessões da área de trabalho que permanecem ociosas por um intervalo especificado são desconectadas, exigindo que os usuários iniciem uma nova sessão em seu espaço de trabalho.
- Gerenciamento de custos e economia de energia: as máquinas com desktops que permanecem ociosas são desligadas. As máquinas são ligadas para atender à demanda programada e real.

Você pode configurar uma programação de energia ao criar um catálogo personalizado ou fazer isso mais tarde. Se nenhum agendamento for selecionado ou configurado, uma máquina será desligada quando uma sessão terminar.

Você não pode selecionar ou configurar uma programação de energia ao criar um catálogo com criação rápida. Por padrão, os catálogos de criação rápida usam a programação predefinida de Cost Saver. Você pode selecionar ou configurar uma programação diferente posteriormente para esse catálogo.

O gerenciamento de agendamento inclui:

- Saber quais informações um cronograma contém
- Criação de um cronograma

Informações em uma programação

O diagrama a seguir mostra as configurações de agendamento para um catálogo que contém máquinas com várias sessões. As configurações de um catálogo contendo máquinas de sessão única (aleatórias ou estáticas) diferem ligeiramente.

Um cronograma de gerenciamento de energia contém as seguintes informações.

Programações predefinidas O Citrix DaaS for Azure oferece várias programações predefinidas. Você também pode configurar e salvar agendas personalizadas. Embora você possa excluir predefinições personalizadas, não é possível excluir predefinições fornecidas pela Citrix.

Time zone Usada com a configuração de máquinas de ligar para estabelecer horas de trabalho e horas extras, com base no fuso horário selecionado.

Essa configuração é válida para todos os tipos de máquinas.

Ligar as máquinas: horas de trabalho e após o expediente Os dias da semana e as horas de início e parada do dia que formam suas horas de trabalho. Isso geralmente indica os intervalos em que você deseja que as máquinas estejam ligadas. Qualquer horário fora desses intervalos é considerado após o expediente. Várias configurações de agendamento permitem que você insira valores separados para horas de trabalho e horas extras. Outras configurações se aplicam o tempo todo.

Essa configuração é válida para todos os tipos de máquinas.

Hibernar máquinas: horas de trabalho e após o expediente Você pode hibernar máquinas. Enquanto uma máquina está hibernando, você não é cobrado pelo uso e economiza no consumo de energia. Os aplicativos e arquivos abertos são salvos quando a máquina começa a hibernar e ficam rapidamente disponíveis na próxima vez que um usuário se conecta à máquina.

Essa configuração está disponível quando todos os critérios a seguir são atendidos:

- A máquina suporta a hibernação.
- O tipo de máquina é estático ou aleatório.
- O sistema operacional é Windows, não Linux.
- O MCSIO não está habilitado.
- A assinatura é uma assinatura do Azure gerenciada pelo cliente.

Desligar as máquinas quando não houver reconexão Especifique por quanto tempo uma máquina permanece suspensa antes de ser desligada. Insira um valor maior que o valor especificado no campo Quando desconectado.

Essa configuração é válida somente para máquinas aleatórias.

Desconectar sessões da área de trabalho quando ociosas Por quanto tempo uma área de trabalho pode permanecer ociosa (não usada) antes que a sessão seja desconectada. Depois que uma sessão é desconectada, o usuário deve ir para o Workspace e iniciar uma área de trabalho novamente. Essa é uma configuração de segurança.

Essa configuração é válida para todos os tipos de máquinas. Uma configuração se aplica o tempo todo.

Power off idle desktops Por quanto tempo uma máquina pode permanecer desconectada antes de ser desligada. Depois que uma máquina é desligada, o usuário deve ir para o Workspace e iniciar uma área de trabalho novamente. Essa é uma configuração de economia de energia.

Por exemplo, digamos que você queira que os desktops se desconectem depois de ficarem ociosos por 10 minutos. Depois, desligar as máquinas se elas permanecerem desconectadas por mais 15 minutos.

Se um determinado usuário parar de usar a área de trabalho e sair para uma reunião de uma hora, a área de trabalho será desconectada após 10 minutos. Depois de mais 15 minutos, a máquina será desligada (25 minutos no total).

Do ponto de vista do usuário, as duas configurações de inatividade (desconexão e desligamento) têm o mesmo efeito. Se esse usuário ficar longe de sua área de trabalho por 12 minutos ou uma hora, ele deve iniciar uma área de trabalho novamente a partir do Workspace. A diferença nos dois temporizadores afeta o estado da máquina virtual que fornece a área de trabalho.

Essa configuração é válida para máquinas de sessão única (estáticas ou aleatórias). Você pode inserir valores para horas de trabalho e após o expediente.

Log off disconnected sessions Por quanto tempo uma máquina pode permanecer desconectada antes que a sessão seja fechada.

Essa configuração é válida para máquinas com várias sessões. Uma configuração se aplica o tempo todo.

Power Off Delay A quantidade mínima de tempo que uma máquina deve ser ligada antes de ser qualificável para desligamento (junto com outros critérios). Esta configuração evita que as máquinas "liguem e desliguem"durante as demandas oscilantes das sessões mais voláteis.

Essa configuração é válida para máquinas com várias sessões e se aplica o tempo todo.

Minimum running machines Quantas máquinas devem permanecer ligadas, independentemente de quanto tempo estão ociosas ou desconectadas.

Essa configuração é válida para máquinas aleatórias e com várias sessões. Você pode inserir valores para horas de trabalho e após o expediente.

Capacity buffer Um buffer de capacidade ajuda a acomodar picos repentinos na demanda, mantendo um buffer de máquinas ligado. O buffer é especificado, como uma porcentagem da demanda da sessão atual. Por exemplo, se houver 100 sessões ativas e o buffer de capacidade for 10%, o Citrix DaaS for Azure fornecerá capacidade para 110 sessões. Um aumento na demanda pode ocorrer durante o horário de trabalho ou adicionar novas máquinas ao catálogo.

Um valor menor diminui o custo. Um valor mais alto ajuda a garantir uma experiência de usuário otimizada. Ao iniciar sessões, os usuários não precisam esperar que máquinas extras sejam ligadas.

Quando há máquinas mais do que suficientes para suportar o número de máquinas ligadas necessárias no catálogo (incluindo o buffer de capacidade), as máquinas extras são desligadas. O desligamento pode ocorrer devido a horários fora de pico, logoffs de sessão ou menos máquinas no catálogo. A decisão de desligar uma máquina deve atender aos seguintes critérios:

- A máquina está ligada e não está no modo de manutenção.
- A máquina está registrada como disponível ou aguardando registro após ser ligada.
- A máquina não tem sessões ativas. Todas as sessões restantes foram encerradas. (A máquina ficou ociosa durante o período de tempo limite de inatividade.)
- A máquina foi ligada por pelo menos "X"minutos, onde "X"é o atraso de desligamento especificado para o catálogo.

  Em um catálogo estático, depois que todas as máquinas no catálogo são atribuídas, o buffer de capacidade não desempenha um papel na ativação ou desativação das máquinas.

Essa configuração é válida para todos os tipos de máquinas. Você pode inserir valores para horas de trabalho e após o expediente.

Crie um cronograma de gerenciamento de energia

1. No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Power Management**, determine se alguma das programações predefinidas (no menu na parte superior) atende às suas necessidades. Selecione uma predefinição para ver os valores que ela usa. Se quiser usar uma predefinição, deixe-a selecionada.
3. Se você alterar os valores em qualquer campo (como dias, horas ou intervalos), a seleção predefinida será alterada para **Custom** automaticamente. Um asterisco indica que as configurações personalizadas não foram salvas.
4. Defina os valores desejados para a programação personalizada.
5. Clique em **Personalizar** na parte superior e salve as configurações atuais como uma nova predefinição. Digite um nome para a nova predefinição e clique na marca de seleção.
6. Quando terminar, clique em **Salvar alterações**.

Posteriormente, você pode editar ou excluir uma predefinição personalizada usando os ícones de lápis ou lixeira no menu **Predefinições**. Você não pode editar ou excluir predefinições comuns.

Instantâneo e restauração do VDA

Os recursos de instantâneo e restauração do Citrix DaaS for Azure fornecem uma maneira de se recuperar de perda de dados não planejada ou outras falhas em VDAs que fornecem desktops e aplicativos. A operação de instantâneo tira e armazena um instantâneo da máquina. Posteriormente, uma operação de restauração usa um instantâneo selecionado.

- Você pode configurar agendas de instantâneos diárias e semanais para todas as máquinas em um catálogo. Esses instantâneos são chamados *de instantâneos automáticos*. Um instantâneo é tirado de cada máquina no catálogo. Não há agendamentos de instantâneos padrão.
- Você pode fazer backup de um único V em um catálogo sob demanda. Isso é chamado de instantâneo manual. Você pode criar um *instantâneo manual* de uma máquina mesmo que o catálogo ao qual ela pertence tenha instantâneos agendados. (No entanto, você não pode agendar instantâneos de uma única máquina.)

> **Importante:**
>
> Os recursos de instantâneo e restauração do Citrix DaaS for Azure são suportados apenas para máquinas em catálogos estáticos e atribuídos aos usuários.

Horários de instantâneos

Lembre-se: as agendas de instantâneos se aplicam a todas as máquinas em um catálogo.

Por padrão, não há agendamentos de instantâneos.

Para gerenciar agendas de instantâneos:

1. No painel **Gerenciar**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Detalhes**, clique em **Agendar instantâneos**.
3. Na página **Agendar Instantâneos**, configure agendas para instantâneos automáticos semanais ou diários, ou ambos:
    - Para adicionar ou alterar instantâneos semanais, mova o controle deslizante para **Instantâneos automáticos semanais** até que uma marca de seleção apareça. Selecione o dia da semana e a hora de início.
    - Para adicionar ou alterar instantâneos diários, mova o controle deslizante para **Instantâneos automáticos diários** até que uma marca de seleção apareça. Selecione a hora de início.
    - Para remover instantâneos semanais, mova o controle deslizante para **Instantâneos automáticos semanais** até que um **X** apareça.
    - Para remover instantâneos diários, mova o controle deslizante para **Instantâneos automáticos diários** até que um **X** apareça.

4. Quando terminar, clique em **Salvar** na parte inferior da página.

Instantâneos manuais

Um instantâneo manual é para uma única máquina em um catálogo. (Você não pode criar um cronograma para tirar um instantâneo de máquinas individuais.)

1. No painel **Gerenciar**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Máquinas**, encontre a máquina da qual você deseja tirar um instantâneo. Selecione **Instantâneos** no menu de reticências dessa máquina.
3. Na página **Instantâneos do *VDA-name***, clique em **Criar Instantâneo Manual**.
4. Forneça um nome para o instantâneo. Recomendado: Escolha um nome que você possa identificar facilmente mais tarde.
5. Confirme sua solicitação.

Exibir e gerenciar instantâneos

1. No painel **Gerenciar**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Máquinas**, encontre a máquina da qual você deseja tirar um instantâneo. Selecione **Instantâneos** no menu de reticências dessa máquina.
3. Na página **Backups para *VDA-name***:
   - Se não houver instantâneos para a máquina, uma mensagem o orientará a criar um instantâneo manual para esta máquina ou criar instantâneos agendados para todas as máquinas no catálogo que contém essa máquina.
   - Você pode selecionar um dos instantâneos e restaurar a máquina. Consulte Restaurar.
   - Você pode excluir instantâneos. Marque as caixas de seleção para um ou mais instantâneos e clique em **Excluir** no cabeçalho da tabela. Confirme sua solicitação.

Dica: quando você exclui um catálogo, todos os instantâneos são destruídos.

Restaurar

Você pode restaurar uma máquina a partir de qualquer instantâneo disponível para essa máquina.

Durante uma restauração, a máquina é desligada. Nenhuma das ações no menu de reticências de uma máquina está disponível enquanto um instantâneo está sendo restaurado.

1. No painel **Gerenciar**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Máquinas**, encontre a máquina da qual você deseja tirar um instantâneo. Selecione **Instantâneos** no menu de reticências dessa máquina.

3. Na página **Snapshots para *VDA-name***, marque a caixa de seleção do instantâneo que você deseja usar.
4. Clique em **Restaurar** no cabeçalho da tabela.
5. Confirme a solicitação.

A coluna **Status** na guia **Máquinas** indica o progresso e o resultado da operação de restauração.

Se uma máquina não conseguir restaurar um instantâneo, tente novamente.

Informações correlatas

- Atualizar um catálogo com uma nova imagem
- Adicionar e remover usuários em um catálogo
- Ingressou no domínio e não ingressado no domínio

Monitoramento

May 11, 2023

No painel **Monitor**, você pode exibir o uso da área de trabalho, as sessões e as máquinas na sua implantação do Citrix DaaS Standard for Azure (antigo Citrix Virtual Apps and Desktops Standard for Azure). Você também pode controlar sessões, gerenciar máquinas de energia, encerrar aplicativos em execução e encerrar processos em execução.

Para acessar o painel **Monitor** :

1. Faça login no Citrix Cloud, se ainda não o fez. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**.
2. No painel **Manage**, clique na guia **Monitor**.

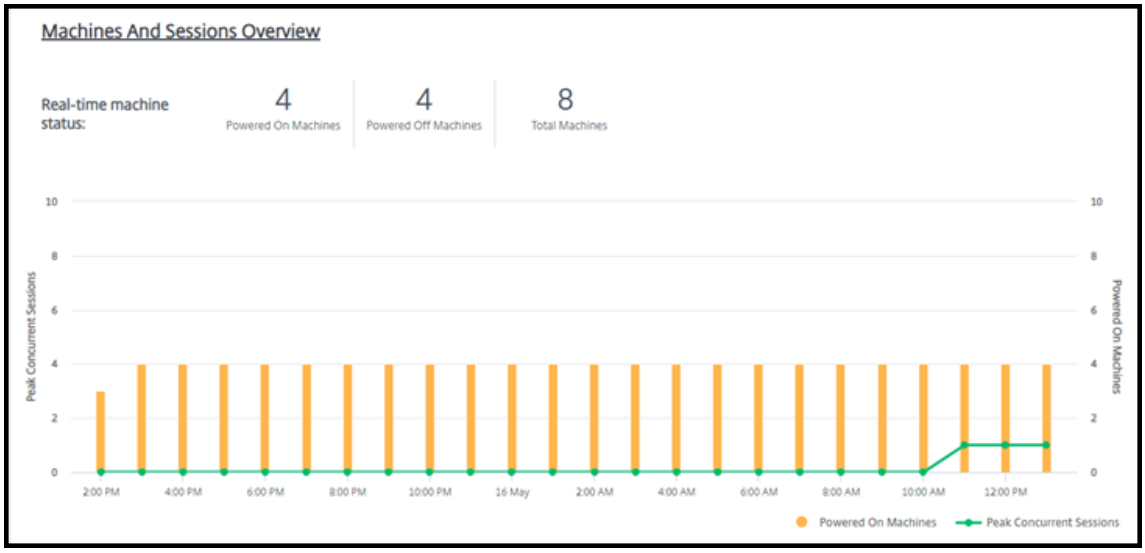
Monitorar o uso de

As exibições nesta página são atualizadas a cada cinco minutos.

- **Visão geral da máquina e das sessões:** Você pode personalizar a exibição para mostrar informações sobre todos os catálogos (padrão) ou um catálogo selecionado. Você também pode personalizar o período: o último dia, semana ou mês.

  As contagens na parte superior do display indicam o número total de máquinas, mais o número de máquinas que estão ligadas e desligadas. Passe o mouse sobre um valor para exibir quantas são de sessão única e de várias sessões.

O gráfico abaixo das contagens mostra o número de máquinas ligadas e picos de sessões simultâneas em pontos regulares durante o período selecionado. Passe o mouse sobre um ponto do gráfico para exibir as contagens nesse ponto.



- **Top 10s:** para personalizar uma exibição dos 10 principais, selecione um período de tempo: a semana passada (padrão), mês ou três meses. Você também pode personalizar a exibição para mostrar somente informações sobre atividades envolvendo máquinas de sessão única, máquinas com várias sessões ou aplicativos.
  - **Top 10 Active Users:** lista os usuários que iniciaram desktops com mais frequência durante o período. Passar o mouse sobre uma linha exibe o total de inicializações.
  - **Top 10 Active Catalogs:** lista os catálogos com maior duração durante o período selecionado. A duração é a soma de todas as sessões do usuário desse catálogo.

Relatório de uso de desktop

Para baixar um relatório contendo informações sobre inícios de máquinas durante o último mês, clique em **Iniciar atividade**. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

Filtre e pesquise para monitorar máquinas e sessões

Quando você está monitorando as informações da sessão e da máquina, todas as máquinas ou sessões são exibidas por padrão. Você pode:

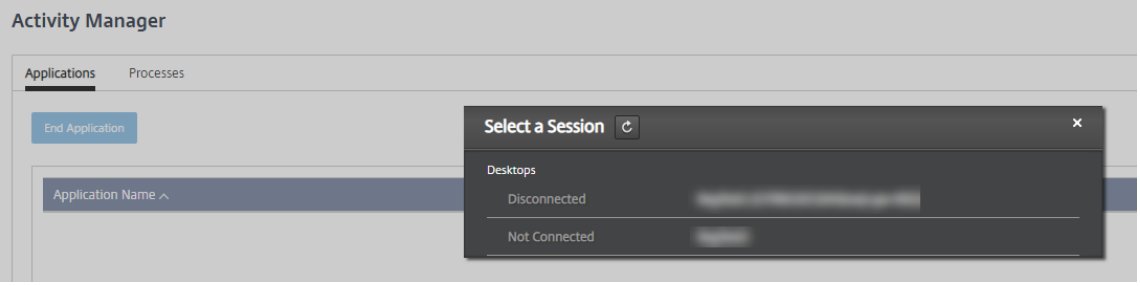
- Filtrar a exibição por máquinas, sessões, conexões ou aplicativos.
- Refinar a exibição de sessões ou máquinas escolhendo os critérios desejados, criando um filtro usando expressões.

- Salvar os filtros que você cria para reutilização.

Controlar os aplicativos de um usuário

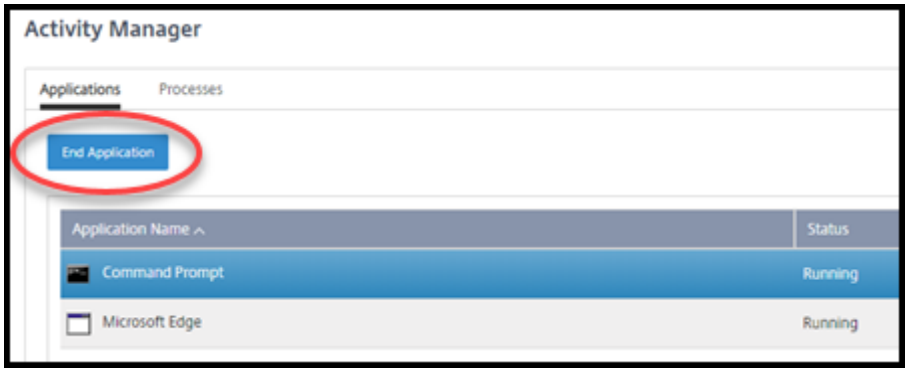
Você pode exibir e gerenciar aplicativos e processos para um usuário que tem uma sessão em execução ou uma área de trabalho atribuída.

1. No painel **Monitor**, clique em **Search** e insira o nome do usuário (ou os caracteres iniciais do nome do usuário), máquina ou ponto de extremidade. Nos resultados da pesquisa, selecione o item que você está procurando. (Para recolher a caixa de pesquisa sem pesquisar, clique em **Pesquisar** novamente.)
2. Selecione uma sessão.



   O Activity Manager lista os aplicativos e os processos da sessão do usuário.

3. Para encerrar um aplicativo, na guia **Aplicativos** do Gerenciador de Atividades, clique na linha do aplicativo para selecionar esse aplicativo e, em seguida, clique em **Finalizar aplicativo**.



4. Para finalizar um processo, na guia **Processos** do Gerenciador de Atividades, clique na linha do processo para selecionar esse processo e, em seguida, clique em **Finalizar processo**.
5. Para exibir os detalhes da sessão, clique em **Detalhes** no canto superior direito. Para retornar à exibição de aplicativos e processos, clique em Gerenciador de atividades no canto superior direito.
6. Para controlar a sessão, clique em **Controle de sessão > Fazer logoff** ou **Controle de sessão > Desconectar**.

Sombrear usuários

Use o recurso de sombreamento para exibir ou trabalhar diretamente na sessão ou na máquina virtual de um usuário. Você pode sombrear VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja sombrear. Verifique isso verificando o nome da máquina listado na barra de `User` título.

O Shadowing é iniciado em uma nova guia do navegador. O seu navegador deve permitir pop-ups do URL do Citrix Cloud.

Em uma assinatura do Citrix Managed Azure, o sombreamento é suportado somente para usuários em máquinas ingressadas no domínio. Para sombrear uma máquina não ingressada no domínio em uma assinatura do Citrix Managed Azure, você deve configurar uma máquina bastion. Para obter detalhes, consulte Bastion access.

O sombreamento deve ser iniciado a partir de uma máquina na mesma rede virtual que as máquinas ingressadas no domínio e também atender aos requisitos de porta.

Ativar sombreamento

1. No painel **Monitor**, acesse a exibição **Detalhes do usuário**.
2. Selecione a sessão do usuário e clique em **Sombra** na exibição **Gerenciador de atividades** ou no painel **Detalhes da sessão**.

Sombra Linux VDAs

O sombreamento, ou shadowing, está disponível para Linux VDAs versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu versão 16.04

O Monitor usa o FQDN para se conectar ao Linux VDA de destino. É preciso que o Monitor cliente possa resolver o FQDN do Linux VDA.

- O VDA deve ter os pacotes `python-websockify` e `x11vn` instalados.
- A conexão `noVNC` com o VDA usa o protocolo WebSocket. Por padrão, é usado o protocolo WebSocket `ws://`. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro `wss://`. Instale certificados SSL em cada cliente do Monitor e Linux VDA.

Siga as instruções em Session Shadowing para configurar seu VDA Linux para sombreamento.

1. Depois de habilitar o sombreamento, a conexão de sombreamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
3. O administrador pode exibir somente a sessão sombreada.

VDAs do Windows sombra

As sessões do Windows VDA são sombreadas usando a Assistência Remota do Windows. Ative o recurso `Use Windows Remote Assistance` ao instalar o VDA.

1. Depois de habilitar o sombreamento, a conexão de sombreamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo `.msrc incident`.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ainda não estiver selecionado por padrão. Um prompt de confirmação é exibido no dispositivo do usuário.
3. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
4. Para obter mais controle, peça ao usuário que compartilhe o controle do teclado e do mouse.

Monitorar e controlar sessões

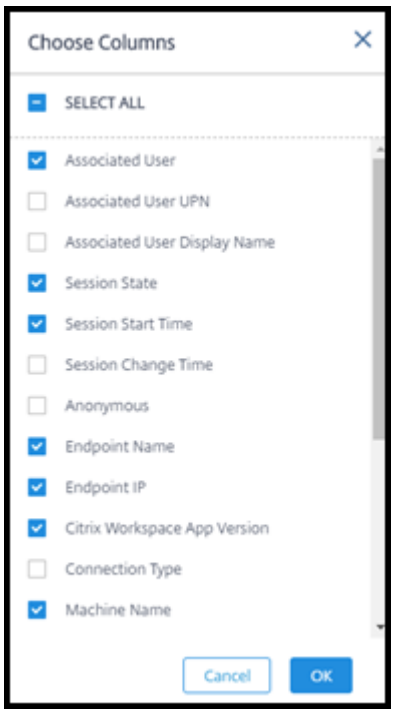
A exibição da sessão são atualizadas a cada minuto.

Além de visualizar sessões, você pode desconectar uma ou mais sessões ou fazer logoff de usuários das sessões.

1. No painel **Monitor**, clique em **Filters**.

2. Selecione a visualização **Sessions** .

3. Para personalizar a exibição, clique em **Escolher colunas** e marque as caixas de seleção dos itens que você deseja que apareçam. Quando terminar, clique em **OK**. A exibição das sessões é atualizada automaticamente.



4. Clique na caixa de seleção à esquerda de cada sessão que você deseja controlar.
5. Para fazer logoff ou desconectar a sessão, selecione **Controle de sessão > Fazer logoff** ou **Controle de sessão > Desconectar**.

Lembre-se de que a programação de gerenciamento de energia para o catálogo também pode controlar a desconexão de sessões e o logoff de usuários de sessões desconectadas.

Como alternativa ao procedimento acima, você também pode **Pesquisar** um usuário, selecionar a sessão que deseja controlar e, em seguida, exibir os detalhes da sessão. Ali, as opções de logoff e desconexão também estão disponíveis.

Relatório de informações da sessão

Para baixar as informações da sessão, clique em **Exportar** na exibição das sessões. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

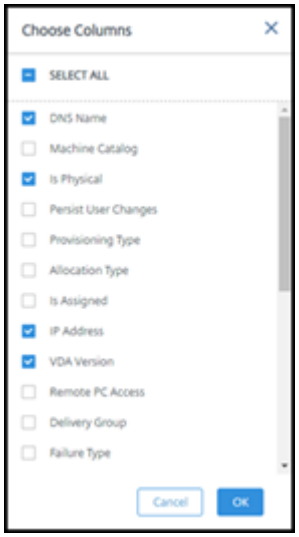
Máquinas de monitoramento e controle de energia

Os monitores da máquina são atualizados a cada minuto.

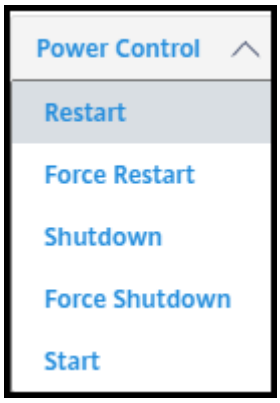
1. No painel **Monitor**, clique em **Filters**.
2. Selecione a exibição **Máquinas**.

Por padrão, a tela lista máquinas com sistema operacional de sessão única. Como alternativa, você pode exibir máquinas com várias sessões.

3. Para personalizar a exibição, clique em **Escolher colunas** e marque as caixas de seleção dos itens que você deseja que apareçam. Quando terminar, clique em **OK**. A exibição das máquinas é atualizada automaticamente.



4. Para controlar máquinas de energia ou colocá-las dentro ou fora do modo de manutenção, clique na caixa de seleção à esquerda de cada máquina que você deseja controlar.
5. Para controlar a energia das máquinas selecionadas, clique em **Controle de energia** e selecione uma ação.



6. Para colocar as máquinas selecionadas dentro ou fora do modo de manutenção, clique em

Modo de **manutenção > LIGADO** ou **Modo de manutenção > DESLIGADO**.

Ao usar o recurso de pesquisa para localizar e selecionar uma máquina, você vê detalhes da máquina, utilização, utilização histórica (dos últimos sete dias) e IOPS médio.

Relatório de informações da máquina

Para baixar as informações da sessão, clique em **Exportar** na tela das máquinas. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

Verificação da integridade de aplicativos e desktops

A investigação automatiza o processo de verificação da integridade de aplicativos e desktops publicados. Os resultados da verificação de integridade estão disponíveis no painel **Monitor** . Para obter detalhes, consulte:

- Investigação de aplicativo
- Investigação de área de trabalho

Citrix DaaS for Azure para provedores de serviços Citrix

September 7, 2022

Este artigo descreve como os Citrix Service Providers (CSPs) podem configurar o Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure service) para clientes (locatários) no Citrix Cloud.

Para obter uma visão geral dos recursos disponíveis para os parceiros Citrix, consulte Citrix Cloud para parceiros.

Requisitos

- Ser um parceiro Citrix Service Provider.
- Ter uma conta do Citrix Cloud.
- Você tem uma assinatura do Citrix DaaS for Azure.

Limitações

- As alterações no nome do cliente podem levar até 24 horas para serem aplicadas em todas as interfaces.
- Ao criar um cliente, o endereço de e-mail deve ser exclusivo.

Problemas conhecidos

- Depois que o usuário de um cliente é atribuído a um recurso, você não pode removê-lo ou cancelar a atribuição dele.
- O console de gerenciamento não impõe a separação do usuário do cliente. Você é responsável por adicionar usuários aos catálogos e recursos apropriados.

Adicionar um cliente

1. Faça login no Citrix Cloud com suas credenciais do CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel do **Cliente**, clique em **Convidar ou Adicionar**. Forneça as informações solicitadas.

   Se o cliente não tiver uma conta do Citrix Cloud, adicione o cliente para criar uma conta de cliente. Ao adicionar o cliente, você também é adicionado automaticamente como administrador com acesso completo à conta do cliente.
3. Se o cliente tiver uma conta do Citrix Cloud:

   a) Um URL do Citrix Cloud é exibido, que você copia e envia para o cliente. Para obter detalhes sobre esse processo, consulte Convidar um cliente para se conectar.
   b) O cliente deve adicioná-lo como administrador com acesso completo à conta. Consulte Adicionar administradores a uma conta do Citrix Cloud.

Você pode adicionar mais administradores posteriormente e controlar quais clientes eles podem ver nos painéis do Citrix DaaS for Azure **Manage** and **Monitor** .

Adicione o Citrix DaaS for Azure a um cliente

1. Faça login no Citrix Cloud com suas credenciais do CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel **Cliente**, selecione **Adicionar serviço** no menu de reticências do cliente.
3. Em **Selecione um serviço para adicionar**, clique em **Citrix DaaS Standard for Azure**.
4. Clique em **Continue**.

Depois de concluir esse procedimento, o cliente é integrado à sua assinatura do Citrix DaaS for Azure.

Quando a integração é concluída, um novo cliente é criado automaticamente no Citrix DaaS para Azure. O cliente está visível em **Gerenciar > Implantação rápida**.

Filtrar recursos por cliente

Você pode filtrar recursos por cliente no painel Citrix DaaS for Azure **Manage > Azure Quick Deploy** . (Por padrão, todos os recursos são exibidos.) Ao trabalhar com recursos como catálogos, imagens de máquina e assinaturas do Azure, você pode selecionar exibições específicas do cliente para ajudar a organizar os recursos de seus locatários.

As conexões SD-WAN são criadas por cliente. O cliente deve ter um direito de serviço do SD-WAN Orchestrator.

- Para criar uma conexão SD-WAN para um cliente, siga as orientações em Criar uma conexão SD-WAN. Na página **Adicionar uma conexão de rede**, selecione o cliente. Você pode selecionar a caixa de tipo de conexão SD-WAN somente se esse cliente tiver um direito de serviço do SD-WAN Orchestrator.
- Para que a criação da conexão seja bem-sucedida, o cliente também deve ter um Nó de Controle Mestre (MCN) instalado. No entanto, somente o direito de serviço do SD-WAN Orchestrator determina se o tipo de conexão SD-WAN pode ser selecionado.

Crie catálogos para entregar aplicativos e desktops

Um catálogo é um grupo de usuários e a coleção de máquinas virtuais às quais eles têm acesso. Quando você cria um catálogo, uma imagem é usada (com outras configurações) como um modelo para criar as máquinas. Para obter detalhes, consulte Criar catálogos.

Domínios federados

Os domínios federados permitem que os usuários clientes usem credenciais de um domínio anexado ao local do recurso para entrar no espaço de trabalho. Você pode fornecer espaços de trabalho dedicados aos seus clientes que os usuários podem acessar por meio de um URL de espaço de trabalho personalizado (por exemplo, `customer.cloud.com`), enquanto o local do recurso permanece na sua conta do Citrix Cloud.

Você pode fornecer espaços de trabalho dedicados ao lado do espaço de trabalho compartilhado que os clientes podem acessar usando o URL do espaço de trabalho do CSP (por exemplo, `csppartner.cloud.com`). Para permitir o acesso do cliente ao espaço de trabalho dedicado, você os adiciona aos domínios apropriados que você gerencia.

Depois de configurar o espaço de trabalho por meio da Configuração do espaçode trabalho, os usuários dos clientes podem entrar no espaço de trabalho e acessar os aplicativos e áreas de trabalho que você disponibilizou.

Adicionar um cliente a um domínio

1. Faça login no Citrix Cloud com suas credenciais do CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel do **Cliente**, selecione **Gerenciamento de identidade e acesso** no menu superior esquerdo.
3. Na guia **Domínios**, selecione **Gerenciar domínio federado** no menu de reticências do domínio.
4. No cartão **Gerenciar domínio federado**, na coluna **Clientes disponíveis**, selecione um cliente que você deseja adicionar ao domínio. Clique no sinal de mais ao lado do nome do cliente. O cliente selecionado agora aparece na coluna **Clientes federados**. Repita para adicionar outros clientes.
5. Quando terminar, clique em **Aplicar**.

Remover um cliente de um domínio

Quando você remove um cliente de um domínio que você gerencia, os usuários do cliente não podem mais acessar seus espaços de trabalho usando as credenciais do seu domínio.

1. No Citrix Cloud, selecione **Gerenciamento de identidade e acesso** no menu superior esquerdo.
2. Na guia **Domínios**, selecione **Gerenciar domínio federado** no menu de reticências do domínio que você deseja gerenciar.
3. Na lista de clientes federados, localize ou pesquise os clientes que você deseja remover.

   - Clique em **X** para remover um cliente.
   - Para remover todos os clientes listados do domínio, clique em **Remover tudo**.

   Os clientes selecionados são movidos para a lista de **Clientes disponíveis**.
4. Clique em **Aplicar**.
5. Revise os clientes que você selecionou e clique em **Remover clientes**.

Adicionar um administrador com acesso restrito

1. Faça login no Citrix Cloud com suas credenciais do CSP. Clique em **Clientes** no menu superior esquerdo.

2. No painel do **Cliente**, selecione **Gerenciamento de identidade e acesso** no menu superior esquerdo.
3. Na guia **Administradores**, clique em **Adicionar administradores de**e selecione **Citrix Identity**.
4. Digite o endereço de e-mail da pessoa que você está adicionando como administrador e clique em **Convidar**.
5. Configure as permissões de acesso apropriadas para o administrador. A Citrix recomenda selecionar **Custom access**, a menos que você queira que o administrador tenha controle de gerenciamento do Citrix Cloud e de todos os serviços assinados.
6. Selecione um ou mais pares de função e escopo para o Citrix DaaS for Azure, conforme necessário.
7. Quando terminar, clique em **Enviar convite**.

Quando o administrador aceita o convite, ele tem o acesso que você atribuiu.

Acesso do parceiro ao provedor de identidade do cliente

Você pode gerenciar usuários no painel Citrix DaaS for Azure **Manage > Azure Quick Deploy** ou no console do Citrix Cloud.

Ao usar um provedor de identidade não AD para usuários (como o Citrix Managed Azure AD), você deve ser um administrador do Citrix Cloud Identity and Workspace para o cliente antes de poder gerenciar os usuários desse cliente. Se você não for administrador de um cliente, não poderá adicionar ou excluir usuários desse cliente.

Para gerenciar usuários de um cliente no painel **Gerenciar > Implantação Rápida do Azure**, selecione o parceiro ou cliente em **Mostrar itens para**.

- **Exemplo 1:** Selecione o cliente A em **Mostrar itens para**. O painel agora mostra apenas os itens para o cliente A. Quando você seleciona um catálogo, vê apenas os usuários do cliente A na guia **Assinantes** . Você pode adicionar ou remover usuários para o cliente A (supondo que você seja um administrador desse cliente).
- **Exemplo 2:** Você seleciona a entrada de parceiro em **Mostrar itens para**. O painel agora mostra apenas itens de parceiros. Na guia **Assinantes**, você vê apenas os usuários criados para o parceiro. Nenhuma entrada de cliente é exibida. Você pode adicionar ou remover usuários desse parceiro (supondo que você seja um administrador desse parceiro), mas não pode gerenciar nenhum usuário cliente desse local.

Para gerenciar usuários para um cliente a partir do console do Citrix Cloud, selecione o cliente quando solicitado após o login (ou mais tarde, usando **Change Customer** na área superior direita do console do Citrix Cloud). Ao usar a Biblioteca para gerenciar usuários, o contexto de exibição reflete o cliente

selecionado. Por exemplo, se você selecionou o cliente A, a Biblioteca mostra apenas as ofertas do cliente A.

Editar permissões de Administração Delegada para administradores

1. Faça login no Citrix Cloud com suas credenciais do CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel do **Cliente**, selecione **Gerenciamento de identidade e acesso** no menu superior esquerdo.
3. Na guia **Administrators**, selecione **Edit Access** no menu de reticências do administrador.
4. Selecione ou desmarque os pares de função e escopo do Citrix DaaS for Azure, conforme necessário. Certifique-se de habilitar apenas as entradas que contenham o escopo exclusivo que foi criado para o cliente.
5. Clique em **Save**.

Acessar e configurar espaços de trabalho

Cada cliente recebe seu próprio espaço de trabalho com um `customer.cloud.com` URL exclusivo. Esse URL é onde os usuários do cliente acessam seus aplicativos e desktops publicados.

- No**Citrix DaaS Standard para Azure:** no painel **Gerenciar > Implantação Rápida do Azure**, visualize a URL expandindo **Acesso e Autenticação do Usuário** à direita.
- No**Citrix Cloud:** no painel do **Cliente**, selecione **Configuração do espaço de trabalho** no menu superior esquerdo. Visualize o URL na guia **Acesso**.

Você pode alterar o acesso e a autenticação para um espaço de trabalho. Você também pode personalizar a aparência e as preferências do espaço de trabalho. Para obter detalhes, consulte os seguintes artigos:

- Configurar espaços de trabalho
- Espaços de trabalho seguros

Monitorar o serviço de um cliente

O painel do Citrix Daas for Azure **Monitor** em um ambiente CSP é essencialmente o mesmo que um ambiente não CSP. Consulte Monitor para obter detalhes.

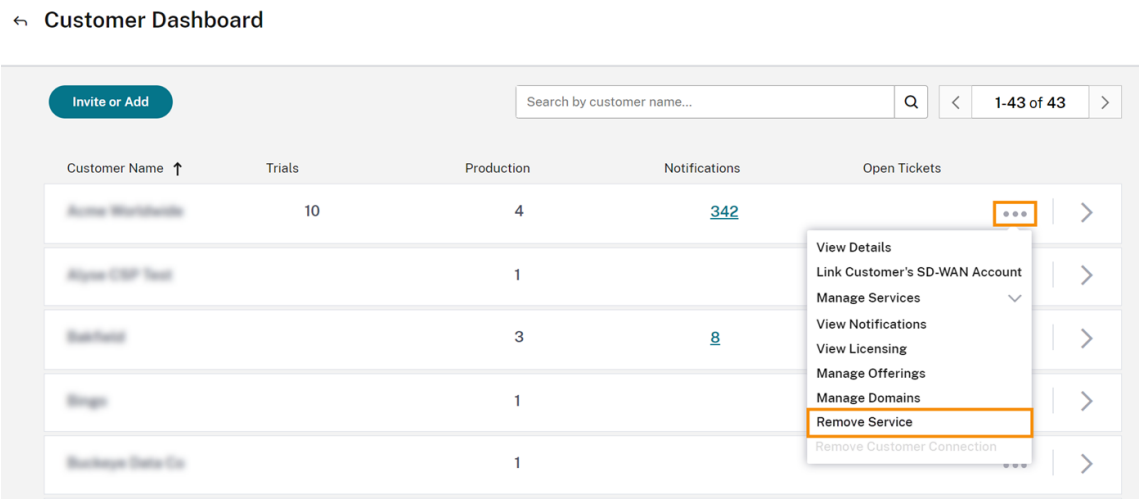
Por padrão, o painel **Monitor** exibe informações sobre todos os clientes. Para exibir informações sobre um cliente, use **Select Customer**.

Lembre-se de que a capacidade de ver as exibições do **Monitor** para um cliente é controlada pelo acesso configurado do administrador.

Remover um serviço

Antes de começar, verifique se o escopo do cliente não está vinculado a nenhum objeto do Citrix DaaS Standard for Azure. Se estiverem vinculados, você não pode remover o serviço. Para desvincular escopos, vá para **Citrix Studio > Administrators > Scopes** e edite o escopo. Para obter mais informações sobre como desvincular escopos, consulte Criar e gerenciar escopos.

1. Faça login no Citrix Cloud com suas credenciais do Citrix Service Providers.
2. No painel do **cliente**, clique no menu de reticências (**...**) do cliente de onde você deseja remover um serviço e selecione **Remover serviço**.



   A página **Service to Remove** é exibida.

3. Clique em **Remove** para remover o serviço.

Solução de problemas

September 7, 2022

Introdução

Os locais de recursos contêm as máquinas que fornecem áreas de trabalho e aplicativos. Essas máquinas são criadas em catálogos, portanto, os catálogos são considerados parte do local de recursos. Cada local de recursos também contém Cloud Connectors. Os Cloud Connectors permitem que o Citrix Cloud se comunique com o local do recurso. A Citrix instala e atualiza os Cloud Connectors.

Opcionalmente, você pode iniciar várias ações do Cloud Connector e de localização de recursos. Veja:

- Ações nos locais de recursos
- Configurações de localização de recursos ao criar um catálogo

O Citrix DaaS for Azure tem ferramentas de solução de problemas e suporte que podem ajudar a resolver problemas de configuração e comunicação com as máquinas que fornecem desktops e aplicativos (os VDAs). Por exemplo, a criação de um catálogo pode falhar ou os usuários podem não conseguir iniciar a área de trabalho ou os aplicativos.

Essa solução de problemas inclui obter acesso à sua assinatura do Citrix Managed Azure por meio de uma máquina bastion ou RDP direto. Depois de obter acesso à assinatura, você pode usar as ferramentas de suporte da Citrix para localizar e resolver problemas. Para obter detalhes, consulte:

- Solução de problemas de VDA usando um bastion ou RDP direto
- Acesso ao bastion
- Acesso direto ao RDP

Solução de problemas de VDA usando um bastion ou RDP direto

Os recursos de suporte são para pessoas com experiência na solução de problemas da Citrix. Isso inclui:

- Citrix Service Providers (CSP) e outros que tenham conhecimento técnico e experiência em solução de problemas com os produtos Citrix DaaS.
- Equipe de suporte Citrix.

Se não estiver familiarizado ou não se sentir seguro para desempenhar a solução de problemas de componentes Citrix, você pode solicitar ajuda do Suporte Citrix. Os representantes do Suporte Citrix podem solicitar que você configure um dos métodos de acesso descritos nesta seção. No entanto, os representantes da Citrix desempenham a real solução do problema, usando as ferramentas e tecnologias Citrix.

> **Importante:**
>
> Esses recursos de suporte são válidos somente para máquinas ingressadas no domínio. Se as máquinas em seus catálogos não tiverem ingressadas no domínio, você será orientado a solicitar ajuda para a solução do problema ao Suporte Citrix.

Métodos de acesso

Estes métodos de acesso são válidos somente para a assinatura do Citrix Managed Azure. Para obter mais informações, consulte Assinaturas do Azure.

Dois métodos de acesso de suporte são fornecidos.

- Acesse seus recursos por meio de uma máquina bastion na assinatura dedicada do Citrix Managed Azure do cliente. O bastion é um ponto de entrada único que permite o acesso às máquinas na assinatura. Ele fornece uma conexão segura com esses recursos, permitindo o tráfego remoto de endereços IP em um intervalo especificado.

  As etapas desse método incluem:

  - Criar a máquina bastion
  - Baixar um agente RDP
  - Fazer RDP para a máquina bastion
  - Conectar-se da máquina bastion às outras máquinas Citrix em sua assinatura

  A máquina bastion é destinada ao uso de curto prazo. Esse método é destinado a problemas que envolvem a criação de catálogos ou máquinas de imagem.

- Acesso RDP direto às máquinas na assinatura dedicada do Citrix Managed Azure do cliente. Para permitir o tráfego RDP, a porta 3389 deve ser definida no grupo de segurança de rede.

  Esse método destina-se a problemas de catálogo não referentes a criação, como usuários que não conseguem iniciar suas áreas de trabalho.

Lembre-se: como alternativa a esses dois métodos de acesso, entre em contato com o Suporte Citrix para obter ajuda.

Acesso ao bastion

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Solução de problemas e suporte** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione um dos dois primeiros tipos de problema e clique em **Use our troubleshooting machine**.
4. Na página **Troubleshoot with Bastion Machine**, selecione o catálogo.

   - Se as máquinas no catálogo selecionado não estiverem ingressadas no domínio, você será instruído a entrar em contato com o Suporte Citrix.
   - Se uma máquina bastion já tiver sido criada com acesso RDP à conexão de rede do catálogo selecionado, pule para a etapa 8.

5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.

6. Digite o nome de usuário e senha que você usará para fazer login quando fizer RDP na máquina bastion. Requisitos de senha.

   Não use caracteres Unicode no nome de usuário.

7. Clique em **Create Bastion Machine**.

   Quando a máquina bastion é criada com sucesso, o título da página muda para **Bastion** — ***conexão***.

   Se a criação da máquina bastion falhar (ou se falhar durante a operação), clique em **Delete** na parte inferior da página de notificação da falha. Tente criar a máquina bastion novamente.

   Você pode alterar a restrição de alcance RDP depois que a máquina bastion for criada. Clique em **Edit**. Insira o novo valor e clique na marca de seleção para salvar a alteração. (Clique no **X** para cancelar a alteração.)

8. Clique em **Download RDP File**.
9. Faça o RDP para o bastion usando as credenciais que você especificou ao criar o bastion. (O endereço da máquina bastion é incorporado ao arquivo RDP que você baixou.)
10. Conecte-se da máquina bastion às outras máquinas Citrix na assinatura. Assim, você pode coletar logs e executar diagnósticos.

As máquinas bastion são ligadas quando são criadas. Para economizar custos, as máquinas são desligadas automaticamente se permanecerem ociosas após a inicialização. As máquinas são excluídas automaticamente após várias horas.

Você pode gerenciar a energia de uma máquina bastion ou excluí-la usando os botões na parte inferior da página. Se você optar por excluir uma máquina bastion, deve confirmar que sabe que todas as sessões ativas na máquina terminarão automaticamente. Além disso, que também todos os dados e arquivos salvos na máquina serão excluídos.

Acesso direto ao RDP

1. No painel **Gerenciar > Implantação Rápida do Azure** no Citrix DaaS para Azure, expanda **Solução de problemas e suporte** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione **Other catalog issue**.
4. Na página **Troubleshoot with RDP Access**, selecione o catálogo.

   Se o RDP já tiver sido habilitado para a conexão de rede do catálogo selecionado, pule para a etapa 7.

5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.
6. Clique em **Enable RDP Access.**

   Quando o acesso RDP é ativado com êxito, o título da página muda para **RDP Access** —***conexão***.

   Se o acesso RDP não for habilitado com êxito, clique em **Retry Enabling RDP** na parte inferior da página de notificação da falha.
7. Conecte-se às máquinas usando suas credenciais de administrador do Active Directory. Assim, você pode coletar logs e executar diagnósticos.

Obtenha ajuda

Se você ainda tiver problemas, abra um tíquete seguindo as instruções em Como obter ajuda e suporte.

Limites

May 11, 2023

Este artigo lista os limites para os recursos em uma implantação do Citrix DaaS Standard for Azure (antigo serviço Citrix Virtual Apps and Desktops Standard for Azure).

> **Nota:**
>
> Os limites são recomendados pela Citrix.

Limites de configuração

Função	Limite
Domínios do Active Directory	25
Catálogos	100
Locais de recursos	25
VDAs por assinatura	2.500

Limites de localização de recursos

A tabela a seguir lista os limites para cada local de recurso. Se seus requisitos excederem esses limites, a Citrix recomenda o uso de mais locais de recursos.

Função	Limite
Domínios do Active Directory	1
VDAs de sessão única	10.000
VDAs de várias sessões	1.000

Os Citrix Cloud Connectors são atribuídos aos locais de recursos e vinculam cargas de trabalho ao Citrix DaaS for Azure. Para obter informações sobre os limites do Cloud Connector e recomendações de tamanho e escala, consulte Considerações de tamanho e escala de Cloud Connectors.

Limites de provisionamento

A tabela a seguir lista os máximos recomendados para uma única conta do Citrix Cloud.

Para implantações de maior escala, a Citrix recomenda um modelo hub-and-spoke, em que os VDAs são distribuídos por várias assinaturas e conexões de rede.

Função	Limite
VDAs de várias sessões por catálogo	500
VDAs de sessão única por catálogo	1.200
VDAs por assinatura do Microsoft Azure	2.500

Limites de uso

Função	Limite
Monitoramento simultâneo de administradores completos	5
Usuários finais simultâneos	100.000
Recursos publicados para um único usuário	250
Inícios de sessão por minuto	3.000

Limites de teste

A tabela a seguir lista os limites durante uma avaliação do Citrix DaaS for Azure.

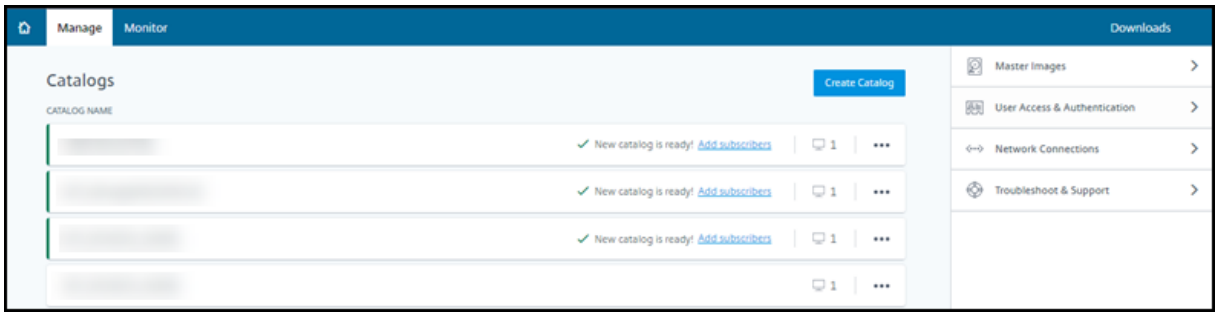
Assinatura do Azure	Função	Limite
Assinatura do Citrix Managed Azure	Número máximo de catálogos	3
	Número máximo de usuários	25
	Número máximo de VDAs por catálogo	3
Assinatura do Azure gerenciada pelo cliente	Número máximo de catálogos	10
	Número máximo de usuários	25
	Número máximo de VDAs por catálogo	10

Referência

September 7, 2022

Painéis

A maioria das atividades de administrador do Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure service) pode ser inserida por meio dos painéis **Gerenciar** e **monitorar**. Depois de criar seu primeiro catálogo, o painel **Gerenciar** é iniciado automaticamente quando você entra no Citrix Cloud e seleciona Citrix DaaS para Azure.



Você pode acessar os painéis depois que sua solicitação de avaliação ou compra for aprovada e concluída.

Para acessar os painéis:

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Meus serviços > DaaS Standard for Azure**. (Como alternativa, você pode clicar em **Gerenciar** no bloco **DaaS Standard for Azure** na área principal da exibição.)
3. Se um catálogo ainda não tiver sido criado, clique em **Primeiros passos** na página de **boas-vindas**. Você é levado ao painel **Gerenciar > Implantação Rápida do Azure** .
4. Se um catálogo já tiver sido criado, você será levado automaticamente para o painel **Gerenciar > Implantação Rápida do Azure** .
5. Para acessar o painel **Monitor**, clique na guia **Monitor**.

Para obter orientações sobre o produto no painel, clique no ícone no canto inferior direito.

Guias de catálogo no painel Gerenciar

No painel **Gerenciar > Implantação Rápida do Azure**, clique em qualquer lugar na entrada do catálogo. As guias a seguir contêm informações sobre o catálogo:

- **Details:** lista as informações especificadas quando o catálogo foi criado (ou sua edição mais recente). Também contém informações sobre a imagem que foi usada para criar o catálogo.

  Nessa guia, você pode:

  - Alterar a imagem usada no catálogo.
  - Excluir o catálogo.
  - Acessar a página que contém detalhes do local do recurso usado pelo catálogo.

- **Desktop:** disponível somente para catálogos contendo máquinas de sessão única (estáticas ou aleatórias). Nessa guia, você pode alterar o nome e a descrição do catálogo.

- **Desktop and Apps:** a guia **Desktop and Apps** está disponível somente para catálogos contendo máquinas multissessão. Nessa guia, você pode:

  - Adicionar, editar ou remover aplicativos que os usuários do catálogo possam acessar no Citrix Workspace.
  - Alterar o nome e a descrição do catálogo.

- **Subscribers:** lista todos os usuários, incluindo o tipo (usuário ou grupo), nome da conta, nome de exibição, além do domínio do Active Directory e do nome UPN.

  Nessa guia, você pode adicionar ou remover usuários de um catálogo.

- **Machines:** mostra o número total de máquinas no catálogo, além do número de máquinas registradas, máquinas não registradas e máquinas que têm o modo de manutenção ativado.

  Para cada máquina no catálogo, a exibição inclui o nome de cada máquina, estado de energia (ligado/desligado), estado de registro (registrado/não registrado), usuários atribuídos, contagem de sessões (0/1) e status do modo de manutenção (um ícone indicando ligado ou desligado).

  Nessa guia, você pode:

  - Adicionar ou excluir uma máquina
  - Iniciar, reinicializar, forçar a reinicialização ou desligar uma máquina
  - Ativar ou desativar o modo de manutenção de uma máquina

  Para obter detalhes, consulte Gerenciar catálogos. Muitas das ações da máquina também estão disponíveis no painel **Monitor**. Consulte Monitorar e controlar máquinas de controle de energia.

- **Power Management:** permite gerenciar quando as máquinas no catálogo são ligadas e desligadas. Uma programação também indica quando as máquinas ociosas são desconectadas.

  Você pode configurar uma programação de energia quando cria um catálogo personalizado ou posteriormente. Se não houver uma programação agendada explicitamente, uma máquina será desligada quando uma sessão terminar.

  Quando cria um catálogo usando o modo de criação rápida, você não pode selecionar ou configurar uma programação de energia. Por padrão, os catálogos de criação rápida usam a programação predefinida de Cost Saver. No entanto, você pode editar o catálogo posteriormente e alterar a programação.

  Para obter detalhes, consulte Gerenciar programações de gerenciamento de energia.

Servidores DNS

Esta seção se aplica a todas as implantações que contêm máquinas ingressadas no domínio. Você pode ignorar esta seção se usar somente máquinas não ingressadas no domínio.

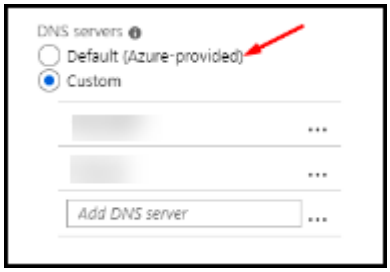
1. Antes de criar um catálogo associado ao domínio (ou uma conexão, se você estiver usando uma assinatura do Citrix Managed Azure), verifique se você tem entradas de servidor DNS que podem resolver nomes de domínio públicos e privados.

   Quando o Citrix DaaS for Azure cria um catálogo ou uma conexão, ele procura pelo menos uma entrada de servidor DNS válida. Se nenhuma entrada válida for encontrada, a operação de criação falhará.

   Onde verificar:

- Se você estiver usando sua própria assinatura do Azure, verifique as entradas de **servidores DNS** no seu Azure.
- Se você estiver usando uma assinatura do Citrix Managed Azure e criando uma conexão de emparelhamento da VNet do Azure, verifique as entradas de **servidores DNS** na VNet do Azure que está emparelhando.
- Se você estiver usando uma assinatura do Citrix Managed Azure e criando uma conexão SD-WAN, verifique as entradas DNS no SD-WAN Orchestrator.

2. No Azure, a configuração **Personalizada** deve ter pelo menos uma entrada válida. O Citrix DaaS for Azure não pode ser usado com a configuração **Padrão (fornecida pelo Azure)**.



- Se **Padrão (fornecido pelo Azure)** estiver habilitado, altere a configuração para **Personalizado**e adicione pelo menos uma entrada de servidor DNS.
- Se você já tiver entradas de servidor DNS em **Personalizado**, verifique se as entradas que deseja usar com o Citrix DaaS para Azure podem resolver nomes IP de domínio público e privado.
- Se você não tiver nenhum servidor DNS que possa resolver nomes de domínio, a Citrix recomenda adicionar um servidor DNS fornecido pelo Azure que tenha esses recursos.

3. Se você alterar qualquer entrada do servidor DNS, reinicie todas as máquinas conectadas à rede virtual. A reinicialização atribui as novas configurações do servidor DNS. (As máquinas virtuais continuam usando suas configurações de DNS atuais até a reinicialização.)

Se você quiser alterar os endereços DNS posteriormente, depois que uma conexão for criada:

- Ao usar sua própria assinatura do Azure, você pode alterá-la no Azure (conforme descrito nas etapas anteriores). Ou você pode alterá-los no Citrix DaaS para Azure.
- Ao usar uma assinatura do Citrix Managed Azure, o Citrix DaaS for Azure não sincroniza as alterações de endereço DNS que você faz no Azure. No entanto, você pode alterar as configurações de DNS para a conexão no Citrix DaaS para Azure.

Lembre-se de que alterar os endereços do servidor DNS pode causar problemas de conectividade para máquinas em catálogos que usam essa conexão.

Adicionando servidores DNS por meio do Citrix DaaS for Azure

Antes de adicionar um endereço de servidor DNS a uma conexão, verifique se o servidor DNS pode resolver nomes de domínio públicos e internos. A Citrix recomenda que você teste a conectividade com um servidor DNS antes de adicioná-lo.

1. Para adicionar, alterar ou remover um endereço de servidor DNS ao criar uma conexão, clique em **Editar servidores DNS** na página **Adicionar** *tipo de conexão*. Ou, se uma mensagem indicar que nenhum endereço de servidor DNS foi encontrado, clique em **Adicionar servidores DNS**. Continue com a etapa 3.
2. Para adicionar, alterar ou remover um endereço de servidor DNS de uma conexão existente:
   a) No painel **Gerenciar > Implantação Rápida do Azure**, **expanda Conexões de Rede** à direita.
   b) Selecione a conexão que deseja editar.
   c) Clique em **Editar servidores DNS**.
3. Adicione, altere ou remova endereços.
   a) Para adicionar um endereço, clique em **Adicionar servidor DNS** e insira o endereço IP.
   b) Para alterar um endereço, clique dentro do campo de endereço e altere os números.
   c) Para remover um endereço, clique no ícone da lixeira ao lado da entrada de endereço. Você não pode remover todos os endereços de servidor DNS. A conexão deve ter pelo menos um.
4. Quando terminar, clique em **Confirmar alterações** na parte inferior da página.
5. Reinicie todas as máquinas que usam essa conexão. A reinicialização atribui as novas configurações do servidor DNS. (As máquinas virtuais continuam usando suas configurações de DNS atuais até a reinicialização.)

Políticas

Definir políticas de grupo para máquinas não ingressadas no domínio

1. Usando o protocolo RDP, conecte-se à máquina que está sendo usada para a imagem.
2. Instale o Gerenciamento de política de grupo Citrix:
   a) Navegue para CTX220345. Baixe o anexo.
   b) Clique duas vezes no arquivo baixado. Na `Group Policy Templates 1912 > Group Policy Management` pasta, clique duas vezes `CitrixGroupPolicyManagement_x64.msi`.
3. Use o comando **Executar** para iniciar o `gpedit.msc`, o que abre o Editor de Diretiva de Grupo.

4. Em `User Configuration Citrix Policies` > `Unfiltered`, clique em **Editar política**.

   Se o Console de Gerenciamento de Diretiva de Grupo falhar (conforme descrito em CTX225742), instale o Microsoft Visual C++ 2015 Runtime (ou uma versão posterior desse tempo de execução).

5. Ative as configurações de política conforme necessário. Por exemplo:

   - Quando trabalhar em **Computer Configuration** ou **User Configuration** (dependendo do que deseja configurar) na guia **Settings**, em `Category` > `ICA` / `Printing`, selecione **Auto-create PDF Universal Printer** e defina como `Enabled`.
   - Se quiser que os usuários conectados sejam administradores da área de trabalho, adicione o grupo **Interactive User** ao grupo interno de administradores.

6. Quando terminar, salve a imagem.
7. Atualize o catálogo existente ou crie um novo catálogo usando a nova imagem.

Definir políticas de grupo para máquinas ingressadas no domínio

1. Confirme que o recurso de Gerenciamento de política de grupo está instalado.

   - Em uma máquina multissessão Windows, adicione o recurso Gerenciamento de política de grupo usando a ferramenta do Windows para adicionar funções e recursos (como **Adicionar funções e recursos**).
   - Em uma máquina de sessão única Windows, instale as Ferramentas de Administração do Servidor Remoto para o SO apropriado. (Essa instalação requer uma conta de administrador de domínio.) Após a instalação, o Console de gerenciamento de política de grupo estará disponível no menu **Iniciar**.

2. Baixe e instale o pacote de gerenciamento da Política de Grupo Citrix na página de download da Citrix e, em seguida, defina as configurações da política conforme necessário. Siga o procedimento em Definir políticas de grupo para máquinas não ingressadas no domínio, etapa 2 até o final.

> **Nota:**
>
> Embora o console do Citrix Studio não esteja disponível no Citrix DaaS para Azure, consulte os artigos de referência de configurações de política para saber mais sobre o que está disponível.

Ações de localização de recursos

A Citrix cria automaticamente um local de recursos e dois Cloud Connectors quando você cria o primeiro catálogo para publicar áreas de trabalho e aplicativos. Você pode especificar algumas

informações relacionadas ao local de recursos quando criar um catálogo. Consulte Configurações de localização do recurso ao criar um catálogo.

(Para o Acesso ao PC remoto, você cria o local do recurso e os Cloud Connectors.)

Esta seção descreve as ações disponíveis depois que um local de recursos é criado.

1. No painel **Gerenciar > Implantação Rápida do Azure**, **expanda Assinaturas de nuvem** à direita.
2. Clique na assinatura.
    - A guia **Detalhes** mostra o número e os nomes dos catálogos e imagens na assinatura. Ele também indica o número de máquinas que podem fornecer desktops ou aplicativos. Essa contagem não inclui máquinas usadas para outros fins, como imagens, Cloud Connectors ou servidores de licenças do RDS
    - A guia **Locais de recursos** lista cada local de recurso. Cada entrada de local de recursos inclui o status e o endereço de cada Cloud Connector no local de recursos.

O menu de reticências na entrada de um local de recursos contém as seguintes ações.

Executar verificação de integridade, em Run Health Check

Selecionar **Run Health Check** inicia a verificação de conectividade imediatamente. Se a verificação falhar, o estado do Cloud Connector será desconhecido, porque ele não está se comunicando com o Citrix Cloud. Reinicie o Cloud Connector.

Reinicializar conectores, em Restart Connectors

A Citrix recomenda reiniciar apenas um Cloud Connector por vez. A reinicialização deixa o Cloud Connector offline e interrompe o acesso do usuário e a conectividade da máquina.

Marque a caixa de seleção do Cloud Connector que você deseja reiniciar. Clique em **Reiniciar**.

Adicionar conectores

A adição de um Cloud Connector normalmente leva 20 minutos para ser concluída.

Forneça as seguintes informações:

- Quantos Cloud Connectors adicionar.
- Credenciais da conta de serviço de domínio, que são usadas para ingressar as máquinas do Cloud Connector no domínio.
- Desempenho da máquina.

- Grupo de recursos do Azure. O padrão é o último grupo de recursos usado pelo local de recursos.
- Organizational Unit (OU). O padrão é a UO usada pela última vez pelo local de recursos.
- Se sua rede requer ou não um servidor proxy para conectividade com a Internet. Se você indicar **Sim**, forneça o FQDN ou o endereço IP do servidor proxy e o número da porta.

Quando terminar, clique em **Adicionar conectores**.

Excluir conectores

Se um Cloud Connector não conseguir se comunicar com o Citrix Cloud e uma reinicialização não resolver o problema, o suporte Citrix pode recomendar a exclusão do Cloud Connector.

Marque a caixa de seleção do Cloud Connector que você deseja excluir. Depois clique em **Excluir**. Quando solicitado, confirme a exclusão.

Você também pode excluir um Cloud Connector disponível. No entanto, se a exclusão do Cloud Connector resultar em menos de dois Cloud Connectors disponíveis no local de recursos, você não pode excluir o Cloud Connector selecionado.

Selecionar horário de atualização, em Select Update Time

A Citrix fornece automaticamente atualizações de software para os Cloud Connectors. Durante uma atualização, um Cloud Connector é colocado offline e atualizado, enquanto outros Cloud Connectors permanecem em serviço. Quando a primeira atualização é concluída, outro Cloud Connector é colocado offline e atualizado. Esse processo continua até que todos os Cloud Connectors no local de recursos sejam atualizados. O melhor momento para iniciar as atualizações geralmente é fora do horário comercial regular.

Escolha o horário para iniciar as atualizações ou indique que você deseja que as atualizações sejam iniciadas quando uma atualização estiver disponível. Quando terminar, clique em **Salvar**.

Renomear

Insira o novo nome para o local do recurso. Clique em **Save**.

Configurar conectividade

Indique se os usuários podem acessar áreas de trabalho e aplicativos por meio do serviço Citrix Gateway ou somente de dentro de sua rede corporativa.

Profile Management

O Profile Management garante que as configurações pessoais se apliquem aos aplicativos virtuais dos usuários, independentemente da localização do dispositivo do usuário.

A configuração do Profile Management é opcional.

Você pode ativar o Profile Management com o serviço de otimização de perfil. O serviço fornece uma maneira confiável de gerenciar essas configurações no Windows. O gerenciamento de perfis garante uma experiência consistente, mantendo um único perfil que segue o usuário. Ele consolida automaticamente e otimiza os perfis de usuário para minimizar os requisitos de gerenciamento e armazenamento. O serviço de otimização de perfil requer o mínimo em administração, suporte e infraestrutura. Além disso, a otimização de perfil fornece aos usuários uma experiência aprimorada de logon e logoff.

O serviço de otimização de perfil requer um compartilhamento de arquivos em que todas as configurações pessoais persistam. Você gerencia os servidores de arquivos. Recomendamos configurar a conectividade de rede para permitir o acesso a esses servidores de arquivos. Você deve especificar o compartilhamento de arquivos como um caminho UNC. O caminho pode conter variáveis de ambiente do sistema, atributos de usuário do Active Directory ou variáveis do Profile Management. Para saber mais sobre o formato da cadeia de texto UNC, consulte Especificar o caminho para o armazenamento do usuário.

Ao ativar o Profile Management, considere otimizar ainda mais o perfil do usuário configurando o redirecionamento de pasta para minimizar os efeitos do tamanho do perfil do usuário. A aplicação do redirecionamento de pasta complementa a solução Profile Management. Para obter mais informações, consulte Redirecionamento de pasta da Microsoft.

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

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

Com este método, você pode fazer com que esse serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações da Política de Grupo

da Microsoft. Para obter mais informações, consulte o documento da Microsoft License your RDS deployment with client access licenses (CALs).

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

1. Instale um Servidor de Licenças de Serviços de Área de Trabalho Remota em uma das máquinas virtuais disponíveis. A VM deve estar sempre disponível. As cargas de trabalho do serviço Citrix devem poder acessar esse servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Specify the Remote Desktop Licensing Mode for an RD Session Host Server

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

Uso confirmado de consumo

> **Nota:**
>
> Esse recurso está como Preview.

No cartão **Geral** no painel **Gerenciar > Implantação Rápida do Azure**, o valor **Consumo** indica quanto consumo foi usado no mês do calendário atual. Esse valor inclui compromissos mensais e com prazo.

Quando você clica em **Geral**, a guia **Notificações** inclui:

- Consumo total usado para o mês (mensal e a termo).
- Número de unidades de compromisso mensal de consumo.
- Porcentagem do compromisso de consumo com prazo.

Os valores e as barras de progresso podem alertá-lo sobre excedentes de uso potenciais ou reais.

Os dados reais podem levar 24 horas para serem exibidos. Os dados de uso e faturamento são considerados finais 72 horas após o fim de um mês.

Para obter mais informações de uso, consulte Monitorar licenças e uso do Citrix DaaS Standard for Azure.

Opcionalmente, você pode solicitar que as notificações apareçam no painel **Gerenciar** quando o uso do consumo (para compromissos mensais, de prazo ou de ambos) atingir um nível especificado. Por padrão, as notificações estão desativadas.

1. Na guia **Notificações**, clique em **Editar preferências de notificação**.
2. Para ativar as notificações, clique no controle deslizante para que a marca de seleção apareça.

3. Insira um valor. Repita para o outro tipo de consumo, se necessário.
4. Clique em **Save**.

Para desativar as notificações, clique no controle deslizante para que a marca de seleção não apareça mais e clique em **Salvar**.

Monitorar o uso de licença Citrix

Para visualizar as informações de uso da licença Citrix, siga as orientações em Monitorar licenças e uso do Citrix DaaS Standard for Azure. Você pode ver:

- Resumo do licenciamento
- Relatórios de uso
- Tendências de uso e atividade de licença
- Usuários licenciados

Você também pode liberar licenças.

Balanceamento de carga

O balanceamento de carga se aplica a máquinas multissessão, não a máquinas de sessão única.

> **Importante:**
>
> Alterar o método de balanceamento de carga afeta todos os catálogos em sua implantação. Isso inclui todos os catálogos criados usando qualquer tipo de host compatível, baseado em nuvem e local, independentemente da interface usada para criá-los (como Studio ou Quick Deploy).
>
> Certifique-se de ter limites máximos de sessão configurados para todos os catálogos antes de continuar.
>
> - Na interface de gerenciamento Quick Deploy para Citrix DaaS for Azure, essa configuração está localizada na guia **Detalhes** de cada catálogo.
> - Em outros serviços e edições do Citrix DaaS, use as configurações de política de gerenciamento de carga.

O balanceamento de carga mede a carga da máquina e determina qual máquina de várias sessões selecionar para uma sessão de usuário de entrada nas condições atuais. Essa seleção é baseada no método de balanceamento de carga configurado.

Você pode configurar um dos dois métodos de balanceamento de carga: horizontal ou vertical. O método se aplica a todos os catálogos de várias sessões (e, portanto, a todas as máquinas com várias sessões) em sua implantação de serviço.

- **Balanceamento de carga horizontal:** Uma sessão de usuário de entrada é atribuída à máquina ligada menos carregada disponível.

  Exemplo simples: você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com cinco sessões simultâneas. A segunda máquina lida com cinco.

  O balanceamento de carga horizontal oferece alto desempenho ao usuário, mas pode aumentar os custos à medida que mais máquinas são mantidas ligadas e ocupadas.

  Esse método está ativado por padrão.

- **Balanceamento de carga vertical:** Uma sessão de usuário de entrada é atribuída à máquina ligada com o maior índice de carga. (O Citrix DaaS for Azure calcula e, em seguida, atribui um índice de carga para cada máquina com várias sessões. O cálculo considera fatores como CPU, memória e simultaneidade.)

  Esse método satura as máquinas existentes antes de passar para novas máquinas. À medida que os usuários se desconectam e liberam capacidade nas máquinas existentes, uma nova carga é atribuída a elas.

  Exemplo simples: você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com as 10 primeiras sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

  Com o balanceamento de carga vertical, as sessões maximizam a capacidade da máquina ligada, o que pode economizar custos com a máquina.

Para configurar o método de balanceamento de carga:

1. No painel **Gerenciar > Implantação Rápida do Azure**, expanda **Geral** à direita.
2. Em **Configurações globais**, clique em **Exibir tudo**.
3. Na página **Configurações Globais**, em **Balanceamento de Carga do Catálogo Multissessão**, escolha o método de balanceamento de carga.
4. Clique em **Confirmar**.

Crie um catálogo em uma rede que usa um servidor proxy

Siga este procedimento se a sua rede exigir um servidor proxy para conectividade com a Internet e você estiver usando sua própria assinatura do Azure. (O uso de uma assinatura do Citrix Managed Azure com uma rede que exige um servidor proxy não é suportado.)

1. No painel **Gerenciar > Implantação Rápida do Azure**, inicie o processo de criação do catálogo fornecendo as informações necessárias e clicando em **Criar Catálogo** na parte inferior da página.

2. A criação do catálogo falha devido ao requisito de proxy. No entanto, um local de recursos é criado. O nome desse local de recurso começa com "DAS", a menos que você tenha fornecido um nome de local de recurso ao criar o catálogo. No console do Citrix DaaS para Azure, expanda **Assinaturas na nuvem**. Na guia **Locais de recursos**, verifique se o local do recurso recém-criado tem algum Cloud Connectors. Se tiver, exclua-os.
3. No Azure, crie duas máquinas virtuais (consulte Requisitos de sistema do Cloud Connector). Ingresse essas máquinas no domínio.
4. No console do Citrix Cloud, instale um Cloud Connector em cada VM. Verifique se os Cloud Connectors estão no mesmo local de recurso criado anteriormente. Siga as orientações em:
   - Configuração de proxy e firewall do Cloud Connector
   - Requisitos de sistema e conectividade
5. No painel **Gerenciar > Implantação Rápida do Azure**, repita o processo de criação do catálogo. Quando o catálogo é criado, ele usa o local de recursos e os Cloud Connectors que você criou nas etapas anteriores.

Obtenha ajuda

- Revise a solução de problemas.
- Se precisar de mais assistência com o Citrix DaaS para Azure, abra um tíquete de suporte seguindo as orientações em Como obter ajuda e suporte.