Citrix DaaS™ para Azure

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix DaaS Padrão para Azure 12
Introdução 12
Como os usuários acessam desktops e aplicativos 13
Conceitos e terminologia 13
Catálogos 13
Locais de recursos 14
Imagens 15
Assinaturas do Azure 16
Conexões de rede 16
Associado a domínio e não associado a domínio 16
Cenários de implantação 18
Implantação em uma assinatura do Azure gerenciada pela Citrix 18
Implantação em uma assinatura do Azure gerenciada pelo cliente 21
Interfaces de gerenciamento 22
Gerenciar catálogos criados na interface do Quick Deploy 22
Mais informações 23
Novidades 25
Atualizações de imagem preparadas pela Citrix® 25
Julho de 2024 25
Agosto de 2022 25
Maio de 2022 26
Abril de 2022 26
Janeiro de 2022 26
Novembro de 2021 27
Outubro de 2021 27
Setembro de 2021 27

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Julho de 2021 27
Junho de 2021 27
Maio de 2021 27
Abril de 2021 28
Janeiro de 2021 28
Outubro de 2020 28
Setembro de 2020 28
Agosto de 2020 28
Julho de 2020 29
Junho de 2020 29
Maio de 2020 29
Março de 2020 29
Fevereiro de 2020 29
Janeiro de 2020 30
Novembro de 2019 30
Outubro de 2019 30
Visão geral de segurança técnica 31
Responsabilidade da Citrix® 32
Assinatura do Azure e Microsoft Entra ID 32
Redes virtuais e infraestrutura 32
Responsabilidade da Citrix ao usar conexões de emparelhamento de VNet do Azure 33
Política de firewall para conexões de emparelhamento de VNet do Azure 33
Acesso à infraestrutura 34
Backups para catálogos não associados ao domínio 34
Backups para imagens de máquina 34
Política de firewall ao usar ferramentas de solução de problemas 35
Assinaturas gerenciadas pelo cliente 35
Responsabilidade do cliente 36

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VDAs e imagens de máquina 36
Responsabilidade do cliente ao usar o emparelhamento de VNet 37
Proxy 37
Resiliência do catálogo 37
Backups para catálogos ingressados no domínio 38
Recuperação de desastres 38
Responsabilidades compartilhadas da Citrix e do cliente 38
Citrix Cloud Connector™ para catálogos ingressados no domínio 38
Solução de problemas 39
Bastions 40
Acesso RDP 40
Credenciais de domínio 41
Mais informações 41
Assinar o Citrix DaaS Standard para Azure 42
Introdução 42
Resumo do pedido 42
Períodos de avaliação 43
Obtenha uma conta Citrix Cloud 43
Se você assina atualmente o Citrix DaaS 43
Fazer pedido através da Citrix 44
Cancelar uma assinatura mensal através da Citrix 44
Quando seu pedido é aprovado e processado 45
Primeiros passos 46
Resumo das tarefas de configuração 46
Preparação 46
Configurar uma implantação rápida de prova de conceito 47
Configurar uma implantação de produção 47
Requisitos do sistema 48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sistemas operacionais suportados 49

URL do Workspace 49

Obter ajuda 49

Criar catálogos 51

Tipos de máquina 51

Maneiras de criar um catálogo 52

Criar um catálogo usando a criação rápida 53

Criar um catálogo usando criação personalizada 54

Criação de catálogos de máquinas unidas ao Microsoft Entra 58

Requisitos 58

Para criar um catálogo 58

Configurações de localização de recursos ao criar um catálogo 59

Esquema de nomenclatura de máquina 60

Informações relacionadas 61

Acesso Remoto a PC 62

Introdução 62

Diferenças em relação à entrega de desktops e aplicativos virtuais 62

Resumo da instalação e configuração 63

Requisitos e considerações 63

Preparar 65

Instalar um VDA 66

Baixar um VDA 66

Tipos de pacote de instalação do VDA do Windows 66

Instalar um VDA do Windows para Acesso Remoto a PC interativamente 67

Instalar um VDA do Windows para Acesso Remoto a PC usando uma linha de comando 68

Instalar um VDA Linux 69

Criar um catálogo de Acesso Remoto para PC 69

Métodos de atribuição de usuário 70

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Métodos para adicionar máquinas a um catálogo 70
Adicionar nomes de máquinas 71
Adicionar UOs 71
Adicionar em massa 71
Gerenciar catálogos do Remote PC Access 72
Assinaturas do Azure 73
Introdução 73
Visualizar assinaturas 74
Adicionar assinaturas do Azure gerenciadas pelo cliente 74
Adicionar assinaturas do Azure gerenciadas pelo cliente se você for um Administrador Global 75
Adicionar assinaturas do Azure gerenciadas pelo cliente se você não for um Administrador Global 75
Crie um aplicativo no Microsoft Entra ID e adicione-o como colaborador 75
Adicionar sua assinatura ao Citrix DaaS para Azure 76
Adicionar assinaturas do Azure gerenciadas pela Citrix 77
Remover assinaturas do Azure 79
Conexões de rede 80
Introdução 80
Requisitos para todas as conexões de rede 80
Sem conectividade 81
Sobre as conexões de emparelhamento de VNet do Azure 81
Rotas personalizadas de emparelhamento de VNet do Azure 83
Requisitos e preparação para emparelhamento de VNet do Azure 84
Criar uma conexão de emparelhamento de VNet do Azure 85
Exibir detalhes da conexão de emparelhamento de VNet do Azure 91
Gerenciar rotas personalizadas para conexões de emparelhamento de VNet do Azure existentes 93

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Excluir uma conexão de emparelhamento de VNet do Azure 94
Gateway VPN do Azure 95
Sobre as conexões de gateway VPN do Azure 95
Rotas personalizadas do gateway VPN do Azure 95
Requisitos e preparação da conexão do gateway VPN do Azure 96
Criar uma conexão de gateway VPN do Azure 96
Visualizar uma conexão de gateway VPN do Azure 100
Gerenciar rotas personalizadas para uma conexão de gateway VPN do Azure 101
Redefinir ou excluir uma conexão de gateway VPN do Azure 102
Criar um endereço IP estático público 102
Imagens 104
Imagens preparadas pela Citrix® 104
Maneiras de usar imagens 104
Exibir informações da imagem 105
Preparar uma nova imagem 106
Conectar-se a uma nova imagem e personalizá-la 109
Importar uma imagem do Azure 110
Requisitos da imagem importada 111
Importar a imagem 111
Atualizar um catálogo com uma nova imagem 113
Excluir uma imagem 114
Instalar um VDA do Windows em uma imagem 114
Usuários e autenticação 116
Métodos de autenticação de usuário 116
Configurar a autenticação de usuário no Citrix Cloud 117
Adicionar e excluir usuários no Managed Microsoft Entra ID 118
Adicionar ou remover usuários em um catálogo 120
Mais informações 122

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gerenciar catálogos 123
Adicionar máquinas a um catálogo 123
Alterar o número de sessões por máquina 124
Gerenciar máquinas em um catálogo 125
Adicionar aplicativos a um catálogo 125
Editar um aplicativo em um catálogo 129
Passar parâmetros para aplicativos publicados 130
Remover aplicativos de um catálogo 130
Excluir um catálogo 130
Gerenciar agendamentos de gerenciamento de energia 131
Informações em um agendamento 131
Agendamentos predefinidos 132
Fuso horário 132
Ligar máquinas: Horário de trabalho e horário pós-expediente 133
Hibernar máquinas: Horário de trabalho e após o expediente 133
Desligar máquinas quando não houver reconexão 133
Desconectar sessões de desktop quando ociosas 133
Desligar desktops ociosos 134
Fazer logoff de sessões desconectadas 134
Atraso de desligamento 134
Mínimo de máquinas em execução 134
Buffer de capacidade 135
Criar um agendamento de gerenciamento de energia 135
Instantâneo e restauração de VDA 136
Agendamentos de instantâneos 136
Snapshots manuais 137
Visualizar e gerenciar snapshots 137
Restaurar 138

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informações relacionadas 138
Monitoramento 139
Monitorar o uso da área de trabalho 139
Relatório de uso da área de trabalho 140
Filtrar e pesquisar para monitorar máquinas e sessões 140
Controlar os aplicativos de um usuário 141
Espelhar usuários 142
Habilitar espelhamento 142
Espelhar VDAs Linux 142
Espelhar VDAs Windows 143
Monitorar e controlar sessões 143
Relatório de informações da sessão 144
Monitorar e controlar a energia das máquinas 144
Relatório de informações da máquina 146
Verificando a integridade de aplicativos e desktops 146
Citrix DaaS™ para Azure para Provedores de Serviços Citrix 147
Requisitos 147
Limitações 147
Problemas conhecidos 147
Adicionar um cliente 147
Adicionar Citrix DaaS for Azure a um cliente 148
Filtrar recursos por cliente 148
Criar catálogos para entregar aplicativos e desktops 149
Domínios federados 149
Adicionar um cliente a um domínio 149
Remover um cliente de um domínio 150
Adicionar um administrador com acesso restrito 150
Acesso do parceiro ao provedor de identidade do cliente 151

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Editar permissões de Administração Delegada para administradores 151
Acessar e configurar espaços de trabalho 152
Monitorar o serviço de um cliente 152
Remover um Serviço 152
Solução de problemas 154
Introdução 154
Solução de problemas de VDA usando um bastion ou RDP direto 154
Métodos de acesso 155
Acesso Bastion 156
Acesso RDP direto 157
Obter ajuda 158
Limites 159
Limites de configuração 159
Limites de localização de recursos 159
Limites de provisionamento 160
Limites de uso 160
Limites de avaliação 160
Referência 162
Painéis 162
Guias de catálogo no painel Gerenciar 162
Servidores DNS 164
Adicionando servidores DNS através do Citrix DaaS para Azure 165
Políticas 166
Definir políticas de grupo para máquinas não associadas a domínio 166
Definir políticas de grupo para máquinas ingressadas no domínio 167
Ações de localização de recursos 167
Executar Verificação de Integridade 168
Reiniciar Conectores 168

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Adicionar Conectores 168

Excluir Conectores 169

Selecionar Hora da Atualização 169

Renomear 169

Configurar Conectividade 169

Gerenciamento de Perfil 169

Configurar o Servidor de Licenças RDS da Microsoft para cargas de trabalho do Windows Server 170

Uso do compromisso de consumo 171

Monitorar o uso de licenças Citrix 172

Balanceamento de carga 172

Criar um catálogo em uma rede que usa um servidor proxy 174

Obter ajuda 174

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS Padrão para Azure

Introdução

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

Esta solução inclui:

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

O recurso Citrix Remote PC Access permite que os usuários usem remotamente máquinas físicas existentes localizadas no escritório. Os usuários recebem a melhor experiência de usuário usando o Citrix HDX™ para fornecer sua sessão de PC do escritório.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Para saber mais sobre componentes, fluxo de dados e considerações de segurança, consulte Visão geral técnica de segurança. 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 até uma URL do Citrix Workspace que é fornecida por você, o administrador. A plataforma Citrix Workspace enumera e entrega os recursos digitais aos usuários. Os usuários iniciam um desktop ou um aplicativo de seu workspace.

Depois de configurar um catálogo de máquinas que entregam desktops e aplicativos (ou um catálogo contendo máquinas físicas para Acesso Remoto a PC), o Citrix DaaS para Azure exibe a URL do Workspace. Em seguida, você notifica seus usuários para acessarem essa URL para iniciar seus desktops e aplicativos.

Como alternativa à navegação para o Citrix Workspace para acessar seus desktops e aplicativos, os usuários podem instalar um aplicativo Citrix Workspace em seu dispositivo. Baixe o aplicativo adequado para o sistema operacional do dispositivo de 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
- Ingressado no domínio e não ingressado no domínio

Catálogos

Um catálogo é um grupo de máquinas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

  Ao implantar desktops, as máquinas no catálogo são compartilhadas com usuários selecionados. Ao publicar aplicativos, máquinas multissessão hospedam aplicativos que são compartilhados com usuários selecionados.
- Para Acesso Remoto a PC, 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 está familiarizado com outros produtos Citrix DaaS, um catálogo no Citrix DaaS é semelhante a combinar uma conexão de hospedagem, um catálogo de máquinas e um grupo de entrega.

Para obter mais informações, consulte:

- Criar catálogos para desktops e aplicativos publicados.
- Criar catálogos para Acesso Remoto a PC.
- Gerenciar catálogos.
- Usuários e autenticação.

Locais de recursos

As máquinas de um catálogo residem em um local de recurso. Um local de recurso também pode conter dois ou mais Cloud Connectors. Os Cloud Connectors são criados apenas para catálogos ingressados no domínio.

- Ao publicar desktops ou aplicativos, o Citrix cria automaticamente o local de recurso e os Cloud Connectors (se ingressados no domínio) ao criar o primeiro catálogo.
- Para Acesso Remoto a PC, o administrador cria o local de recurso e os Cloud Connectors antes de criar um catálogo.

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

Para obter mais informações, consulte:

- Especificar informações de local de recurso ao criar um catálogo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ações de local de recurso.

Imagens

Ao criar um catálogo para desktops e aplicativos publicados, uma imagem de máquina é usada (com outras configurações) como um modelo para criar as máquinas.

- O Citrix DaaS para Azure fornece várias imagens preparadas pela Citrix:
  - Windows 11 Pro (sessão única)
  - Windows 11 Enterprise Virtual Desktop (sessão múltipla)
  - Windows 11 Enterprise Virtual Desktop (sessão múltipla) com Office 365 ProPlus
  - Windows 10 Pro (sessão única)
  - Windows 10 Enterprise Virtual Desktop (sessão múltipla)
  - Windows 10 Enterprise Virtual Desktop (sessão múltipla) com Office 365 ProPlus
  - Windows Server 2019 (sessão múltipla)
  - Windows Server 2022 (sessão múltipla)
  - Windows Server 2025 (sessão múltipla)
  - Linux Ubuntu 22.04 LTS (sessão única)
  - Linux Ubuntu 22.04 LTS (sessão múltipla)

  Cada imagem preparada pela Citrix possui um VDA Citrix e ferramentas de solução de problemas instalados. O VDA é o mecanismo de comunicação entre as máquinas dos seus usuários e a infraestrutura 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 ela possa ser usada para criar um catálogo.

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

Para obter mais informações, consulte Imagens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assinaturas do Azure

Você pode criar catálogos para entregar desktops e aplicativos, e criar/importar imagens em uma assinatura do Azure gerenciada pela Citrix 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 Azure da Citrix, receberá uma assinatura do Azure gerenciada pela Citrix. Você pode então usar uma assinatura do Azure gerenciada pela Citrix ou uma de suas assinaturas do Azure importadas ao criar um catálogo ou construir uma nova imagem.

Para obter mais informações, consulte:

- Cenários de implantação ilustram maneiras de usar assinaturas do Azure com o Citrix DaaS para Azure.
- Assinaturas do Azure explica as diferenças entre as assinaturas do Azure gerenciadas pela Citrix e as gerenciadas pelo cliente. Este artigo também descreve como visualizar, adicionar e remover assinaturas.
- Visão geral de segurança técnica descreve as diferenças de responsabilidade entre as assinaturas do Azure gerenciadas pela Citrix e as gerenciadas pelo cliente.

Conexões de rede

Ao criar um catálogo usando uma assinatura do Azure gerenciada pela Citrix, 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 de VNet do Azure e gateway VPN do Azure.

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

Para obter mais informações, consulte Conexões de rede.

Associado a domínio e não associado a domínio

Várias operações e recursos de serviço diferem, dependendo se as máquinas (VDAs) estão associadas a um domínio ou não. A associação ao domínio também afeta os cenários de implantação disponíveis.

- Máquinas associadas a domínio e não associadas a domínio suportam qualquer um dos métodos de autenticação de usuário disponíveis no espaço de trabalho do usuário.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Você pode publicar desktops, aplicativos ou ambos a partir de máquinas associadas a domínio e não associadas a domínio. As máquinas em catálogos de Acesso Remoto a PC devem ser associadas a domínio.

A tabela a seguir lista várias diferenças entre máquinas não associadas a domínio e associadas a domínio ao entregar desktops e aplicativos.

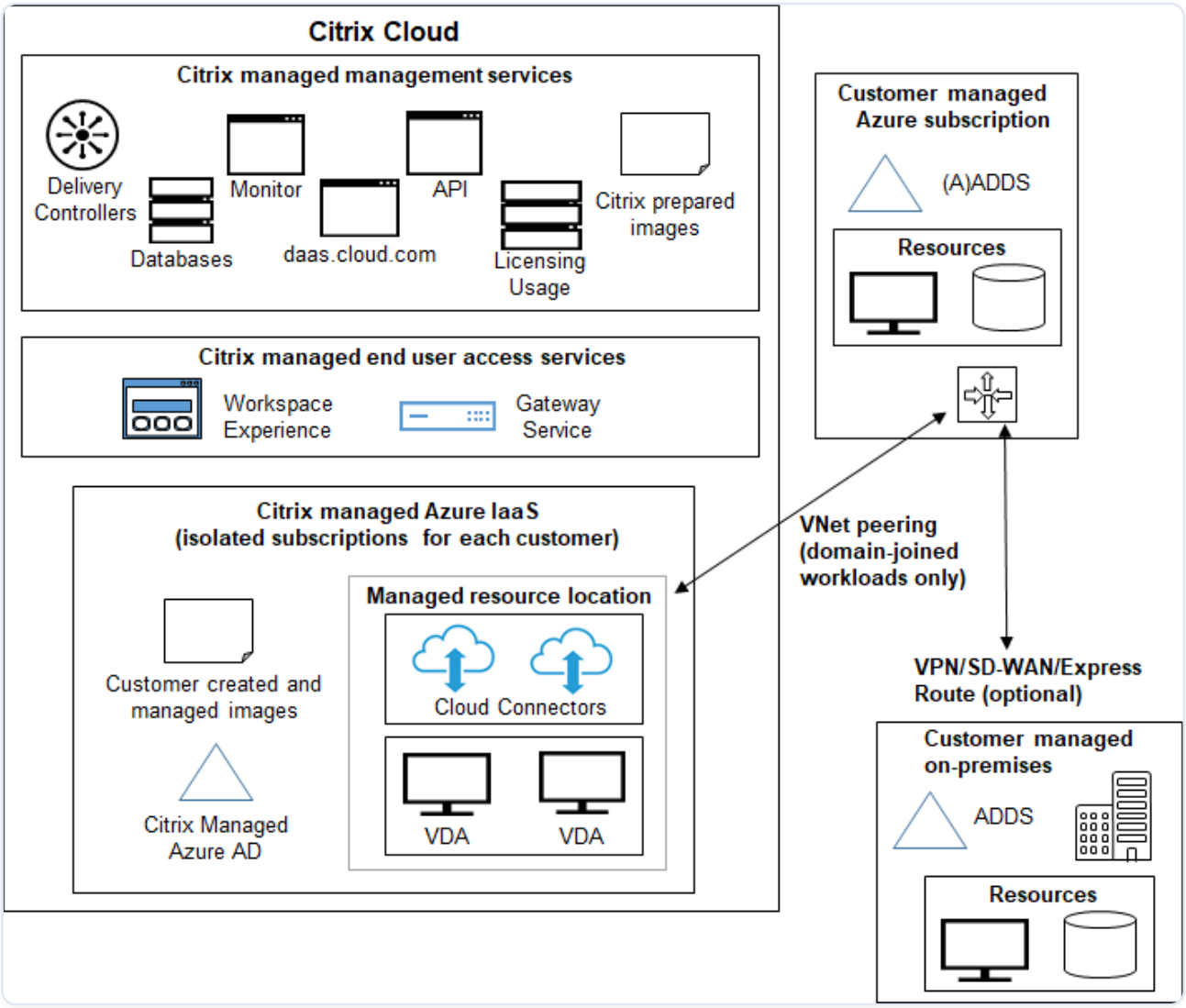
NÃO ASSOCIADO A DOMÍNIO	ASSOCIADO A DOMÍNIO
O Active Directory não é usado para máquinas. As máquinas não estão associadas a um domínio AD.	O Active Directory é usado para máquinas. As máquinas estão associadas a um domínio AD.
As políticas de grupo do Active Directory não podem ser aplicadas a máquinas (VDAs). (Você pode aplicar GPO local na imagem usada para criar um catálogo.)	Os VDAs herdam as políticas de grupo para a OU do AD especificada durante a criação do catálogo.
Os usuários fazem login usando logon único.	Quando os usuários fazem login em seu espaço de trabalho usando um método de autenticação diferente do Active Directory, o FAS deve ser configurado para obter logon único.
Não precisam de uma conexão com uma rede local.	(Ao usar uma assinatura do Azure gerenciada pela Citrix) Deve ter uma conexão para acessar uma rede local, usando o Microsoft Azure VNet ou o gateway VPN do Azure.
Sem Cloud Connectors.	Os Cloud Connectors são criados automaticamente.
Não é possível solucionar problemas usando uma máquina bastion ou RDP direto.	É possível solucionar problemas usando uma máquina bastion ou RDP direto.
Não é possível usar o Citrix Profile Management. (Recomendado: Use catálogos persistentes.)	É possível usar o Citrix Profile Management ou o FSLogix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cenários de implantação

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

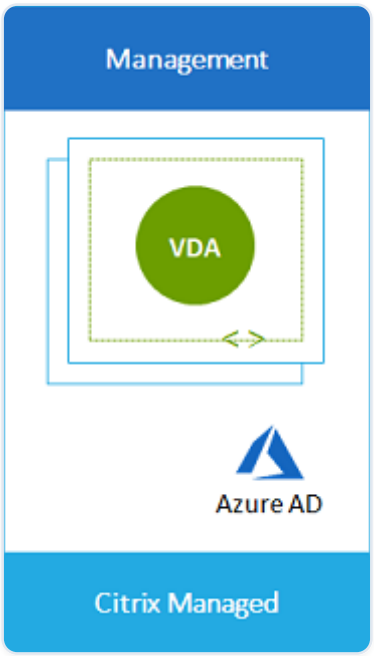
Implantação em uma assinatura do Azure gerenciada pela Citrix



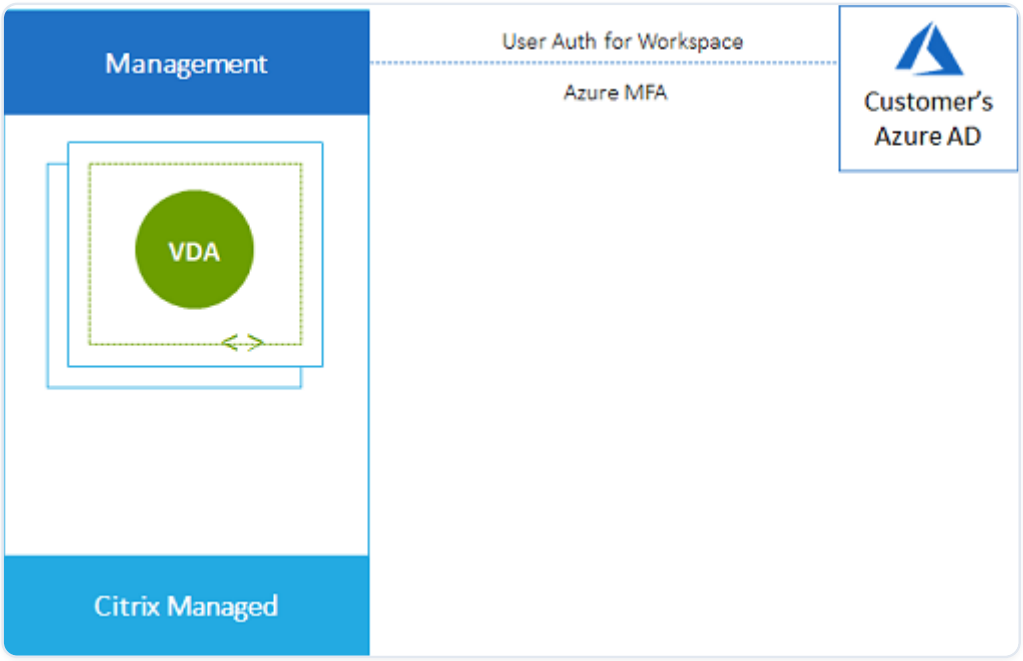
O Citrix DaaS para Azure oferece suporte a vários cenários de implantação para conexão e autenticação de usuário.

- **Managed Microsoft Entra ID:** Esta é a implantação mais simples, com VDAs não associados a domínio. É recomendada para provas de conceito. Você usa o Managed Microsoft Entra ID (que a Citrix gerencia) para gerenciar usuários. Seus usuários não precisam acessar recursos em sua rede local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

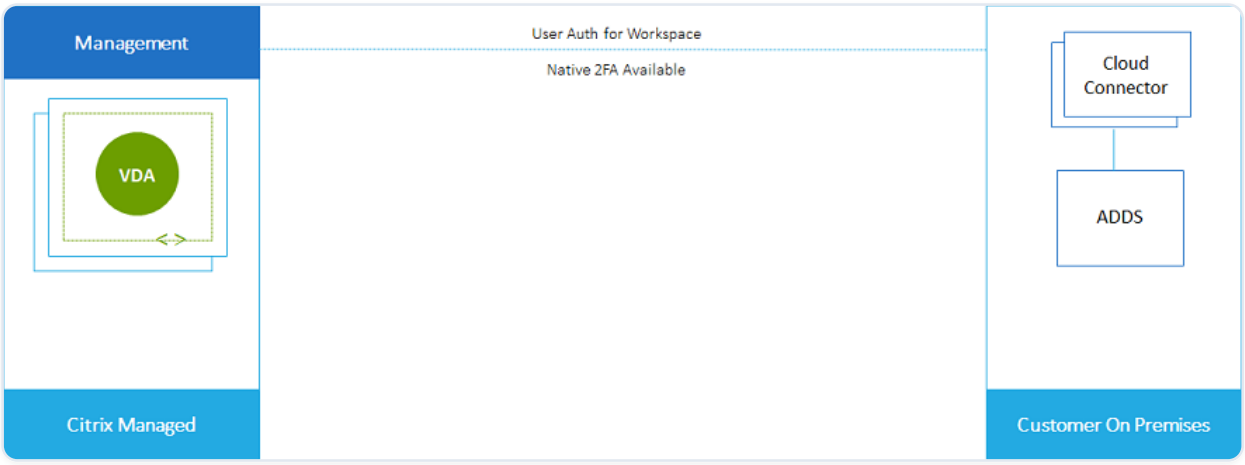


- **Microsoft Entra ID do Cliente:** Esta implantação contém VDAs não associados a domínio. Você usa seu próprio Active Directory ou Microsoft Entra ID para autenticação de usuário final. Neste cenário, seus usuários não precisam acessar recursos em sua rede local.

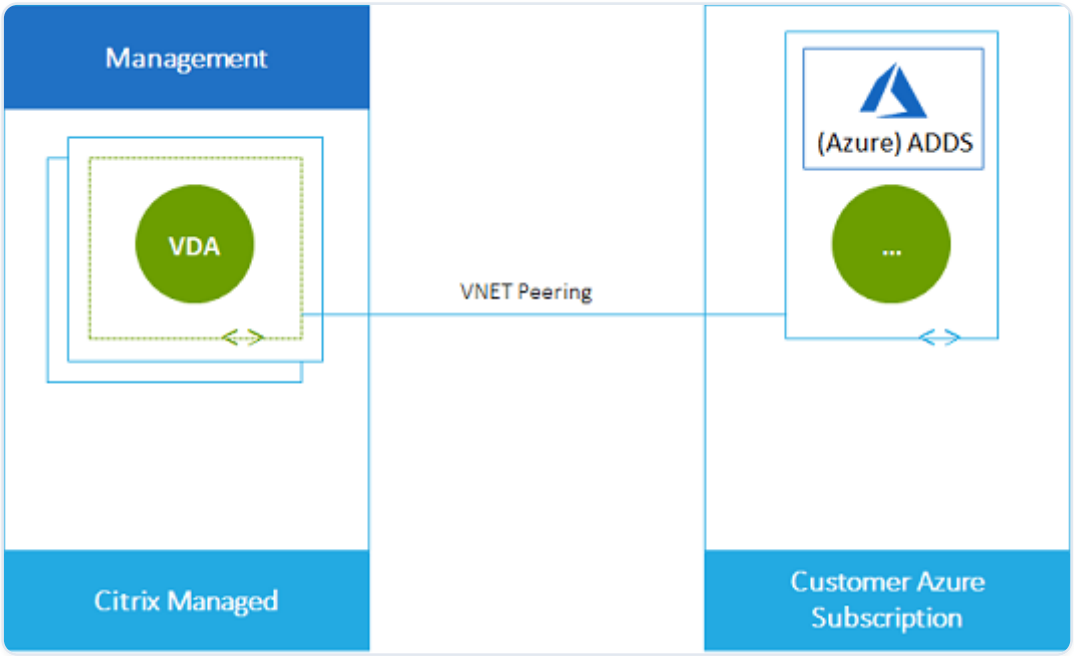


- **ID do Microsoft Entra do cliente com acesso local:** Esta implantação contém VDAs não associados a domínio. Você usa seu próprio AD ou AAD para autenticação de usuário final. Neste cenário, a instalação de Citrix Cloud Connectors em sua rede local permite o acesso a recursos nessa rede.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

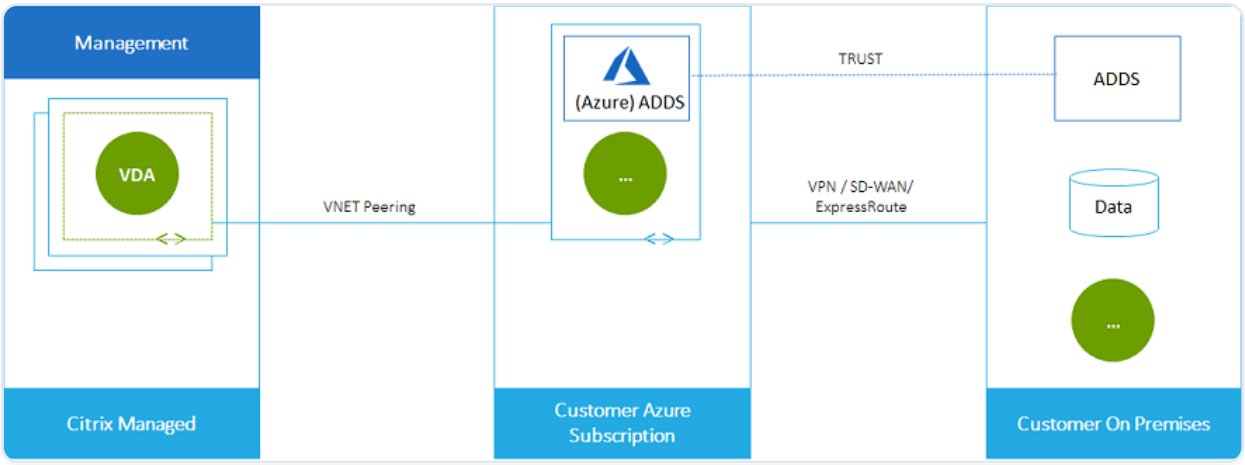


- **Serviços de Domínio do Microsoft Entra do cliente e emparelhamento de VNet:** Se seu AD ou AAD residir em sua própria VNet do Azure e assinatura do Azure, você poderá usar o recurso de emparelhamento de VNet do Microsoft Azure para uma conexão de rede e os Serviços de Domínio do Microsoft Entra para autenticação de usuário final. Os VDAs são associados ao seu domínio.

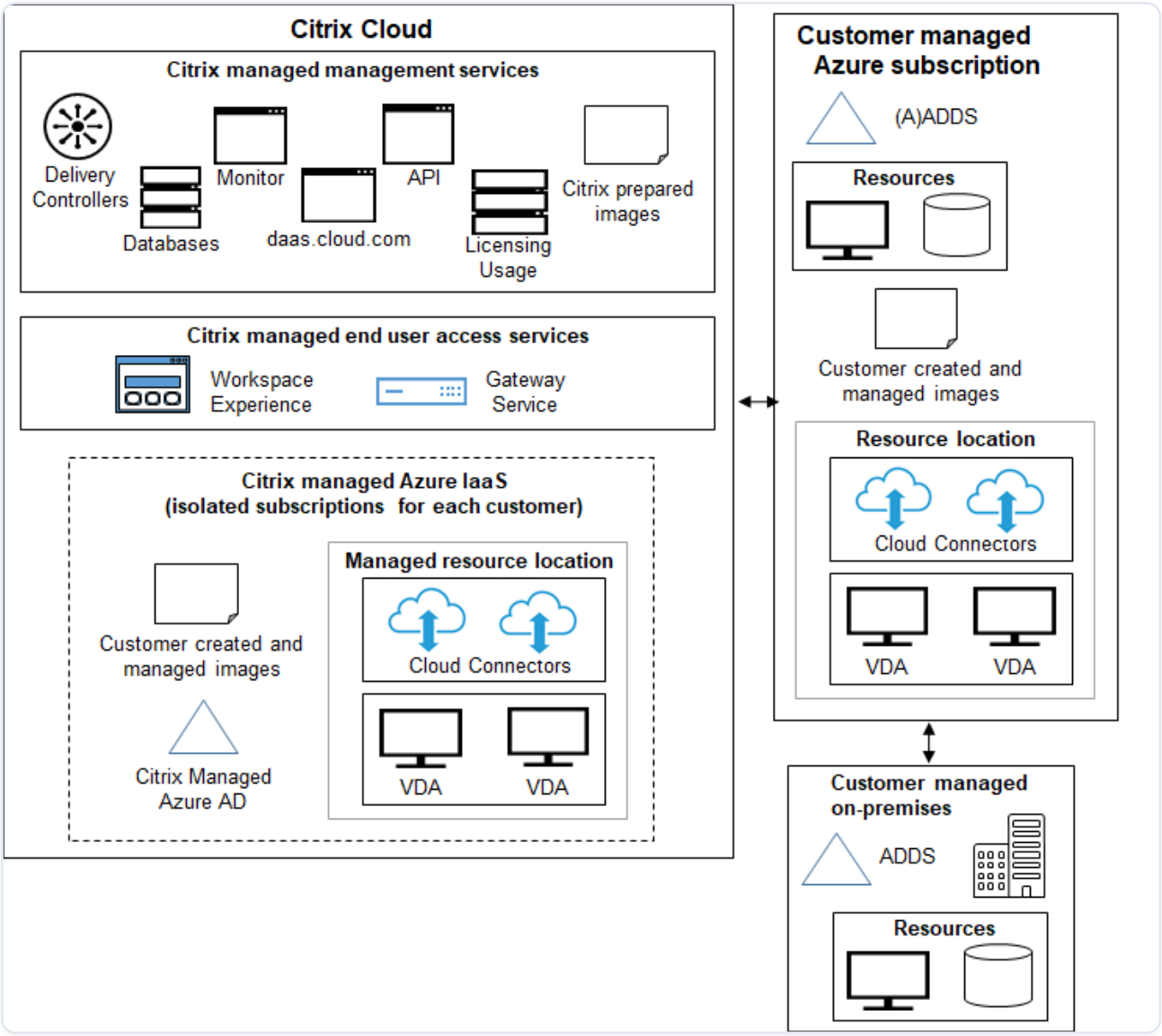


Para permitir que seus usuários acessem dados armazenados em sua rede local, você pode usar sua conexão VPN de sua assinatura do Azure para o local local. O emparelhamento de VNet do Azure é usado para conectividade de rede. Os Serviços de Domínio do Active Directory no local local são usados para autenticação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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 Azure gerenciada pela Citrix continua sendo uma opção para outros catálogos e imagens, conforme indicado pelo contorno pontilhado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Interfaces de gerenciamento

O Citrix DaaS para Azure possui duas interfaces gráficas de gerenciamento: Quick Deploy e Web Studio.

- **Quick Deploy** permite que você crie rapidamente catálogos e comece a entregar desktops e aplicativos aos seus usuários. (Daí o nome, Quick Deploy.) É a interface padrão ao iniciar o Citrix DaaS para Azure. Você também pode acessar esta interface selecionando **Quick Deploy > Microsoft Azure**. As instruções neste conjunto de documentação do produto pressupõem que você esteja usando o Quick Deploy.

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

- **Web Studio** oferece recursos avançados e opções de configuração para personalizar e gerenciar sua implantação. Os catálogos que você cria no Quick Deploy aparecem automaticamente no Web Studio.

  Ao criar um catálogo no Quick Deploy, um catálogo de máquinas associado, um grupo de entrega e uma conexão de host são criados automaticamente no Web Studio.

  O Web Studio também oferece seu próprio processo de criação de catálogo que inclui a criação de uma conexão com o host do Azure, e então a criação de um catálogo e de um grupo de entrega. Esse processo é suportado apenas se você usar sua própria assinatura do Azure. É muito mais fácil criar o catálogo no Quick Deploy.

  O Web Studio suporta processos relacionados a hosts de hipervisor e serviços de nuvem que não sejam o Azure. Esses não estão disponíveis para clientes do Citrix DaaS para Azure.

Gerenciar catálogos criados na interface do Quick Deploy

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

Ao criar um catálogo no Quick Deploy, esse catálogo (além do grupo de entrega e da conexão de hospedagem que são criados automaticamente nos bastidores) recebe um escopo de `Citrix managed object`. Os escopos são usados na administração delegada para agrupar objetos.

Catálogos, grupos de entrega e conexões com o escopo `Citrix managed object` são proibidos de certas ações na interface do Web Studio. (Permitir essas ações no Web Studio pode afetar

© 1997–2026 Citrix Systems, Inc. All rights reserved.

adversamente a capacidade do sistema de suportar tanto o Quick Deploy quanto o Web Studio, então essas ações são desabilitadas.) Na interface do Web Studio:

- **Catálogo:** A maioria das ações de gerenciamento de catálogo não está disponível. Você não pode excluir um catálogo.
- **Grupo de entrega:** A maioria das ações de gerenciamento de 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 no Quick Deploy usando sua própria assinatura do Azure (que você adicionou ao Quick Deploy) e quiser gerenciar o catálogo (e seu grupo de entrega e conexão) inteiramente no Web Studio, você pode *converter* o catálogo.

- A conversão de um catálogo restringe seu gerenciamento apenas à interface do Web Studio. Depois que um catálogo é convertido, você não pode mais usar a interface do Quick Deploy para gerenciar esse catálogo.
- Depois que um catálogo é convertido, as ações que antes não estavam disponíveis no Web Studio podem ser selecionadas. (O escopo `Citrix managed object` é removido do catálogo, grupo de entrega e conexão de hospedagem convertidos.)
- Para converter um catálogo:

  No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, clique em qualquer lugar na entrada do catálogo. Na guia **Detalhes**, em **Configurações avançadas**, selecione **Converter Catálogo**. Quando solicitado, confirme a conversão.
- Você não pode converter um catálogo que foi criado no Quick Deploy usando uma assinatura do Azure gerenciada pela Citrix.

Para obter informações sobre como gerenciar catálogos convertidos no Web Studio, consulte:

- Gerenciar catálogos de máquinas (o Web Studio se refere aos catálogos como catálogos de máquinas)
- Gerenciar grupos de entrega

Mais informações

Para detalhes técnicos, consulte:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Tech Zone arquitetura de referência

Para obter informações sobre como automatizar suas implantações, consulte as APIs de Implantação Rápida do serviço de Catálogo.

Quando estiver pronto, comece.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Novidades

Um objetivo da Citrix é fornecer novos recursos e atualizações de produtos para os clientes do Citrix DaaS™ para Azure assim que estiverem disponíveis. Novos lançamentos oferecem mais valor, portanto, não há razão para atrasar as atualizações. Para você, administrador do cliente, este processo é transparente.

Atualizações de imagem preparadas pela Citrix®

As imagens preparadas pela Citrix têm um Citrix Virtual Delivery Agent (VDA) atual 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 os recursos novos e aprimorados na versão atual do VDA, consulte:

- VDAs do Windows
- VDAs do Linux

Julho de 2024

Suporte à hibernação. Agora você pode criar máquinas virtuais que podem ser hibernadas. Enquanto uma máquina está hibernando, você não é cobrado pelo seu uso e economiza no consumo de energia. 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 agendamentos de hibernação, consulte Criar um catálogo usando 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 de 2022

- Este recurso está geralmente disponível: Agora você pode criar catálogos de máquinas unidas ao seu Azure Active Directory. Consulte Criar catálogos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Maio de 2022

- Agora você pode criar catálogos de máquinas unidas ao seu Azure Active Directory. Este recurso está em pré-visualização. Consulte Criar catálogos.
- Os Provedores de Serviços Citrix agora podem remover o serviço Citrix DaaS para Azure dos clientes. Consulte Remover um Serviço.

Abril de 2022

- A criação de conexão de host para Citrix Hypervisor™, Microsoft SCVMM, VMware vSphere, Prism Central e Nutanix AHV agora está disponível. Sendo assim, agora você pode usar hipervisores locais além do Azure.
- Mudança do nome do produto de Citrix Virtual Apps and Desktops Standard for Azure para Citrix DaaS Standard for Azure. Para obter mais informações sobre a reformulação da marca de todas as ofertas do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), consulte Novidades no Citrix DaaS. Saiba mais sobre as mudanças de nome em nosso anúncio em nosso blog.

Janeiro de 2022

- Ao criar catálogos, agora você pode armazenar suas máquinas em armazenamento SSD padrão. Anteriormente, apenas discos padrão (HDD) e SSD premium eram suportados.
- Suporte para estas novas regiões para hospedar cargas de trabalho VDA: Brasil Sul, Índia Central, Japão Leste, Centro-Sul dos EUA e Reino Unido Sul.
- Snapshots e restauração agora estão disponíveis para desktops persistentes hospedados no Citrix Managed Azure e BYO Azure. Consulte Snapshot e restauração de VDA.
- Endereço IP público estático para todo o tráfego de saída de VDAs hospedados agora está disponível. Você pode configurar um Azure NAT Gateway para obter o endereço IP. Consulte Criar um endereço IP público estático.
- O Azure VPN está disponível para visualização técnica. O Azure VPN permite conectar o Citrix Managed Azure diretamente com data centers locais. Consulte Visualização Técnica do Azure VPN.
- Novas imagens Linux estão disponíveis para imagens preparadas pela Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Novembro de 2021

- Testes de 7 dias trials aprovados automaticamente agora estão disponíveis (além dos testes aprovados por vendas).
- Os Citrix Service Providers agora podem gerenciar usuários a partir do painel **Quick Deploy > Microsoft Azure** do serviço ou do console do Citrix Cloud. Para obter detalhes, consulte Acesso do parceiro ao provedor de identidade do cliente.

Outubro de 2021

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

Setembro de 2021

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

Julho de 2021

- A interface de gerenciamento do Web Studio foi renomeada para Configuração Completa.

Junho de 2021

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

Maio de 2021

- Este serviço oferece suporte à visualização de Continuidade do Serviço.
- Imagens preparadas pela Citrix agora incluem versões Ubuntu de sessão única e multi-sessão.
- Ao adicionar um Cloud Connector a um local de recurso, usando uma assinatura do Azure gerenciada pela Citrix, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Abril de 2021

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

Janeiro de 2021

- Suporte de visualização para exibir uso de compromisso de consumo.

Outubro de 2020

- Você pode usar o recurso Monitor shadow para visualizar ou trabalhar na VM ou sessão de um usuário.
- Suporte de produção para Acesso Remoto a PC.
- Opção aprimorada de criação de catálogo para usar sua licença elegível do Azure Virtual Desktop ou o Azure Hybrid Benefit.
- Se uma ação de reinicialização em uma máquina não for bem-sucedida, você poderá usar uma ação de reinicialização forçada.

Setembro de 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 de 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 de 2020

- Suporte de visualização para Acesso Remoto a PC.
- Uma imagem do Windows Server 2019 preparada pela Citrix agora está disponível.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 local de recurso.
- Ao criar um catálogo, você pode especificar um esquema de nomenclatura de máquina. Consulte Criar um catálogo usando criação personalizada.

Junho de 2020

- Em um ambiente CSP, as conexões SD-WAN são criadas por locatário. Para que a opção de conexão SD-WAN esteja disponível para o administrador CSP, o locatário deve ter um direito de serviço do SD-WAN Orchestrator. Para detalhes, consulte Filtrar recursos por cliente (implantações multilocatário).
- Suporte de produção para VDAs Linux ao usar uma assinatura do Azure gerenciada pelo cliente.
- O limite de VDAs por assinatura agora é de 1.200.

Maio de 2020

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

Março de 2020

- Suporte de produção para conexões SD-WAN.

Fevereiro de 2020

- Para visualizar suas informações de uso de licença da Citrix, siga as orientações em Monitorar o monitoramento de licenças e uso para Citrix DaaS Standard para Azure.
- Suporte de visualização para catálogos contendo máquinas Red Hat Enterprise Linux ou Ubuntu. Este recurso é válido apenas ao usar uma assinatura do Azure gerenciada pelo cliente e requer uma imagem importada contendo um VDA Linux da Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Agora você pode configurar o balanceamento de carga vertical ou horizontal para todas as suas máquinas multissessão. (Anteriormente, todas as máquinas usavam balanceamento de carga horizontal.) Esta seleção global se aplica a todos os catálogos em sua implantação. Consulte Balanceamento de carga.
- Agora você pode adicionar uma assinatura do Azure se não for um Administrador Global.
- Uma imagem preparada pela Citrix agora está disponível para Windows 10 Enterprise Virtual Desktop (multissessão) com Office 365 ProPlus.

Janeiro de 2020

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

Novembro de 2019

- Suporte de visualização para conexões SD-WAN.

Outubro de 2019

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

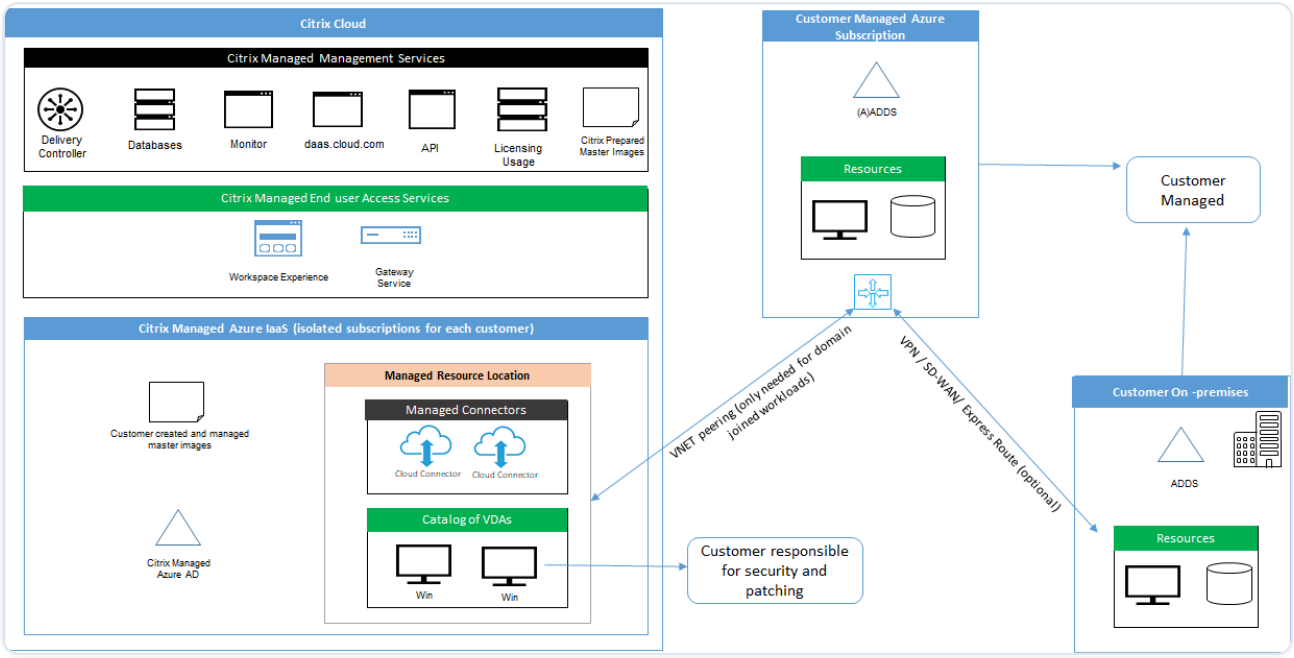
Setembro de 2019

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Visão geral de segurança técnica

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 de VNet.



Com o Citrix DaaS for Azure, os Virtual Delivery Agents (VDAs) do cliente que entregam desktops e aplicativos, além dos 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 Azure gerenciada pela Citrix. Para uma visão geral arquitetônica de uma implantação do Citrix DaaS for Azure usando uma assinatura do Azure gerenciada pelo cliente, incluindo informações de segurança, consulte Arquitetura de Referência: Serviço Virtual Apps and Desktops - Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Responsabilidade da Citrix®

Assinatura do Azure e Microsoft Entra ID

A Citrix é responsável pela segurança da assinatura do Azure e do Microsoft Entra ID que são criados para o cliente. A Citrix garante o isolamento do locatário, de modo que cada cliente tenha sua própria assinatura do Azure e AAD, e a comunicação cruzada entre diferentes locatários seja evitada. A Citrix também restringe o acesso ao AAD apenas ao Citrix DaaS™ for Azure e ao pessoal de operações da Citrix. O acesso da Citrix à assinatura do Azure de cada cliente é auditado.

Clientes que utilizam catálogos não associados a domínio podem usar o AAD gerenciado pela Citrix como um meio de autenticação para o 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 executar quaisquer ações no AAD gerenciado pela Citrix. Se esses clientes optarem por usar seu próprio AAD, eles serão totalmente responsáveis pela segurança dele.

Redes virtuais e infraestrutura

Dentro da assinatura do Azure gerenciada pela Citrix do cliente, a Citrix cria redes virtuais para isolar locais de recursos. Dentro dessas redes, a Citrix cria máquinas virtuais para os VDAs, Cloud Connectors e máquinas de criação de imagem, além de contas de armazenamento, Key Vaults e outros recursos do Azure. A Citrix, em parceria com a Microsoft, é responsável pela segurança das redes virtuais, incluindo firewalls de rede virtual.

A Citrix garante que a política de firewall padrão do Azure (grupos de segurança de rede) seja configurada para limitar o acesso a interfaces de rede em conexões de emparelhamento de VNet. Geralmente, isso controla o tráfego de entrada para VDAs e Cloud Connectors. Para detalhes, consulte:

- Política de firewall para conexões de emparelhamento de VNet do Azure

Os clientes não podem alterar esta política de firewall padrão, mas podem implantar regras de firewall adicionais nas máquinas VDA criadas pela Citrix; por exemplo, para restringir parcialmente o tráfego de saída. Clientes que instalam clientes de rede privada virtual, ou outro software capaz de ignorar 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 para Azure para criar e personalizar uma nova imagem de máquina, a porta 3389 é aberta temporariamente na VNet gerenciada pela Citrix, para

© 1997–2026 Citrix Systems, Inc. All rights reserved.

que o cliente possa fazer RDP para a máquina que contém a nova imagem de máquina, a fim de personalizá-la.

Responsabilidade da Citrix ao usar conexões de emparelhamento de VNet do Azure

Para que os VDAs no Citrix DaaS para Azure entrem em contato com controladores de domínio locais, compartilhamentos de arquivos ou outros recursos de intranet, o Citrix DaaS para Azure oferece 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 do 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 da nuvem para o local de escolha do cliente, como Azure ExpressRoute ou túneis iPsec.

A responsabilidade da Citrix pelo emparelhamento de VNet limita-se a dar suporte ao fluxo de trabalho e à configuração de recursos do Azure relacionados para estabelecer o relacionamento de emparelhamento entre as VNets gerenciadas pela Citrix e pelo cliente.

Política de firewall para conexões de emparelhamento de VNet do Azure

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

VNet gerenciada pela Citrix com máquinas não ingressadas no domínio

- Regras de entrada
  - Negar todo o tráfego de entrada. Isso inclui o tráfego intra-VNet de VDA para VDA.
- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pela Citrix com máquinas ingressadas no domínio

- Regras de entrada:
  - Permitir as portas 80, 443, 1494 e 2598 de entrada internamente para os VDAs e Connectors.
  - Permitir as portas 49152-65535 de entrada para os VDAs de um intervalo de IP usado pelo recurso de sombreamento do Monitor. Consulte Portas de comunicação usadas pelas tecnologias Citrix.
  - Negar todo o outro tráfego de entrada.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Regras de saída
  - Permitir todo o tráfego de saída.

VNet gerenciada pelo cliente com máquinas ingressadas no domínio

- Cabe ao cliente configurar sua VNet corretamente. Isso inclui a abertura das seguintes portas para ingresso no domínio.
- Regras de entrada:
  - Permitir entrada nas portas 443, 1494, 2598 dos IPs de seus clientes para inicializações internas.
  - Permitir entrada nas portas 53, 88, 123, 135-139, 389, 445, 636 da VNet Citrix (intervalo de IP especificado pelo cliente).
  - Permitir entrada nas portas abertas com uma configuração de proxy.
  - Outras regras criadas pelo cliente.
- Regras de saída:
  - Permitir saída nas portas 443, 1494, 2598 para a VNet Citrix (intervalo de IP especificado pelo cliente) para inicializações internas.
  - Outras regras criadas pelo cliente.

Acesso à infraestrutura

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

Backups para catálogos não associados ao domínio

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

Backups para imagens de máquina

A Citrix é responsável por fazer backup de quaisquer imagens de máquina carregadas para o Citrix DaaS para Azure, incluindo imagens criadas com o construtor de imagens. A Citrix usa armazenamento localmente redundante para essas imagens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Política de firewall ao usar ferramentas de solução de problemas

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

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

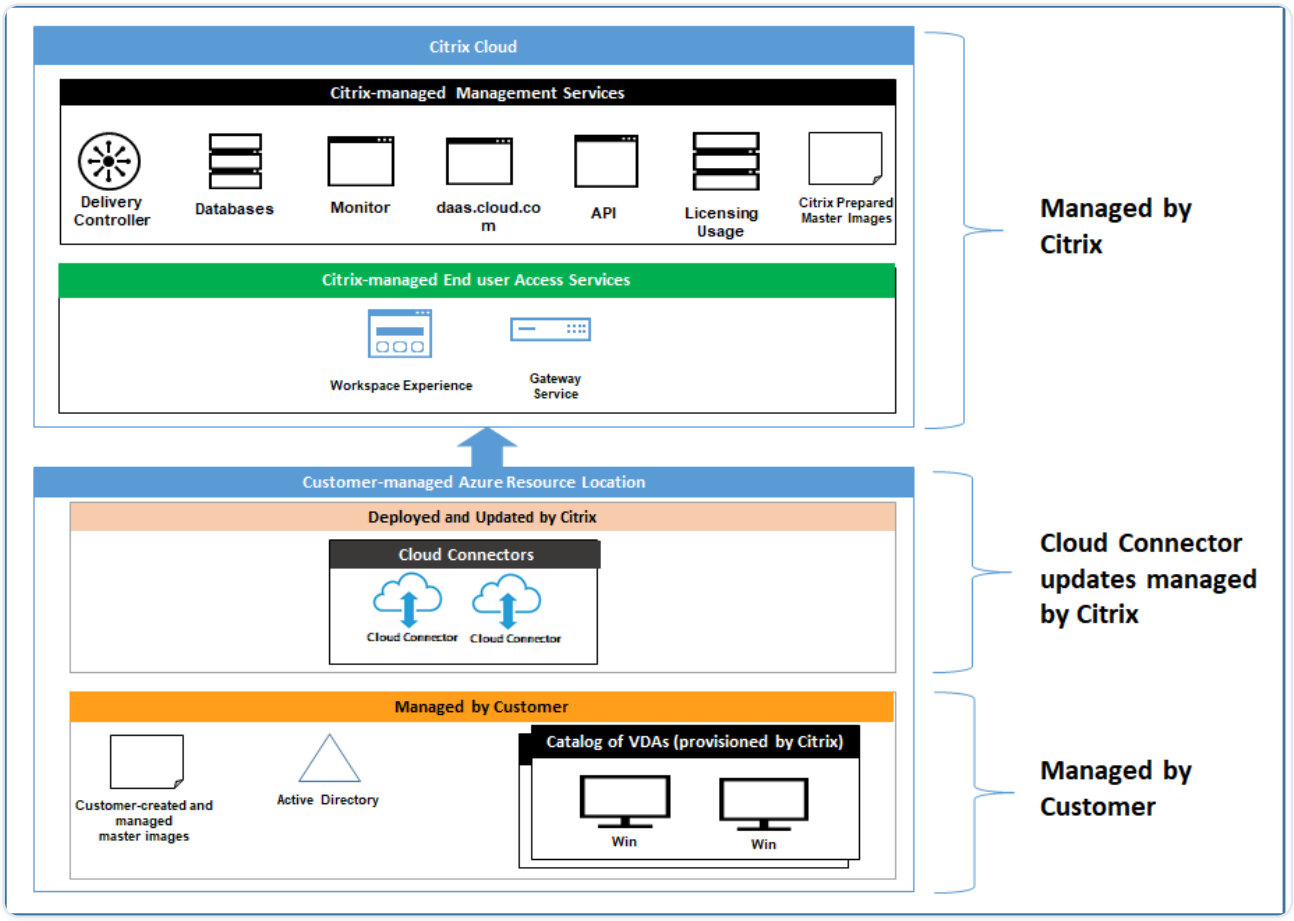
Quando um cliente habilita o acesso RDP para solução de problemas, as seguintes modificações de grupo de segurança são feitas na VNet gerenciada pela Citrix:

- Permitir temporariamente 3389 de entrada do intervalo de IP especificado pelo cliente para qualquer endereço na VNet (VDAs e Cloud Connectors).
- Continuar a bloquear o acesso RDP entre os Cloud Connectors, 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 o que foi mencionado acima passa a ser responsabilidade do cliente, pois o cliente é o proprietário da assinatura do Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Responsabilidade do cliente

VDAs e imagens de máquina

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 VDA e patches de segurança
- Regras adicionais de firewall de software (especialmente tráfego de saída)
- Siga as considerações de segurança e melhores práticas da Citrix

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Responsabilidade do cliente ao usar o emparelhamento de VNet

O cliente deve abrir todas as portas especificadas em VNet gerenciada pelo cliente com máquinas ingressadas no domínio.

Quando o emparelhamento de VNet é configurado, o cliente é responsável pela segurança de sua própria rede virtual e sua conectividade 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 para os recursos locais do cliente.

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

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

Proxy

O cliente pode escolher se deseja usar um proxy para o tráfego de saída do VDA. Se um proxy for usado, o cliente é responsável por:

- Configurar as configurações do proxy na imagem da máquina VDA ou, se o VDA estiver ingressado em um domínio, usando a Política de Grupo do Active Directory.
- Manutenção e segurança do proxy.

Proxies não são permitidos para uso com Citrix Cloud Connectors ou outras infraestruturas gerenciadas pela Citrix.

Resiliência do catálogo

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

- **Estático:** Cada usuário é atribuído a um único VDA. Este tipo de catálogo não oferece alta disponibilidade. Se o VDA de um usuário falhar, ele terá que ser colocado em um novo para recuperação. O Azure oferece um SLA de 99,5% para VMs de instância única com SSDs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

padrão. O cliente ainda pode fazer backup do perfil do usuário, mas quaisquer personalizações feitas no VDA (como instalação de programas ou configuração do Windows) serão perdidas.

- **Aleatório:** Cada usuário é atribuído aleatoriamente a um VDA de servidor no momento do lançamento. Este tipo de catálogo oferece alta disponibilidade por meio de redundância. Se um VDA falhar, nenhuma informação será perdida porque o perfil do usuário reside em outro lugar.
- **Windows 10 multissessão:** Este tipo de catálogo opera da mesma forma que o tipo aleatório, mas usa VDAs de estação de trabalho Windows 10 em vez de VDAs de servidor.

Backups para catálogos ingressados no domínio

Se o cliente usar catálogos ingressados no domínio com um emparelhamento de 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 seu Active Directory ou VDAs para extrair perfis de usuário desses compartilhamentos de arquivos. O cliente é responsável pelo backup e disponibilidade desses compartilhamentos de arquivos.

Recuperação de desastres

Em caso de perda de dados do Azure, a Citrix recuperará o máximo de recursos possível 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 por criar um novo catálogo. A Citrix assume que as imagens de máquina têm backup e que os clientes fizeram backup de seus perfis de usuário, permitindo que o catálogo seja reconstruído.

Em caso de perda de uma região inteira do Azure, o cliente é responsável por reconstruir sua rede virtual gerenciada pelo cliente em uma nova região e criar um novo emparelhamento de VNet dentro do Citrix DaaS para Azure.

Responsabilidades compartilhadas da Citrix e do cliente

Citrix Cloud Connector™ para catálogos ingressados no domínio

O Citrix DaaS para 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 de VNet e domínio que outros catálogos para o mesmo cliente. A Citrix configura os Cloud Connectors ingressados no domínio do cliente para as seguintes configurações de segurança padrão na imagem:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Os clientes também têm controle sobre os Cloud Connectors ingressados no domínio por meio da Política de Grupo do Active Directory. O cliente é responsável por garantir que as políticas de grupo aplicadas ao Cloud Connector sejam seguras e sensatas. Por exemplo, se o cliente optar por desabilitar as atualizações do sistema operacional usando a Política de Grupo, o cliente será responsável por realizar as atualizações do sistema operacional nos Cloud Connectors. O cliente também pode optar por usar a Política de Grupo para impor uma segurança mais rigorosa do que as configurações padrão do Cloud Connector, como instalando um software antivírus diferente. Em geral, a Citrix recomenda que os clientes coloquem os Cloud Connectors em sua própria unidade organizacional do Active Directory sem políticas, pois isso garantirá que as configurações padrão que a Citrix usa possam ser aplicadas sem problemas.

Solução de problemas

Caso o cliente enfrente problemas com o catálogo no Citrix DaaS para Azure, há duas opções para solução de problemas: usar bastions e habilitar o acesso RDP. Ambas as opções introduzem risco de segurança para o cliente. O cliente deve entender e consentir em 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 por restringir quais máquinas podem ser acessadas durante essas operações.

Com bastions ou acesso RDP, o usuário ativo que realiza a operação é responsável pela segurança das máquinas que estão sendo acessadas. Se o cliente acessar o VDA ou Cloud Connector via RDP e acidentalmente contrair um vírus, o cliente é o responsável. Se o pessoal do Suporte Citrix acessar essas máquinas, é responsabilidade desse pessoal realizar as operações com segurança. A responsabilidade por quaisquer vulnerabilidades expostas por qualquer pessoa que acesse o bastion ou outras máquinas na implantação (por exemplo, responsabilidade do cliente de adicionar intervalos de IP à lista de permissões, responsabilidade da Citrix de implementar intervalos de IP corretamente) é abordada em outras partes deste documento.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Em ambos os 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 descarta o bastion ou encerra o acesso RDP através do Citrix DaaS para Azure.

Bastions

A Citrix pode criar bastiões na rede virtual gerenciada pela Citrix do cliente, dentro da assinatura gerenciada pela Citrix do cliente, para diagnosticar e reparar problemas, seja proativamente (sem notificação do cliente) ou em resposta a um problema levantado pelo cliente. O bastião é uma máquina que o cliente pode acessar via RDP e, em seguida, usar para acessar os VDAs e (para catálogos ingressados no domínio) os Cloud Connectors via RDP para coletar logs, reiniciar serviços ou executar outras tarefas administrativas. Por padrão, a criação de um bastião abre uma regra de firewall externa para permitir o tráfego RDP de um intervalo de endereços IP especificado pelo cliente para a máquina bastião. Também abre uma regra de firewall interna para permitir o acesso aos Cloud Connectors e VDAs via 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 externos que permita o acesso RDP ao bastião. 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 acesso tentado por endereços IP maliciosos.

O cliente também é responsável por excluir o bastião após a conclusão da solução de problemas. O host bastião expõe uma superfície de ataque adicional, então a Citrix desliga automaticamente a máquina oito (8) horas após ser ligada. No entanto, a Citrix nunca exclui automaticamente um bastião. Se o cliente optar por usar o bastião por um período prolongado, ele será responsável por aplicar patches e atualizá-lo. A Citrix recomenda que um bastião seja usado apenas por alguns dias antes de ser excluído. Se o cliente quiser um bastião atualizado, ele pode excluir o atual e criar um novo bastião, que provisionará uma máquina nova com os patches de segurança mais recentes.

Acesso RDP

Para catálogos ingressados no domínio, se o emparelhamento de VNet do cliente estiver funcional, o cliente pode habilitar o acesso RDP de sua VNet emparelhada para sua VNet gerenciada pela Citrix. Se o cliente usar esta opção, ele será responsável por acessar os VDAs e Cloud Connectors através do emparelhamento de VNet. Intervalos de endereços IP de origem podem ser especificados para que o acesso RDP possa ser ainda mais restrito, mesmo dentro da rede interna do cliente. O cliente precisará usar credenciais de domínio para fazer login nessas

© 1997–2026 Citrix Systems, Inc. All rights reserved.

máquinas. Se o cliente estiver trabalhando com o Suporte Citrix para resolver um problema, ele poderá precisar compartilhar essas credenciais com a equipe de suporte. Após a resolução do problema, o cliente é responsável por desabilitar o acesso RDP. Manter o acesso RDP aberto da rede emparelhada ou local do cliente representa um risco de segurança.

Credenciais de domínio

Se o cliente optar por usar um catálogo ingressado no domínio, ele será responsável por fornecer ao Citrix DaaS for Azure uma conta de domínio (nome de usuário e senha) com permissões para ingressar máquinas no 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 uso do Citrix DaaS for Azure, para que seja fácil auditar para que a conta é usada.
- **Escopo:** A conta requer apenas permissões para ingressar máquinas em um domínio. Não deve ser um administrador de domínio completo.
- **Segura:** Uma senha forte deve ser definida para a conta.

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

Mais informações

Para informações relacionadas, consulte:

- Guia de Implantação Segura para a Plataforma Citrix Cloud: Informações de segurança para a plataforma Citrix Cloud.
- Visão geral de segurança técnica: Informações de segurança para o Citrix DaaS
- Notificações de terceiros

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assinar o Citrix DaaS Standard para Azure

Introdução

Você pode assinar o Citrix DaaS Standard para Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard para Azure) e solicitar o Fundo de Consumo do Azure da Citrix, através da Citrix. Você pode avaliar o Citrix DaaS para Azure através da Citrix.

Um pedido abrangente tem duas partes:

- **Citrix DaaS Standard para Azure:** Permite que você use suas próprias assinaturas do Azure (gerenciadas pelo cliente).
- **Fundo de Consumo do Azure da Citrix:** Além disso, permite que você use uma assinatura do Azure gerenciada pela Citrix, além de suas próprias assinaturas do Azure. O uso de uma assinatura do Azure gerenciada pela Citrix oferece os seguintes benefícios:
  - Faturamento único da Citrix, em vez de faturamentos de várias empresas.
  - Diferenças de recursos da assinatura do Azure.
  - Suporte Microsoft de nível Premium através da Citrix.

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

Se você decidir solicitar apenas o Citrix DaaS™ para Azure, você poderá solicitar o Fundo de Consumo do Azure da Citrix posteriormente através do seu representante de conta da Citrix.

Resumo do pedido

Resumo das etapas do pedido:

1. Obter uma conta Citrix Cloud™.

   Se você já tem uma conta Citrix Cloud e atualmente assina o Citrix DaaS, consulte Se você atualmente assina o Citrix DaaS.
2. Peça o Citrix DaaS Standard for Azure e o fundo de consumo através da Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Períodos de avaliação

Você pode usar uma assinatura do Azure Gerenciada pela Citrix durante seu período de avaliação do DaaS Standard for Azure para criar catálogos, imagens e realizar outras tarefas essenciais. Após seu período de avaliação, você pode converter para uma assinatura de serviço paga e solicitar o Fundo de Consumo do Azure Gerenciado pela Citrix. Se você não adquirir o fundo de consumo, excluiremos automaticamente todos os recursos que você criou com a assinatura do Azure Gerenciada pela Citrix. Essa ação pode afetar seus usuários.

Para obter mais informações sobre os períodos de avaliação, consulte períodos de avaliação do serviço Citrix Cloud.

Obtenha uma conta Citrix Cloud

Para se inscrever em uma conta Citrix Cloud e solicitar um período de avaliação, vá para `<https://onboarding.cloud.com>`. Para obter detalhes sobre esse processo, consulte Inscrever-se no Citrix Cloud. Sua conta tem um ID da Organização (OrgID) que sempre aparece no canto superior direito do console do Citrix Cloud.

Próximas etapas: Peça o Citrix DaaS Standard for Azure através da Citrix.

Se você assina atualmente o Citrix DaaS

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

Você pode fazer upgrade do Citrix DaaS Standard for Azure para qualquer uma das seguintes edições:

- Citrix DaaS Edição Avançada
- Citrix DaaS Edição Premium.

Entre em contato com seu representante Citrix para obter detalhes.

Você pode usar uma assinatura do Azure Gerenciada pela Citrix adquirindo o Fundo de Consumo do Azure da Citrix com qualquer uma das seguintes edições de serviço:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix DaaS Premium

Fazer pedido através da Citrix

Você pode fazer o pedido do Citrix DaaS Standard for Azure (incluindo o fundo de consumo) através do Citrix Cloud ou através do seu representante de conta Citrix.

Cancelar uma assinatura mensal através da Citrix

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

(Você não pode usar o painel do Citrix DaaS Standard for Azure para cancelar outros tipos de assinatura que você pediu através da Citrix.)

Para cancelar uma assinatura mensal:

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Soluções > DaaS Standard for Azure**.
3. No painel **Quick Deploy > Microsoft 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. Ela 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 da Citrix ou parceiro Citrix antes do final do mês para reativar o Citrix DaaS Standard for Azure.

IMPORTANTE:

Uma vez que a assinatura mensal do DaaS é cancelada, a Citrix não é mais responsável por gerenciar os recursos na assinatura do Azure de propriedade do cliente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quando seu pedido é aprovado e processado

Após a aprovação de sua avaliação ou serviço, vários blocos aparecem 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:

- Clique no bloco **DaaS Standard for Azure**
- No menu superior esquerdo, selecione **Soluções > DaaS Standard for Azure**.

Para obter orientações de configuração, consulte Introdução.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Primeiros passos

Este artigo resume as tarefas de configuração para entregar desktops e aplicativos usando o Citrix DaaS Standard para Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard para Azure). Recomendamos que você revise cada procedimento antes de realmente executá-lo, para que saiba o que esperar.

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

IMPORTANTE:

Para garantir que você receba informações importantes sobre o Citrix Cloud™ e os serviços Citrix aos quais você assina, certifique-se de que pode receber todas as notificações por e-mail. Por exemplo, a Citrix envia e-mails de notificação informativos mensais detalhando seu consumo (uso) do Azure.

No canto superior direito do console do Citrix Cloud, expanda o menu à direita dos campos de nome do cliente e OrgID. Selecione **Configurações da Conta**. Na guia **Meu Perfil**, selecione todas as entradas na seção **Notificações por E-mail**.

Resumo das tarefas de configuração

As seções a seguir deste artigo o guiam pelas 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
   - Implantação em produção
3. Forneça a URL do workspace aos seus usuários.

Preparação

- Se você não está familiarizado com catálogos, imagens, conexões de rede ou assinaturas do Azure, revise as informações introdutórias de conceitos e terminologia.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Leia a visão geral de segurança para aprender e entender pelo que você (o cliente) e a Citrix são responsáveis.
- Se você ainda não tem uma conta Citrix Cloud que possa ser usada para este serviço, obtenha uma e, em seguida, inscreva-se no serviço.
- Revise os requisitos do sistema.
- Revise as etapas de configuração: prova de conceito ou produção.

Configurar uma implantação rápida de prova de conceito

Este procedimento requer uma assinatura do Azure Gerenciado pela Citrix.

1. Crie um catálogo usando a criação rápida.
2. Adicione seus usuários ao Microsoft Entra ID Gerenciado.
3. Adicione seus usuários ao catálogo.
4. Notifique seus usuários sobre a URL do Workspace.

Configurar uma implantação de produção

1. Se você estiver usando seu próprio Active Directory ou Microsoft Entra ID para autenticar usuários, conecte 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 Azure Gerenciado pela Citrix), importe sua assinatura do Azure.
4. Crie ou importe uma imagem. Embora você possa usar uma das imagens preparadas pela Citrix como está em um catálogo, elas são destinadas principalmente para implantações de prova de conceito.
5. Se você estiver usando uma assinatura do Azure gerenciada pela Citrix e quiser que seus usuários possam acessar itens em sua rede (como servidores de arquivos), configure um emparelhamento de VNet do Azure ou um gateway VPN do Azure.
6. Crie um catálogo usando a criação personalizada.
7. Se você estiver criando um catálogo de máquinas multissessão, adicione aplicativos ao catálogo, se necessário.
8. Se você estiver usando o Microsoft Entra ID gerenciado pela Citrix para autenticar seus usuários, adicione usuários ao diretório.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Adicione usuários ao catálogo.
10. Notifique seus usuários sobre a URL do Workspace.

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

Requisitos do sistema

Para todas as implantações:

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

Se você estiver usando uma assinatura do Azure gerenciada pela Citrix:

- **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 Azure usando conexões de emparelhamento de VNet do Azure, você deve ter uma assinatura do Azure.
- **Ingressando VDAs no Microsoft Entra ID (opcional):** Para ingressar VDAs em 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.

A configuração de conexões com sua rede corporativa local tem requisitos adicionais.

- Qualquer conexão (emparelhamento de VNet do Azure ou gateway VPN do Azure): Requisitos para todas as conexões.
- Conexões de emparelhamento de VNet do Azure: Requisitos e preparação para emparelhamento de VNet.
- Conexões de gateway VPN do Azure: Requisitos e preparação para conexão de gateway VPN do Azure.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informações adicionais:

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

Sistemas operacionais suportados

Ao usar uma assinatura do Azure gerenciada pelo Citrix:

- Windows 11 Pro (sessão única)
- Windows 11 Enterprise Virtual Desktop (multissessão)
- Windows 11 Enterprise Virtual Desktop (multissessão) com Office 365 ProPlus
- Windows 10 Pro (sessão única)
- Windows 10 Enterprise Virtual Desktop (multissessão)
- Windows 10 Enterprise Virtual Desktop (multissessão) com Office 365 ProPlus
- Windows Server 2019 (multi-sessão)
- Windows Server 2022 (multi-sessão)
- Windows Server 2025 (multi-sessão)
- Linux Ubuntu 22.04 LTS (sessão única)
- Linux Ubuntu 22.04 LTS (multi-sessão)

Ao usar uma assinatura do Azure gerenciada pelo cliente, consulte os requisitos do VDA.

URL do Workspace

Depois de criar catálogos e atribuir usuários, notifique-os sobre onde encontrar seus desktops e aplicativos: a URL do Workspace. A URL do Workspace é a mesma para todos os catálogos e usuários.

No painel **Quick Deploy > Microsoft Azure**, visualize a URL expandindo **Acesso e Autenticação do Usuário** à direita.

Você pode alterar a primeira parte da URL do Workspace no Citrix Cloud. Para obter instruções, consulte Personalizar a URL do workspace.

Obter ajuda

Revise o artigo Solução de problemas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Se você ainda tiver problemas com o serviço, abra um tíquete seguindo as instruções em Como Obter Ajuda e Suporte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Criar catálogos

Quando usado para desktops e aplicativos publicados, um catálogo é um grupo de máquinas virtuais idênticas. Ao implantar desktops, as máquinas no catálogo são compartilhadas com usuários selecionados. Ao publicar aplicativos, máquinas multissessão hospedam aplicativos que são compartilhados com usuários selecionados.

NOTA:

Para obter informações sobre como criar catálogos de Acesso Remoto ao PC, consulte Acesso Remoto ao PC.

Tipos de máquina

Um catálogo pode conter um dos seguintes tipos de máquinas:

- **Estático:** O catálogo contém máquinas estáticas de sessão única (também conhecidas como desktops pessoais, dedicados ou persistentes). Estático significa que, quando um usuário inicia um desktop, esse desktop "pertence" a esse usuário. Quaisquer alterações que esse usuário faça no desktop são retidas ao fazer logoff. Mais tarde, quando esse usuário retorna ao Citrix Workspace™ e inicia um desktop, é o mesmo desktop.
- **Aleatório:** O catálogo contém máquinas aleatórias de sessão única (também conhecidas como desktops não persistentes). Aleatório significa que, quando um usuário inicia um desktop, quaisquer alterações que esse usuário faça nesse desktop são descartadas após o logoff. Mais tarde, quando esse usuário retorna ao Citrix Workspace e inicia um desktop, pode ou não ser o mesmo desktop.
- **Multissessão:** O catálogo contém máquinas com aplicativos e desktops. Mais de um usuário pode acessar cada uma dessas máquinas simultaneamente. Os usuários podem iniciar um desktop ou aplicativos de seu workspace. As sessões de aplicativos podem ser compartilhadas. O compartilhamento de sessão não é permitido entre um aplicativo e um desktop.
    - Ao criar um catálogo multissessão, você seleciona a carga de trabalho: leve (como entrada de dados), média (como aplicativos de escritório), pesada (como engenharia) ou

© 1997–2026 Citrix Systems, Inc. All rights reserved.

personalizada. Cada opção representa um número específico de máquinas e sessões por máquina, o que resulta no número total de sessões que o catálogo suporta.

- Se você selecionar a carga de trabalho personalizada, você seleciona entre as combinações disponíveis de CPUs, RAM e armazenamento. Digite o número de máquinas e sessões por máquina, o que resulta no número total de sessões que o catálogo suporta.

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

Maneiras de criar um catálogo

Existem várias maneiras de criar e configurar um catálogo:

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

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 Microsoft Entra gerenciada pela Citrix.	Escolha entre: Microsoft Entra ID gerenciado pela Citrix, ou seu Active Directory/Microsoft Entra ID.
Sem conexão com sua rede local.	Escolha entre: Sem conexão com sua rede local, emparelhamento de VNet do Azure e gateway VPN do Azure.
Usa uma imagem do Windows 10 preparada pela Citrix. Essa imagem contém um VDA de desktop atual.	Escolha entre: imagens preparadas pela Citrix, suas imagens que você importa do Azure, ou imagens que você criou no Citrix DaaS para

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CRIAÇÃO RÁPIDA	CRIAÇÃO PERSONALIZADA
	Azure a partir de uma imagem preparada ou importada pela Citrix.
Cada desktop possui armazenamento em disco padrão do Azure (HDD).	Várias opções de armazenamento estão disponíveis.
Somente desktops estáticos.	Desktops estáticos, aleatórios ou multissessão.
Um agendamento de gerenciamento de energia não pode ser configurado durante a criação. A máquina que hospeda o desktop é desligada quando a sessão termina. (Você pode alterar essa configuração mais tarde.)	Um agendamento de gerenciamento de energia pode ser configurado durante a criação.
Deve usar uma assinatura do Azure gerenciada pela Citrix.	Pode usar o Azure gerenciado pela Citrix ou sua própria assinatura do Azure.

Para obter detalhes, consulte:

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

Criar um catálogo usando a criação rápida

Este método de criação de catálogo sempre usa uma assinatura do Azure gerenciada pela Citrix.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Soluções > DaaS Standard for Azure**.
3. navegar para **Quick Deploy > Microsoft Azure**.
4. Clique em **Criar Catálogo**.

   Botão Criar Catálogo no painel do Azure Quick Deploy(/en-us/citrix-daas-azure/media/dashboard-createcat.png)
5. Clique em **Criação Rápida** na parte superior da página, se ainda não estiver selecionado.

   Campos de catálogo de criação rápida(/en-us/citrix-daas-azure/media/quick-create-1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Desempenho da máquina:** Selecione o tipo de máquina. Cada escolha tem uma combinação única de CPUs, RAM e armazenamento. Máquinas de maior desempenho têm custos mensais mais altos.
- **Região:** Selecione uma região onde você deseja que as máquinas sejam criadas. Você pode selecionar uma região próxima aos seus usuários.
- **Nome:** Digite um nome para o catálogo. Este 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**.

Você é levado automaticamente para o painel **Quick Deploy > Microsoft Azure**. Enquanto o catálogo está sendo criado, o nome do catálogo é adicionado à lista de catálogos, indicando seu progresso durante a criação.

O Citrix DaaS para 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 Microsoft Entra ID para autenticação de usuário, você pode adicionar usuários ao diretório enquanto o catálogo está sendo criado.
- Independentemente do método de autenticação de usuário que você usar, após a criação do catálogo, adicione usuários ao catálogo.

Criar um catálogo usando criação personalizada

Se você estiver usando uma assinatura do Azure gerenciada pela Citrix e planeja usar uma conexão com seus recursos de rede locais, (/pt-br/citrix-daas-azure/network-connections.html) antes de criar o catálogo. Para permitir que seus usuários acessem seus recursos de rede locais ou outros, você também precisa de informações do Active Directory para esse local.

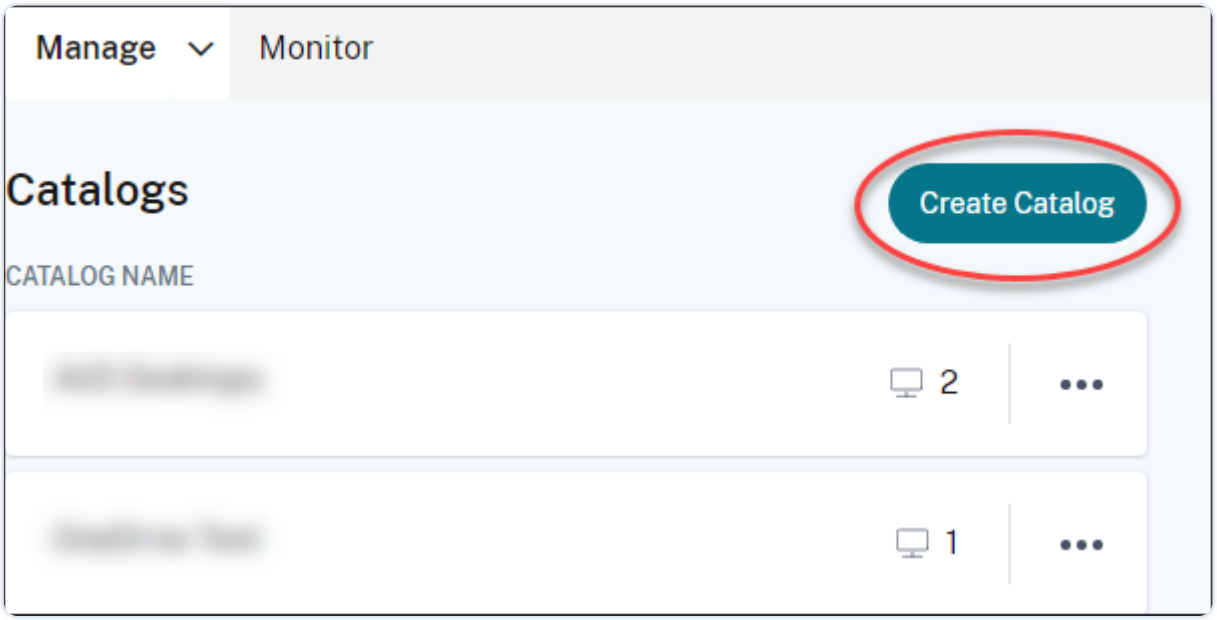
Se você não tiver uma assinatura do Azure gerenciada pela Citrix, deverá (/pt-br/citrix-daas-azure/subscriptions.html#add-customer-managed-azure-subscriptions) no Citrix DaaS para Azure antes de criar um catálogo.

Para criar um catálogo:

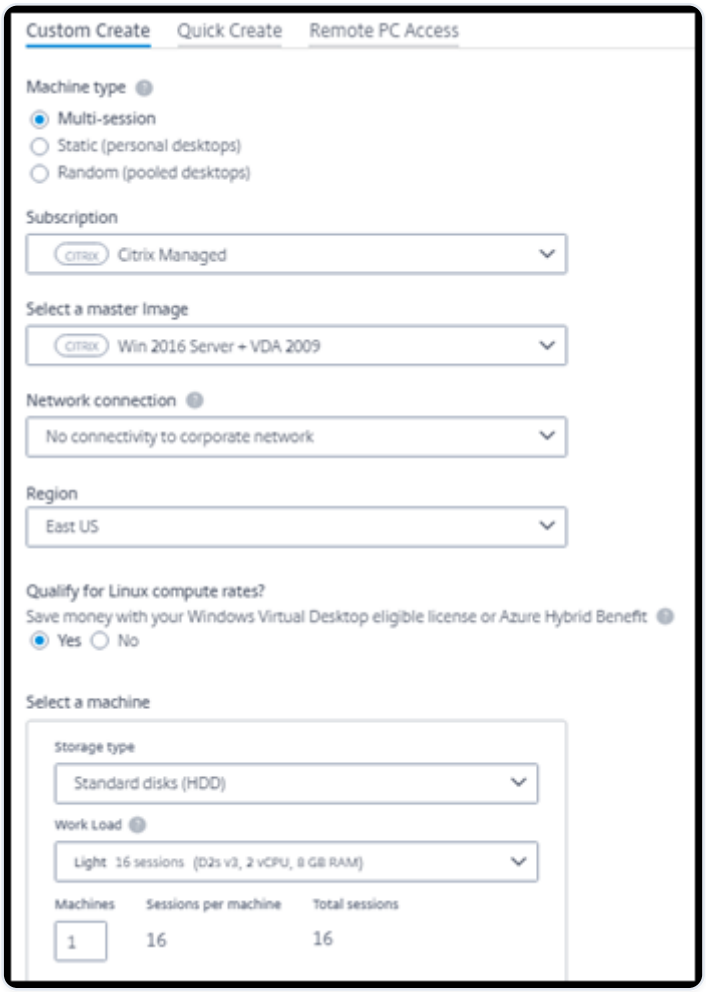
1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Soluções > DaaS Standard for Azure**.
3. navegar para **Quick Deploy > Microsoft Azure**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Clique em **Criar Catálogo**.



5. Selecione **Criação Personalizada** na parte superior da página, se ainda não estiver selecionado.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Preencha os seguintes campos. (Alguns campos são válidos apenas para determinados tipos de máquina. A ordem dos campos pode ser diferente.)

   - **Tipo de máquina**. Selecione um tipo de máquina. Para obter detalhes, consulte (#machine-types).
   - **Assinatura**. Selecione uma assinatura do Azure. Para obter detalhes, consulte (/pt-br/citrix-daas-azure/subscriptions.html).
   - **Imagem mestre:** Selecione uma imagem do sistema operacional. Para obter detalhes, consulte (/pt-br/citrix-daas-azure/master-images.html).
   - **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 Azure gerenciada pelo Citrix, as opções são:
       - **Sem conectividade:** Os usuários não podem acessar locais e recursos em sua rede corporativa local.
       - **Conexões:** Selecione uma conexão, como um emparelhamento de VNet ou uma conexão VPN.
     - 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 selecionou **Sem conectividade** em **Conexão de rede**.) Selecione uma região onde você deseja que os desktops sejam criados. Você pode selecionar uma região que esteja próxima aos seus usuários.

     Se você selecionou um nome de conexão em **Conexão de rede**, o catálogo usa a região dessa rede.
   - **Qualificar-se para taxas de computação Linux?** (Disponível somente se você selecionou uma imagem do Windows.) Você pode economizar dinheiro ao usar sua licença elegível ou o Benefício Híbrido do Azure.

     Benefício do Azure Virtual Desktop: Licenças elegíveis por usuário do Windows 10 ou Windows 11 para:
     - Microsoft 365 E3/E5
     - Microsoft 365 A3/A5/Benefícios de Uso Estudantil
     - Microsoft 365 F3
     - Microsoft 365 Business Premium

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Windows 11 e Windows 10 Enterprise E3/E5
- Windows 11 e Windows 10 Education A3/A5
- Windows 11 e Windows 10 VDA por usuário

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

Benefício Híbrido do Azure: Licenças do Windows Server com Software Assurance ativo ou as licenças de assinatura qualificadas equivalentes. Consulte `<https://azure.microsoft.com/pt-br/pricing/hybrid-benefit/>`.

- **Máquina:**
  - **Tipo de armazenamento**. Disco padrão (HDD), SSD padrão ou SSD premium.
  - **Desempenho da máquina** (para tipo de máquina **Estática** ou **Aleatória**), ou **Carga de trabalho** (para tipo de máquina de várias sessões). As opções incluem apenas aquelas 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 **Desempenho da Máquina**.
  - **Máquinas**. Quantas máquinas você deseja neste catálogo.
- **Esquema de nomenclatura da máquina:** consulte Esquema de nomenclatura da máquina.
- **Nome:** Digite um nome para o catálogo. Este nome aparece no painel **Gerenciar**.
- **Agendamento de energia:** Por padrão, a caixa de seleção **Configurarei isso mais tarde** está marcada. Para obter detalhes, consulte Agendamentos de gerenciamento de energia.

7. Quando terminar, clique em **Criar Catálogo**.

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

O que fazer a seguir:

- Se você ainda não o fez, configure o método de autenticação para que seus usuários autenticar no Citrix Workspace.
- Depois que o catálogo for criado, adicione usuários ao catálogo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Se você criou um catálogo de várias sessões, adicione aplicativos (antes ou depois de adicionar usuários).

Criação de catálogos de máquinas unidas ao Microsoft Entra

Você pode usar a criação personalizada para criar catálogos de máquinas unidas ao seu Microsoft Entra ID. Isso é suportado apenas em sua própria assinatura do Azure.

Requisitos

Sua implantação deve incluir Citrix Cloud Connectors. O Machine Creation Services™ implanta seus Cloud Connectors com base nas informações que você fornece sobre seu domínio Microsoft Entra ao criar um catálogo.

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

Não una a imagem mestre ao Microsoft Entra ID antes de criar um catálogo. O Citrix MCS une a imagem mestre ao Microsoft Entra ID quando o catálogo é criado.

Use a versão 2203 ou superior do VDA.

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 ao usuário atribuído à máquina.
- Método alternativo: Atribua a função aos grupos de recursos que contêm as máquinas virtuais, a todos os usuários com acesso ao catálogo.
- Menos seguro: Atribua a função às assinaturas, a todos os usuários com acesso ao catálogo.

Defina a autenticação do Workspace para usar o Microsoft Entra ID ao qual você está unindo as máquinas no catálogo. Para obter instruções, consulte Configurar autenticação de usuário no Citrix Cloud.

Para obter mais informações sobre requisitos, problemas conhecidos e considerações, consulte as informações sobre configurações de VDA puras unidas ao Microsoft Entra em Configuração de VDA unida ao Microsoft Entra e não unida ao domínio.

Para criar um catálogo

1. Faça login em Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. No menu superior esquerdo, selecione **Soluções > DaaS Standard for Azure**.
3. Selecione **Quick Deploy > Microsoft Azure**.
4. Selecione **Criar Catálogo**.
5. Selecione **Criação Personalizada** na parte superior da página, se ainda não estiver selecionado.
6. Preencha os seguintes campos.

    - **Tipo de máquina.** Selecione **Estático (desktops pessoais)** ou **Aleatório (desktops agrupados)**.
    - **Assinatura**. Selecione sua assinatura do Azure.
    - **Imagem mestre.** Selecione uma imagem de 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 de domínio**. Selecione **Microsoft Entra ID** como seu tipo de domínio. Um aviso pode aparecer lembrando você de configurar a autenticação do Workspace para usar este Microsoft Entra ID.

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 configurar opcionalmente várias configurações de localização de recursos.

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

- 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 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 a configurar um.

Configurar configurações avançadas:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- (Obrigatório apenas quando o local de recurso já está configurado.) Um nome para o local de recurso.
- Tipo de conectividade externa: através do serviço Citrix Gateway, ou de dentro da sua rede corporativa.
- Configurações do Cloud Connector:
  - (Disponível apenas ao usar uma assinatura do Azure gerenciada pelo cliente) Desempenho da máquina. Esta seleção é usada para os Cloud Connectors no local de recurso.
  - (Disponível apenas ao usar uma assinatura do Azure gerenciada pelo cliente) Grupo de recursos do Azure. Esta seleção é usada para os Cloud Connectors no local de recurso. O padrão é o grupo de recursos usado pela última vez pelo local de recurso (se aplicável).
  - Unidade Organizacional (OU). O padrão é a OU usada pela última vez pelo local de recurso (se aplicável).

Quando terminar as configurações avançadas, clique em **Salvar** para retornar à caixa de diálogo de criação de catálogo do Quick Deploy.

Depois de criar um catálogo, várias ações de localização de recursos ficam disponíveis. Para obter detalhes, consulte Ações de localização de recursos.

Esquema de nomenclatura de máquina

Para especificar um esquema de nomenclatura de máquina ao criar um catálogo usando o Quick Deploy, selecione **Especificar esquema de nomenclatura de máquina**. Use de 1 a 4 curingas (sinais 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 completo, incluindo curingas, deve ter entre 2 e 15 caracteres.
- Um nome não pode incluir espaços em branco, barras, barras invertidas, dois pontos, asteriscos, colchetes angulares, pipes, vírgulas, til, pontos de exclamação, arrobas, cifrões, sinais de porcentagem, acentos circunflexos, parênteses, chaves ou sublinhados.
- Um nome não pode começar com um ponto.
- Um nome não pode conter apenas 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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 crescimento.

- Por exemplo, um esquema de nomenclatura com 2 curingas e 13 outros caracteres (por exemplo, `MachineSales-##`) usa o número máximo de caracteres (15).
- Quando o catálogo contém 99 máquinas, a próxima criação de máquina falha. O serviço tenta criar uma máquina com três dígitos (100), mas isso criaria um nome com 16 caracteres. O máximo é 15.
- Assim, 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 para Azure usará o esquema de nomenclatura padrão `DAS%%%%%-**-###`.

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

Informações relacionadas

- Máquinas ingressadas no domínio e não ingressadas no domínio.
- Catálogos de Acesso Remoto a PC.
- Criar um catálogo em uma rede que usa um servidor proxy.
- Exibir informações do catálogo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Acesso Remoto a PC

Introdução

NOTA:

Este artigo descreve como configurar o Acesso Remoto a PC ao usar a interface de gerenciamento Quick Deploy no Citrix DaaS Standard para Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard para Azure). Para obter informações sobre como configurar o Acesso Remoto a PC ao usar a interface de gerenciamento de Configuração Completa, consulte Acesso Remoto a PC.

O Citrix Acesso Remoto a PC permite que os usuários utilizem remotamente máquinas físicas Windows ou Linux localizadas no escritório. Os usuários recebem a melhor experiência de usuário ao usar o Citrix HDX™ para entregar sua sessão de PC do escritório.

O Acesso Remoto a PC suporta máquinas ingressadas no domínio.

Diferenças em relação à entrega de desktops e aplicativos virtuais

Se você está familiarizado com a entrega de desktops e aplicativos virtuais, o recurso Acesso Remoto a PC apresenta várias diferenças:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resumo da instalação e configuração

Revise esta seção antes de iniciar as tarefas.

1. Antes de começar:
    a. Revise 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 para Azure.
    b. Configure um local de recurso que possa acessar seus recursos do Active Directory. Instale pelo menos dois Cloud Connectors no local de recurso. Os Cloud Connectors se comunicam com o Citrix Cloud.

        Siga as orientações para criar um local de recurso e instalar Cloud Connectors nele. Esta informação inclui requisitos de 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 através dos Cloud Connectors no local de recurso.
4. Na interface de gerenciamento do Citrix DaaS™ para Azure Quick Deploy:
    a. Crie um catálogo de Acesso Remoto a PC. Neste procedimento, você especifica a localização do seu local de recurso 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 autoatribuído ou agrupado aleatório. Você não precisa adicionar usuários a um catálogo estático pré-atribuído.
5. Envie a URL do workspace aos usuários. Do seu workspace, 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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- As máquinas devem estar executando um sistema operacional Windows 10 de sessão única ou Linux (Red Hat Enterprise Linux e Ubuntu).
- A máquina deve estar ingressada em um domínio do Active Directory Domain Services.
- Se você está familiarizado com o uso do Acesso Remoto a PC com 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 preferível para maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi:
  - Defina as configurações de energia para manter 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 registrará até que o usuário faça logon. A máquina não estará disponível para acesso remoto até que um usuário faça logon.
  - Certifique-se de que os Cloud Connectors possam ser acessados a partir da rede Wi-Fi.

Dispositivos e periféricos:

- Os seguintes dispositivos não são suportados:
  - Comutadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo laptops e PCs All-in-One e NVIDIA Optimus.
  - Máquinas com dual boot.
- Conecte o teclado e o mouse diretamente à máquina. Conectar a um monitor ou outros componentes que podem ser desligados ou desconectados pode tornar esses periféricos indisponíveis. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desligue esses componentes.
- Para dispositivos laptop e Surface Pro: Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionar com a bateria. Configure as opções de energia do laptop para corresponder às opções de uma máquina desktop. Por exemplo:
  - Desativar o recurso de hibernação.
  - Desativar o recurso de suspensão.
  - Defina a ação de fechar a tampa como **Não fazer nada**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Defina a ação de *pressionar o botão liga/desliga* como **Desligar**.
- Desative os recursos de economia de energia da placa de vídeo e da NIC.

Ao usar uma estação de acoplamento, você pode desacoplar e reacoplar laptops. Quando você desacopla o laptop, o VDA se registra novamente com os Cloud Connectors via Wi-Fi. No entanto, quando você reacopla o laptop, o VDA não muda para usar a conexão com fio até que você desconecte o adaptador sem fio. Alguns dispositivos fornecem funcionalidade integrada para desconectar o adaptador sem fio ao estabelecer uma conexão com fio. Outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador sem fio. Revise as considerações de Wi-Fi mencionadas anteriormente.

Para habilitar o acoplamento e desacoplamento para dispositivos de Acesso Remoto a PC:

- 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 **Permitir que o computador desligue este dispositivo para economizar energia**. Certifique-se de que **Permitir que este dispositivo reative o computador** esteja selecionado.

VDA Linux:

- Use o VDA Linux em máquinas físicas apenas no modo não 3D. Devido a limitações no driver da NVIDIA, a tela local do PC não pode ser desativada e exibe as atividades da sessão quando o modo HDX 3D está habilitado. Mostrar esta tela é um risco de segurança.
- Os 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 autoatribuída ou de pool aleatório.

Considerações do Workspace:

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

Preparar

- Decida como instalar o VDA nas máquinas. Vários métodos estão disponíveis:
  - Instale o VDA manualmente em cada máquina.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Envie a instalação do VDA usando a Política de Grupo, (/pt-br/citrix-virtual-apps-desktops/install-configure/vda-install-scripts.html).
    - 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 (/pt-br/citrix-virtual-apps-desktops/install-configure/install-vdas/third-party-vda-deployment-methods/install-vdas-sccm.html).

- Saiba mais sobre (#user-assignment-methods) e decida qual método você usará. Você especifica o método ao criar um catálogo de Acesso Remoto a PC.
- Decida como as máquinas (na verdade, os VDAs que você instala nas máquinas) se registrarão no Citrix Cloud. Um VDA deve se registrar para estabelecer comunicações com o session broker no Citrix Cloud.

  Os VDAs se registram por meio dos Cloud Connectors em seu local de recurso. Você pode especificar os endereços do Cloud Connector ao instalar um VDA, ou posteriormente.

  Para o primeiro registro (inicial) de um VDA, a Citrix recomenda usar GPO ou LGPO baseado em política. Após o registro inicial, a Citrix recomenda usar a atualização automática, que é habilitada por padrão. (/pt-br/citrix-virtual-apps-desktops/manage-deployment/vda-registration.html).

Instalar um VDA

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

Baixar um VDA

- Para baixar um VDA do Windows:

  a. Usando suas credenciais de conta do Citrix Cloud, navegue até a página de download do Citrix DaaS.

  b. Baixe o VDA mais recente. (#windows-vda-installation-package-types). Os valores de ano e mês no título do VDA variam.

- Para baixar um VDA Linux para Acesso Remoto a PC, siga as orientações na (/pt-br/linux-virtual-delivery-agent/current-release.html).

Tipos de pacote de instalação do VDA do Windows

O site de download da Citrix oferece dois tipos de pacote de instalação do VDA do Windows que podem ser usados para máquinas de Acesso Remoto a PC:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Instalador VDA principal de sessão única (*release* é *aamm*):
  `VDAWorkstationCoreSetup_release.exe`

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

  No entanto, sem o Citrix Profile Management instalado, as exibições do Citrix Analytics for Performance e alguns detalhes do Monitor não estão disponíveis. Para obter detalhes sobre essas limitações, consulte a postagem do blog Monitorar e solucionar problemas de máquinas de Acesso Remoto a PC.

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

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

  Embora o instalador VDA completo de sessão única seja um pacote maior do que o instalador VDA principal de sessão única, você pode adaptá-lo para instalar apenas os componentes de que precisa. Por exemplo, você pode instalar os componentes que suportam o Profile Management.

Instalar um VDA do Windows para Acesso Remoto a PC interativamente

1. Clique duas vezes no arquivo de instalação do VDA que você baixou.
2. Na página **Ambiente**, selecione **Habilitar Acesso Remoto a PC** e clique em **Avançar**.
3. Na página **Delivery Controller™**, selecione uma das seguintes opções:

   - Se você souber os endereços dos seus Cloud Connectors, selecione **Fazer manualmente**. Insira o FQDN de um Cloud Connector e clique em **Adicionar**. Repita para os outros Cloud Connectors em seu local de recurso.
   - Se você souber onde instalou os Cloud Connectors em sua estrutura AD, selecione **Escolher locais do Active Directory** e, em seguida, navegar até esse local. Repita para os outros Cloud Connectors.
   - Se você quiser especificar os endereços do Cloud Connector na Política de Grupo da Citrix, selecione **Fazer mais tarde (Avançado)** e, em seguida, confirme essa seleção quando solicitado.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Quando terminar, clique em **Avançar**.

4. Se você estiver usando o instalador VDA completo de sessão única, na página **Componentes Adicionais**, selecione os componentes que deseja instalar, como o Profile Management. (Esta página não aparece se você estiver usando o instalador VDA principal de sessão única.)
5. Na página **Recursos**, clique em **Avançar**.
6. Na página **Firewall**, selecione **Automaticamente** (se ainda não estiver selecionado). Em seguida, clique em **Avançar**.
7. Na página **Resumo**, clique em **Instalar**.
8. Na página **Diagnosticar**, clique em **Conectar**. Certifique-se de que a caixa de seleção esteja marcada. Quando solicitado, insira suas credenciais de conta Citrix. Depois que suas credenciais forem validadas, clique em **Avançar**.
9. Na página **Concluir**, clique em **Concluir**.

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

Instalar um VDA do Windows para Acesso Remoto a PC usando uma linha de comando

- Se você estiver usando o instalador VDA principal 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 principal de sessão única. O aplicativo Citrix Workspace e outros serviços não essenciais não são instalados. Os FQDNs de dois Cloud Connectors são especificados, e as portas no Serviço de Firewall do Windows serão abertas automaticamente. O administrador manipular os reinícios.

  ```
  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 as opções `/remotepc` e `/includeadditional`. A opção `/remotepc` impede a instalação da maioria dos componentes opcionais. A opção `/includeadditional` 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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 VDA Linux

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

Criar um catálogo de Acesso Remoto para PC

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

IMPORTANTE:

Uma máquina pode pertencer a apenas 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 **Soluções > DaaS Standard for Azure**.
3. Clique em **Criar Catálogo** no painel **Implantação Rápida > Microsoft Azure**.
4. Na guia **Acesso Remoto para PC**, selecione um método para atribuir usuários a máquinas.
5. Insira um nome para o catálogo e selecione o local de recurso que você criou.
6. Adicionar máquinas.
7. Clique em **Criar Catálogo**.
8. Na página **Seu catálogo de Acesso Remoto para PC está sendo criado**, clique em **Concluído**.
9. Uma entrada para o novo catálogo aparece no painel **Gerenciar**.

   Após o catálogo ser criado com sucesso, 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 de pool aleatório não atribuído.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Métodos de atribuição de usuário

O método de atribuição de usuário que você escolhe ao criar um catálogo indica como os usuários são atribuídos às máquinas.

- **Estático autoatribuído:** A atribuição de usuário ocorre quando um usuário faz logon na máquina (não usando Citrix, por exemplo, presencialmente ou RDP), após a instalação de um VDA na máquina. Posteriormente, se outros usuários fizerem logon nessa máquina (não usando Citrix), eles também serão atribuídos. Apenas um usuário pode usar a máquina por vez. Esta é uma configuração típica para trabalhadores de escritório ou trabalhadores por turnos que compartilham um computador.

  Este método é compatível com máquinas Windows. Não pode ser usado com máquinas Linux.
- **Estático pré-atribuído:** Os usuários são pré-atribuídos às máquinas. (Isso geralmente é configurado fazendo upload de um arquivo CSV contendo o mapeamento máquina-usuário.) 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 após sua criação. Isso é melhor para trabalhadores de escritório.

  Este método é compatível com máquinas Windows e Linux.
- **Pool aleatório não atribuído:** Os usuários são atribuídos aleatoriamente a uma máquina disponível. Apenas um usuário pode usar a máquina por vez. Isso é ideal para laboratórios de informática em escolas.

  Este método é compatível com máquinas Windows. Não pode ser usado com máquinas Linux.

Métodos para adicionar máquinas a um catálogo

Lembre-se: Cada máquina deve ter um VDA instalado.

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

- Selecionar contas de máquina uma a uma.
- Selecionar UOs.
- Adicionar em massa usando um arquivo CSV. Um modelo está disponível para você usar para o arquivo CSV.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Adicionar nomes de máquinas

Este método adiciona contas de máquina uma a uma.

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

Adicionar UOs

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

Por exemplo, no caso de `Bank/Officers/Tellers`, selecione `Tellers` para maior granularidade. Caso contrário, você pode selecionar `Officers` ou `Bank`, com base no requisito.

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

Para adicionar UOs:

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

Adicionar em massa

1. Clique em **Baixar Modelo CSV**.
2. No modelo, adicione as informações da conta da máquina (até 100 entradas). O arquivo CSV também pode conter os nomes dos usuários atribuídos a cada máquina.
3. Salve o arquivo.
4. Arraste o arquivo para a página **Adicionar máquinas em massa** ou navegue até o arquivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Uma prévia do conteúdo do arquivo é exibida. Se não for o arquivo desejado, você pode criar outro arquivo e arrastá-lo ou navegar até ele.
6. Quando terminar, clique em **Concluído**.

Gerenciar catálogos do Remote PC Access

Para exibir ou alterar as informações de configuração de um catálogo do Remote PC Access, selecione o catálogo no painel **Quick Deploy > Microsoft Azure** (clique em qualquer lugar em sua entrada).

- Na guia **Detalhes**, você pode adicionar ou remover máquinas.
- Na guia **Assinantes**, você pode adicionar ou remover usuários.
- Na guia **Máquinas**, você pode:
  - Adicionar ou remover máquinas: botão **Adicionar ou remover máquinas**.
  - Alterar atribuições de usuário: ícone de lixeira **Remover atribuição**, **Editar atribuição de máquina** no menu de reticências.
  - Ver quais máquinas estão registradas e colocar máquinas em ou fora do modo de manutenção.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assinaturas do Azure

Introdução

O Citrix DaaS Standard para Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard para Azure) suporta tanto as assinaturas do Azure gerenciadas pela Citrix quanto suas próprias assinaturas do Azure gerenciadas pelo cliente.

- Para usar suas próprias assinaturas do Azure, você primeiro importa (adiciona) uma ou mais dessas assinaturas ao Citrix DaaS™ para Azure. Essa ação permite que o Citrix DaaS para Azure acesse suas assinaturas do Azure.
- Usar uma assinatura do Azure gerenciada pela Citrix não requer configuração de assinatura. No entanto, para ter uma assinatura do Azure gerenciada pela Citrix disponível, você deve ter solicitado o Fundo de Consumo do Azure da Citrix (além do Citrix DaaS Standard para Azure).

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

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

ASSINATURA DO AZURE GERENCIADA PELA CITRIX	SUA PRÓPRIA ASSINATURA DO AZURE
Suporta catálogos de criação rápida e criação personalizada.	Suporta apenas catálogos de criação personalizada.
Sempre disponível (e é a seleção de assinatura padrão) ao criar catálogos e imagens.	É necessário adicionar a assinatura do Azure ao Citrix DaaS para Azure antes de criar um catálogo.
Para autenticação de usuário, suporta o Microsoft Entra ID gerenciado pela Citrix ou seu próprio Active Directory.	Pode conectar seu próprio Active Directory e Microsoft Entra ID.
As opções de conexão de rede incluem **Sem conectividade**.	As opções de conexão de rede incluem apenas suas próprias redes virtuais.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ASSINATURA DO AZURE GERENCIADA PELA CITRIX	SUA PRÓPRIA ASSINATURA DO AZURE
Ao usar o emparelhamento de VNet do Azure para se conectar aos seus recursos, você deve criar uma conexão de emparelhamento de 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 na 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.

Visualizar assinaturas

Para visualizar os detalhes da assinatura, no painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Cloud Subscriptions** 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 onde 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 para 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 um Administrador Global do diretório e tiver privilégios de proprietário para a assinatura:** Basta autenticar em 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 para Azure, crie um aplicativo Azure no seu Microsoft Entra ID e, em seguida, adicione esse aplicativo como um colaborador da assinatura. Ao adicionar essa assinatura ao Citrix DaaS para Azure, você fornece as informações relevantes do aplicativo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Esta tarefa requer privilégios de Administrador Global para o diretório e privilégios de proprietário para a assinatura.

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Cloud Subscriptions** 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 ao Citrix DaaS para Azure acessar suas assinaturas do Azure em seu nome.
5. Clique em **autenticar Azure Account**. Você será levado para a página de login do Azure.
6. Insira suas credenciais do Azure.
7. Você é retornado 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 que você deseja adicionar as assinaturas selecionadas.

As assinaturas do Azure que você selecionou são listadas ao expandir **Assinaturas**. As assinaturas adicionadas estão disponíveis para seleção ao criar um catálogo ou imagem.

Adicionar 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 para Azure, crie um aplicativo no Microsoft Entra ID e, em seguida, adicione esse aplicativo como um colaborador da assinatura.
- Adicione a assinatura ao Citrix DaaS para Azure(#add-your-subscription-to-citrix-daas-for-azure), usando informações sobre o aplicativo que você criou no Azure.

Crie um aplicativo no Microsoft Entra ID e adicione-o como colaborador

1. Registre um novo aplicativo no Microsoft Entra ID:
   a. Em um navegador, navegar para `<https://portal.azure.com>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. No menu superior esquerdo, selecione **Microsoft Entra ID**.

c. Na lista **Gerenciar**, clique em **Registros de aplicativo**.

d. Clique em **+ Novo registro**.

e. Na página **Registrar um aplicativo**, forneça as seguintes informações:

- **Nome:** Insira o nome da conexão
- **Tipo de aplicativo:** Selecione **Aplicativo Web / API**
- **URI de redirecionamento:** deixe em branco

f. Clique em **Criar**.

2. Crie a chave secreta de acesso do aplicativo e adicione a atribuição de função:

a. No procedimento anterior, selecione **Registro de Aplicativo** para visualizar os detalhes.

b. Anote o **ID do Aplicativo** e o **ID do Diretório**. Você os usará mais tarde ao adicionar sua assinatura ao Citrix DaaS para Azure.

c. Em **Gerenciar**, selecione **Certificados e segredos**.

d. Na página **Segredos do cliente**, selecione **+ Novo segredo do cliente**.

e. Na página **Adicionar um segredo do cliente**, forneça uma descrição e selecione um intervalo de expiração. Em seguida, clique em **Adicionar**.

f. Anote o valor do segredo do cliente. Você o usará 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 para Azure e, em seguida, 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:

- **Função:** Colaborador
- **Atribuir acesso a:** Usuário, grupo ou entidade de serviço do Microsoft Entra
- **Selecionar:** O nome do aplicativo Azure que você criou anteriormente.

j. Clique em **Salvar**.

Adicionar sua assinatura ao Citrix DaaS para Azure

Você precisará do ID do aplicativo, ID do diretório e valor do segredo do cliente do aplicativo que você criou no Microsoft Entra ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. No painel **Implantação Rápida > Microsoft 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 **Tenho um aplicativo Azure com função de colaborador para a assinatura**.
5. Insira o ID do locatário (ID do diretório), ID do cliente (ID do aplicativo) e 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 Azure no menu de reticências.

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

Adicionar assinaturas do Azure gerenciadas pela Citrix

Uma assinatura do Azure gerenciada pela Citrix suporta o número de máquinas indicado em Limites. (Neste contexto, *máquinas* refere-se a VMs que têm um Citrix VDA instalado. Essas máquinas entregam aplicativos e desktops aos usuários. Não inclui outras máquinas em um local de recurso, como Cloud Connectors.)

Se sua assinatura do Azure gerenciada pela Citrix provavelmente atingirá seu limite em breve, e você tiver licenças Citrix suficientes, você pode solicitar outra assinatura do Azure gerenciada pela Citrix. 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 Azure gerenciada pela Citrix exceder o valor indicado em Limites.

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

- Digamos que você tenha dois catálogos (`Cat1` e `Cat2`) que usam a mesma assinatura do Azure gerenciada pela Citrix. `Cat1` atualmente contém 500 máquinas, e `Cat2` tem 250.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ao planejar as necessidades futuras de capacidade, você adiciona 200 máquinas a `Cat2`. A assinatura do Azure gerenciada pela Citrix agora suporta 950 máquinas (500 em `Cat 1` e 450 em `Cat 2`). O painel indica que a assinatura está perto do seu limite.
- Quando você precisa de mais 75 máquinas, você não pode usar essa assinatura para criar um catálogo com 75 máquinas (ou adicionar 75 máquinas a um catálogo existente). Isso excederia o limite da assinatura. Em vez disso, você solicita outra assinatura do Azure gerenciada pela Citrix. Então, você pode criar um catálogo usando essa assinatura.

Quando você tem mais de uma assinatura do Azure gerenciada pela Citrix:

- Nada é compartilhado entre essas assinaturas.
- Cada assinatura tem um nome exclusivo.
- Você pode escolher entre as assinaturas do Azure gerenciadas pela Citrix (e quaisquer assinaturas do Azure gerenciadas pelo cliente que você adicionou) ao:
  - Criar um catálogo.
  - Criar ou importar uma imagem.
  - Criar um emparelhamento de VNet ou uma conexão de gateway VPN do Azure.

Requisito:

- Você deve ter licenças Citrix suficientes para justificar a adição de outra assinatura do Azure gerenciada pela Citrix. Usando o exemplo hipotético anterior, se você tiver 2.000 licenças Citrix na expectativa de implantar pelo menos 1.500 máquinas por meio de assinaturas gerenciadas pela Citrix, poderá adicionar outra assinatura do Azure gerenciada pela Citrix.

Para adicionar uma assinatura do Azure gerenciada pela Citrix:

1. Entre em contato com seu representante Citrix para solicitar outra assinatura do Azure gerenciada pela Citrix. Você será notificado quando puder prosseguir.
2. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Cloud Subscriptions** à direita.
3. Clique em **Adicionar assinatura do Azure**.
4. Na página **Adicionar Assinaturas**, clique em **Adicionar uma assinatura do Azure gerenciada pela Citrix**.
5. Na página **Adicionar uma Assinatura Gerenciada pela Citrix**, clique em **Adicionar Assinatura** na parte inferior da página.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Remover assinaturas do Azure

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

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

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS for Azure, expanda **Cloud Subscriptions** à direita.
2. Clique na entrada da assinatura.
3. Na guia **Detalhes**, clique em **Remover Assinatura**.
4. Clique em **autenticar Azure Account**. Você será levado para a página de login do Azure.
5. Insira suas credenciais do Azure.
6. Você será retornado automaticamente ao Citrix DaaS for Azure. Confirme a exclusão nas caixas de seleção e clique em **Sim, Excluir Assinatura**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Conexões de rede

Introdução

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

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

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

- Sem conectividade
- Emparelhamento de VNet do Azure
- Gateway VPN do Azure

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

Você não pode alterar o tipo de conexão de um catálogo depois que ele é criado.

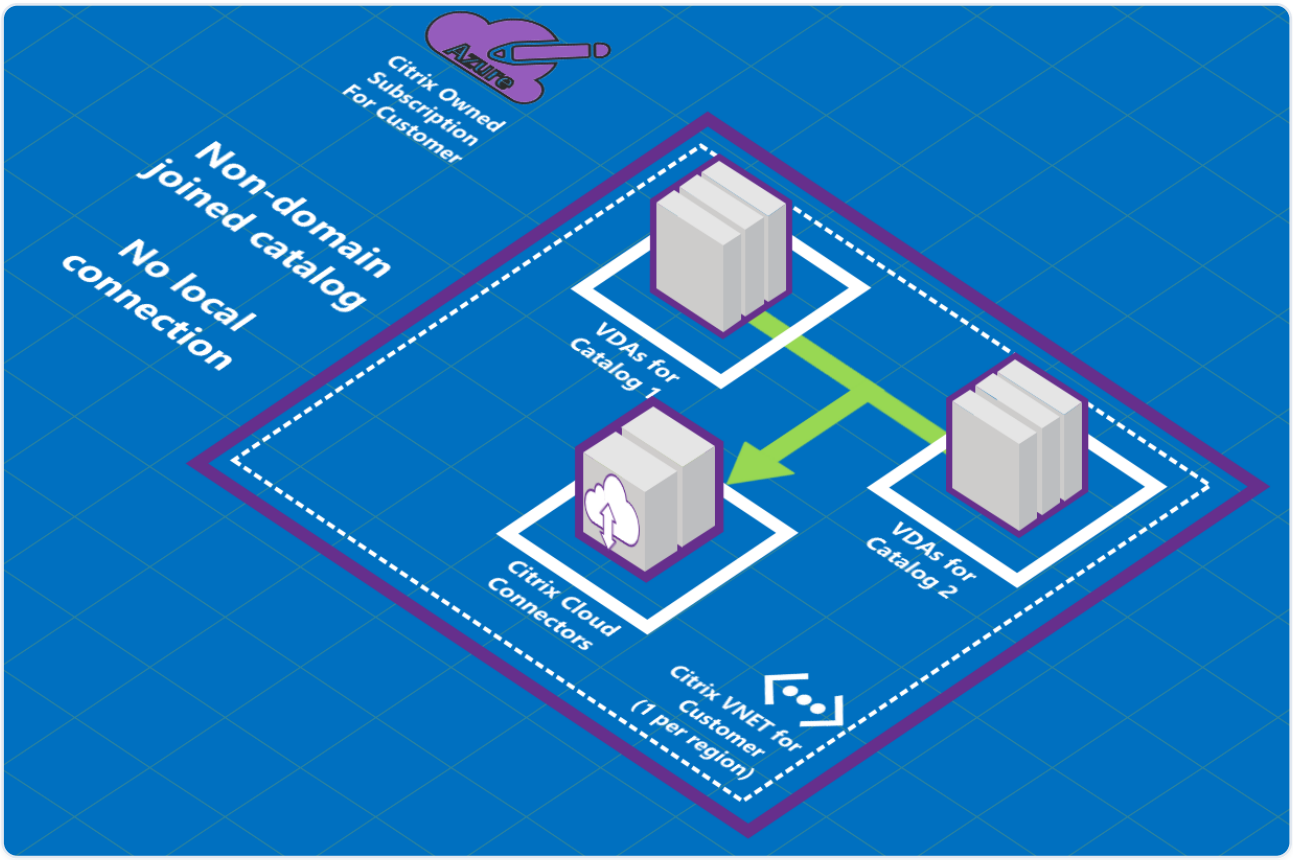
Requisitos para todas as conexões de rede

- Ao criar uma conexão, você deve ter entradas de servidor DNS válidas.
- Ao usar DNS Seguro ou um provedor de DNS de terceiros, você deve adicionar o intervalo de endereços alocado para uso pelo Citrix DaaS™ para 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 alcançar seu servidor Network Time Protocol (NTP) para garantir a sincronização de tempo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sem conectividade

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

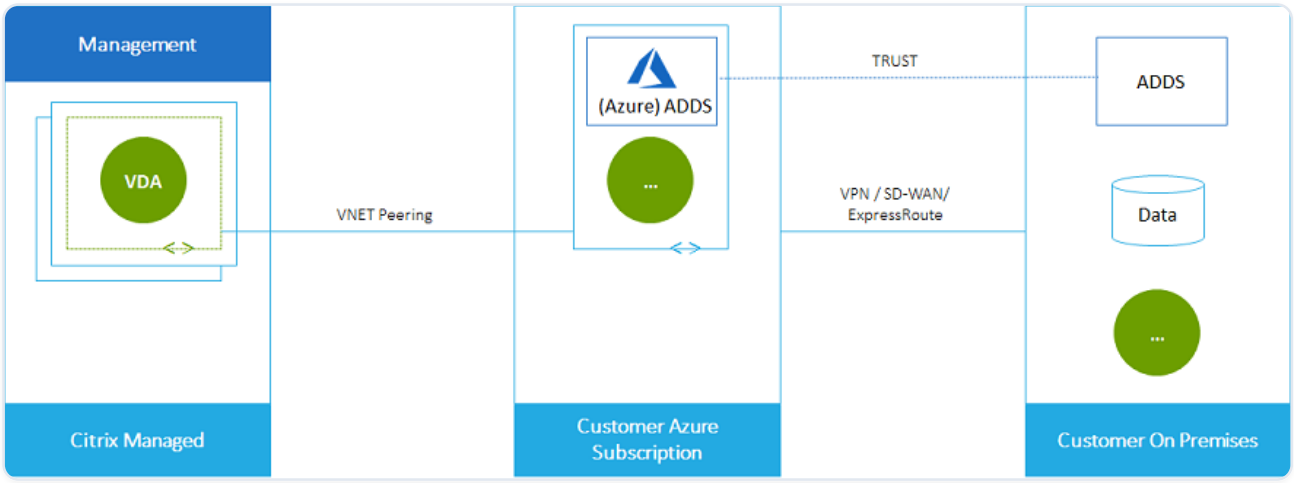


Sobre as conexões de emparelhamento de VNet do Azure

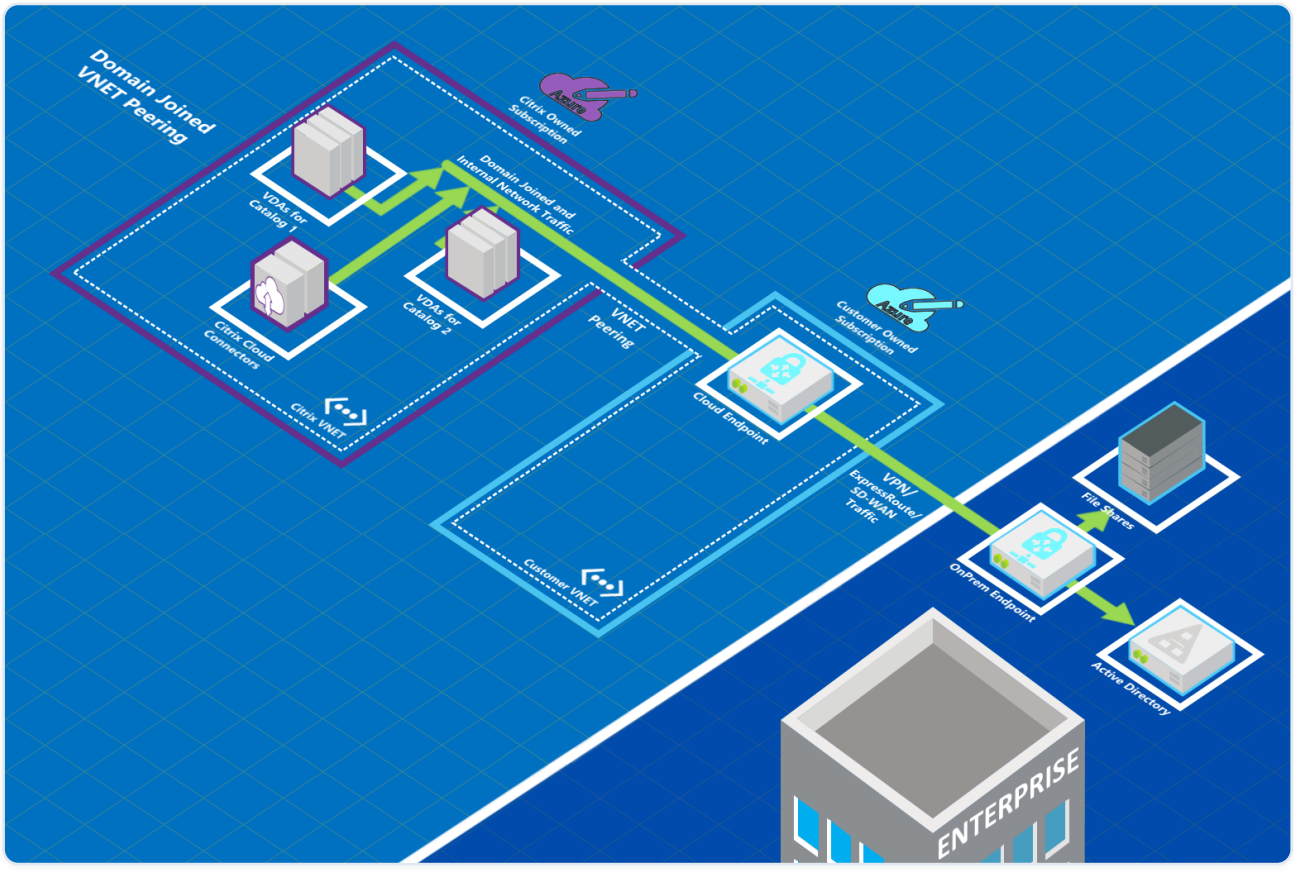
O emparelhamento de rede virtual conecta perfeitamente duas redes virtuais do Azure (VNets): a sua e a VNet do Citrix DaaS para Azure. O emparelhamento também ajuda a permitir que os usuários acessem arquivos e outros itens de suas redes locais.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Aqui está outra ilustração do emparelhamento de VNet.



Os usuários podem acessar seus recursos de rede locais (como servidores de arquivos) ingressando no domínio local ao criar um catálogo. (Ou seja, você ingressa no domínio 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 Azure ExpressRoute). Ao criar o catálogo, você fornece o domínio, a OU e as credenciais da conta.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANTE:

- Saiba mais sobre o emparelhamento de VNet antes de usá-lo no Citrix DaaS para Azure.
- Crie uma conexão de emparelhamento de VNet antes de criar um catálogo que a utilize.

Rotas personalizadas de emparelhamento de VNet do Azure

Rotas personalizadas, ou definidas pelo usuário, substituem as rotas de sistema padrão do Azure para direcionar o tráfego entre máquinas virtuais em um emparelhamento de 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 que não estão diretamente conectadas por meio do emparelhamento de VNet. Por exemplo, você pode criar uma rota personalizada que força o tráfego através 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 VPN do Azure existente ou um dispositivo de rede em seu ambiente Citrix DaaS para Azure.
- Ao adicionar rotas personalizadas, você deve atualizar as tabelas de rotas da sua empresa com as informações da VNet de destino do Citrix DaaS para Azure para garantir a conectividade de ponta a ponta.
- As rotas personalizadas são exibidas no Citrix DaaS para Azure na ordem em que são inseridas. Essa ordem de exibição não afeta a ordem em que o Azure seleciona as rotas.

Antes de usar rotas personalizadas, revise 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 emparelhamento de VNet do Azure ou a conexões existentes em seu ambiente Citrix DaaS para Azure. Quando estiver pronto para usar rotas personalizadas com seu emparelhamento de VNet, consulte as seguintes seções neste artigo:

- Para rotas personalizadas com novos emparelhamentos de VNet do Azure: Criar uma conexão de emparelhamento de VNet do Azure
- Para rotas personalizadas com emparelhamentos de VNet do Azure existentes: Gerenciar rotas personalizadas para conexões de emparelhamento de VNet do Azure existentes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requisitos e preparação para emparelhamento de VNet do Azure

- Credenciais para um proprietário de assinatura do Azure Resource Manager. Esta deve ser uma conta do Microsoft Entra. O Citrix DaaS para Azure não oferece suporte a outros tipos de conta, como live.com ou contas externas (convidado) do Microsoft Entra (em um locatário diferente).
- Uma assinatura do Azure, grupo de recursos e rede virtual (VNet).
- Configure as rotas de rede do Azure para que os VDAs na assinatura do Azure gerenciada pela Citrix 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:** Para cenários ingressados no domínio, 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 de VNet do Azure.

  Por exemplo, a configuração pode incluir o Microsoft Entra Domain Services, uma VM de controlador de domínio na VNet ou o Microsoft Entra Connect para seu Active Directory local.

  Depois de habilitar o AADDS, você não pode 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 prosseguir, revise o artigo da Microsoft Considerações de rede para o Microsoft Entra Domain Services.
- **Intervalo de IP da VNet:** Ao criar a conexão, você deve fornecer um espaço de endereço CIDR disponível (endereço IP e prefixo de rede) que seja exclusivo entre os recursos de rede e as VNets do Azure que estão sendo conectadas. Este é o intervalo de IP atribuído às VMs dentro da VNet emparelhada do Citrix DaaS para Azure.

  Certifique-se de especificar um intervalo de IP que não se sobreponha a nenhum endereço que você usa em suas redes Azure e locais.

  - Por exemplo, se sua VNet do Azure tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão de emparelhamento de 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 endereço sobreposto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

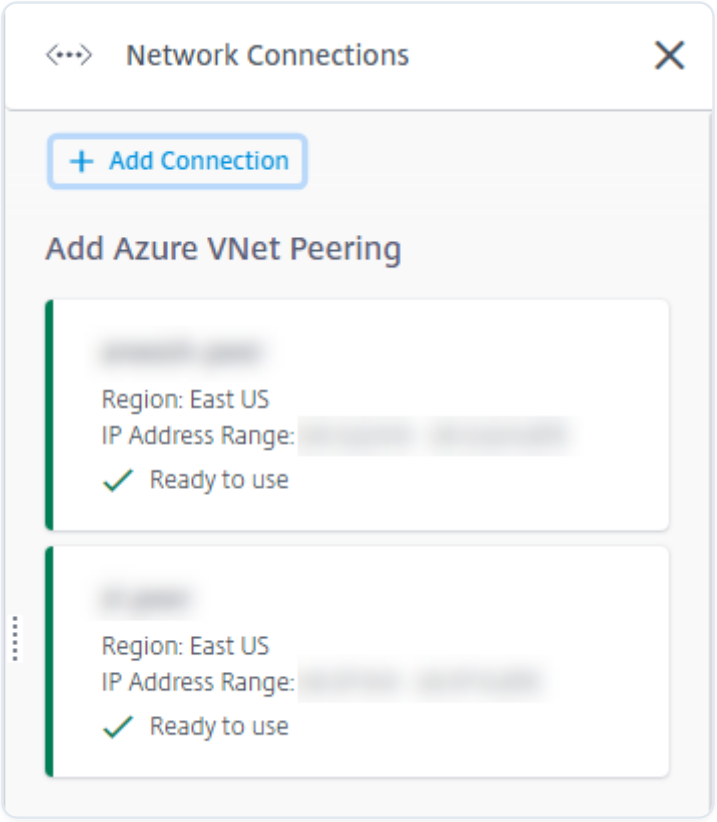
Se os endereços se sobrepuserem, a conexão de emparelhamento de VNet pode não ser criada com sucesso. Também não funciona corretamente para tarefas de administração do site.

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

- Emparelhamento de rede virtual
- Gateway de VPN do Azure
- Criar uma conexão Site a Site no portal do Azure
- Perguntas frequentes sobre o Gateway de VPN (pesquise por "overlap")

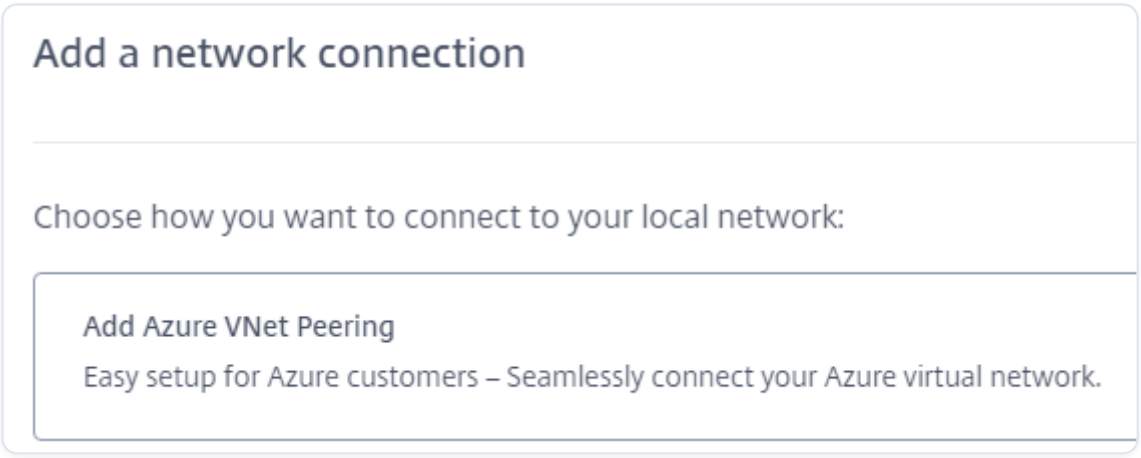
Criar uma conexão de emparelhamento de VNet do Azure

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita. Se você já configurou conexões, elas serão listadas.

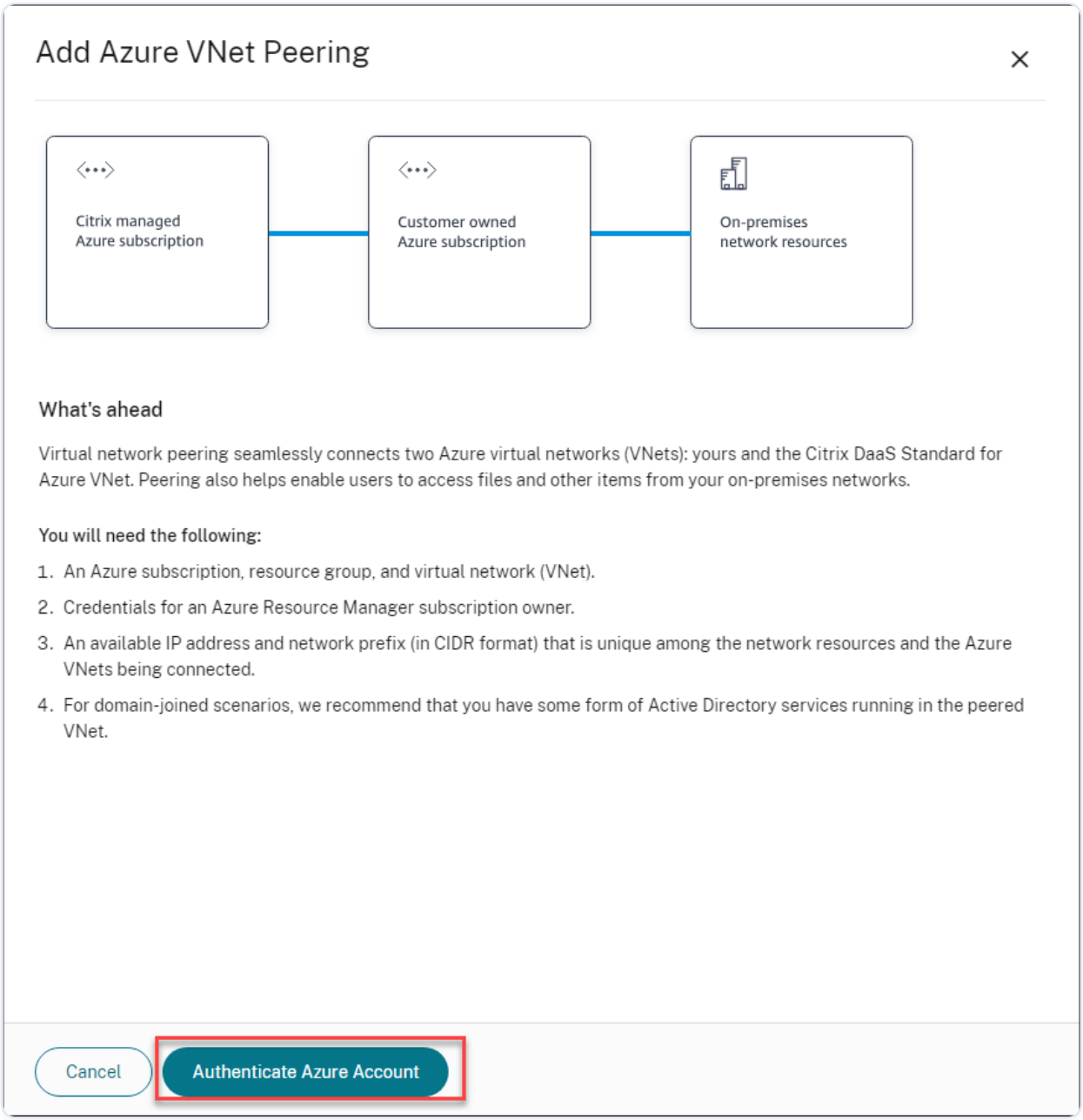


2. Clique em **Adicionar Conexão**.
3. Clique em qualquer lugar na caixa **Adicionar Emparelhamento de VNet do Azure**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



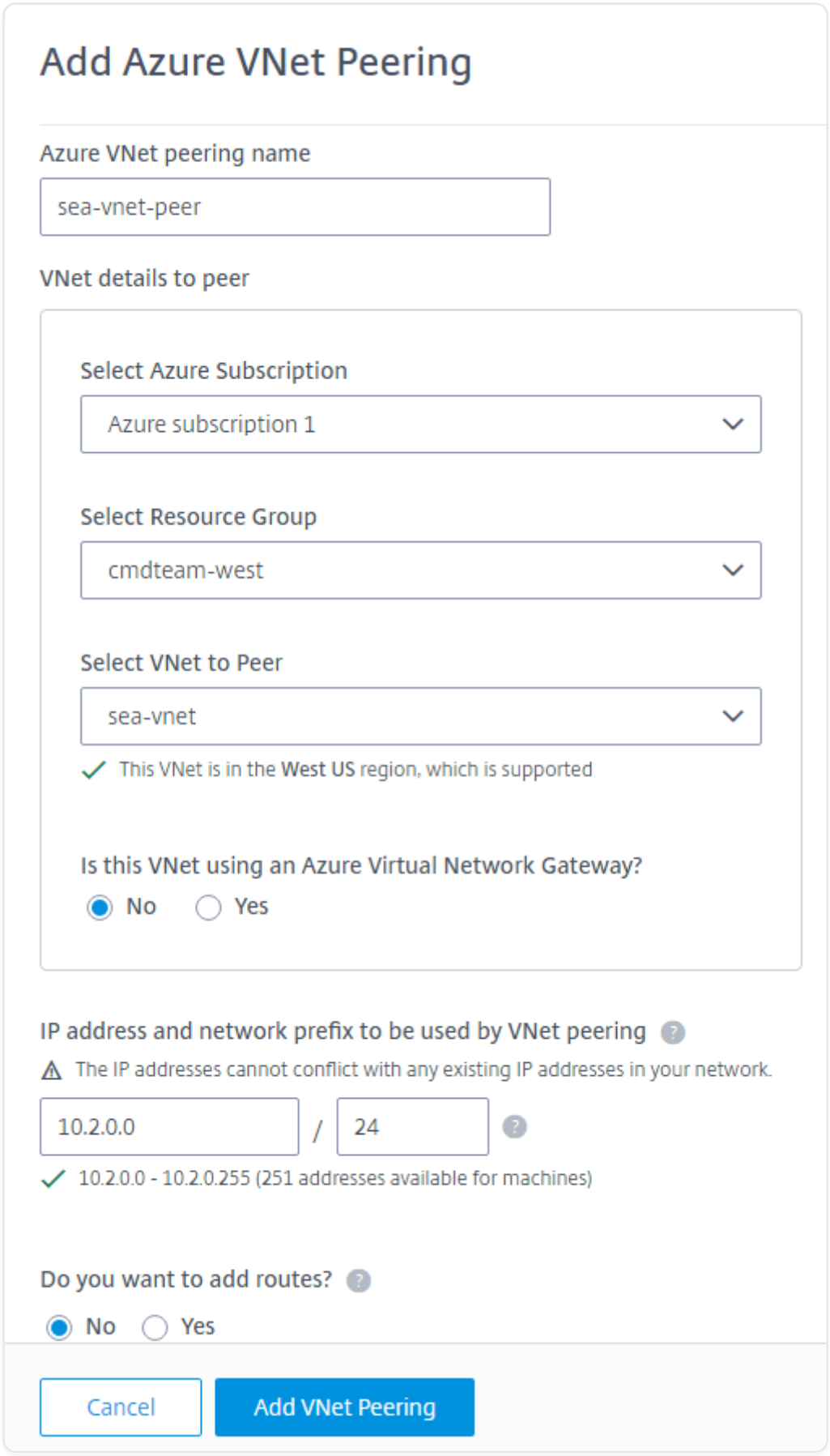
4. Clique em **autenticar Conta do Azure**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. O Citrix DaaS para Azure leva você automaticamente para a página de login do Azure para autenticar suas assinaturas do Azure. Depois de fazer login no Azure (com as credenciais da conta do proprietário da assinatura) e aceitar os termos, você é redirecionado para a caixa de diálogo de detalhes de criação da conexão.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Digite um nome para o emparelhamento de VNet do Azure.
7. Selecione a assinatura do Azure, o grupo de recursos e a VNet para emparelhar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 (adiciona) automaticamente todas as rotas através do gateway.

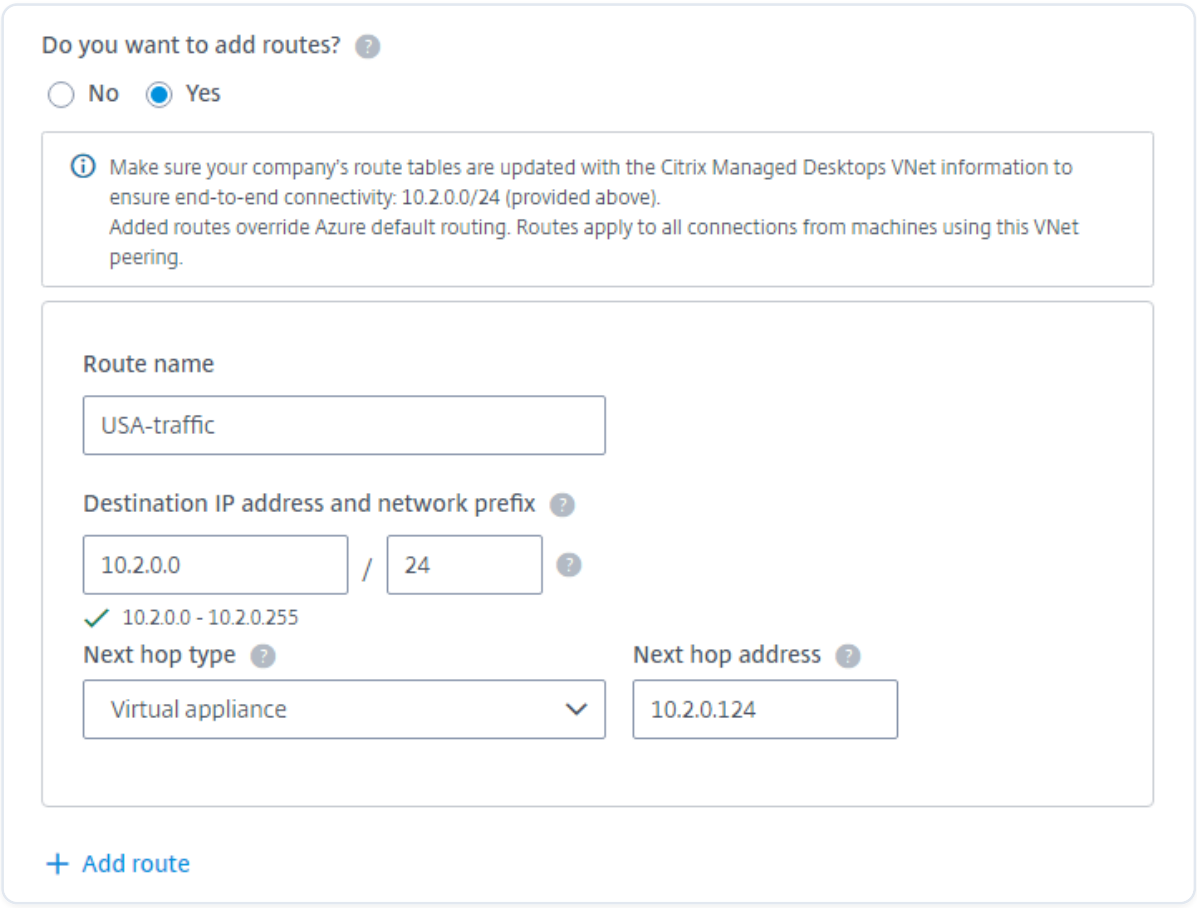
   Você pode alterar essa configuração mais tarde na página **Detalhes** da conexão. No entanto, alterá-la pode causar mudanças nos padrões de rota e interrupções no tráfego de VDA. Além disso, se você desativá-la mais tarde, deverá adicionar rotas manualmente às redes que os VDAs usarão.
10. Digite um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

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

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

    a. Digite um nome amigável para a rota personalizada.
    b. Insira o endereço IP de destino e o prefixo de rede. O prefixo de 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 **Dispositivo virtual**, insira o endereço IP interno do dispositivo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Para obter mais informações sobre os tipos de próximo 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.

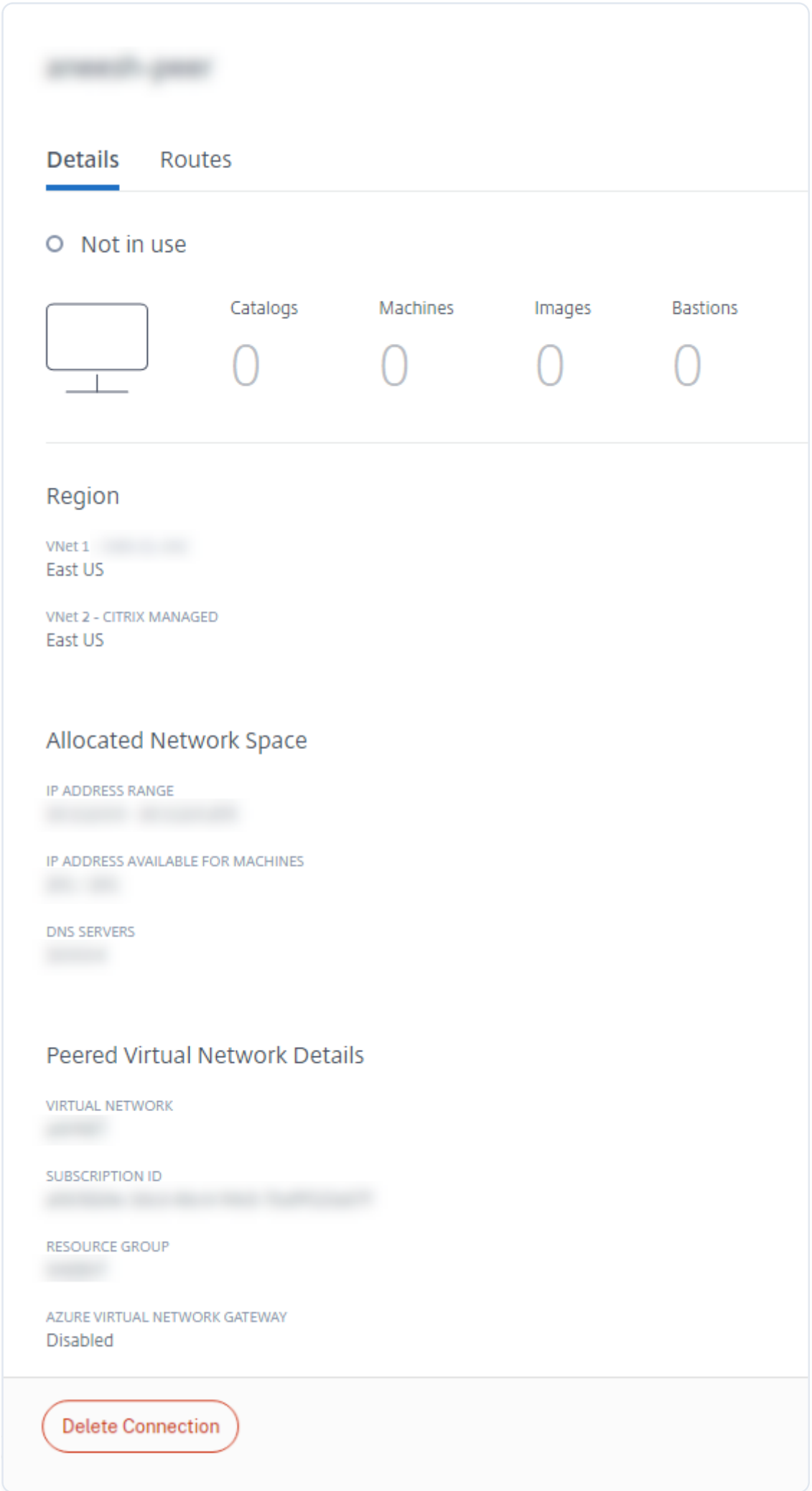
12. Clique em **Adicionar emparelhamento de VNet**.

Após a criação da conexão, ela é listada em **Conexões de Rede > Pares de VNet do Azure** no lado direito do painel **Implantação Rápida > Microsoft Azure**. Ao criar um catálogo, essa conexão é incluída na lista de conexões de rede disponíveis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Exibir detalhes da conexão de emparelhamento de VNet do Azure

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Details
Routes
Not in use
Catalogs
0
Machines
0
Images
0
Bastions
0
Region
VNet 1
East US
VNet 2 - CITRIX MANAGED
East US
Allocated Network Space
IP ADDRESS RANGE
IP ADDRESS AVAILABLE FOR MACHINES
DNS SERVERS
Peered Virtual Network Details
VIRTUAL NETWORK
SUBSCRIPTION ID
RESOURCE GROUP
AZURE VIRTUAL NETWORK GATEWAY
Disabled
Delete Connection

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

Os detalhes incluem:

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

Gerenciar rotas personalizadas para conexões de emparelhamento de VNet do Azure existentes

Você pode adicionar novas rotas personalizadas a uma conexão existente ou modificar rotas personalizadas existentes, incluindo desabilitar ou excluir rotas personalizadas.

IMPORTANTE:

Modificar, desabilitar ou excluir rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper quaisquer sessões de usuário que possam estar ativas.

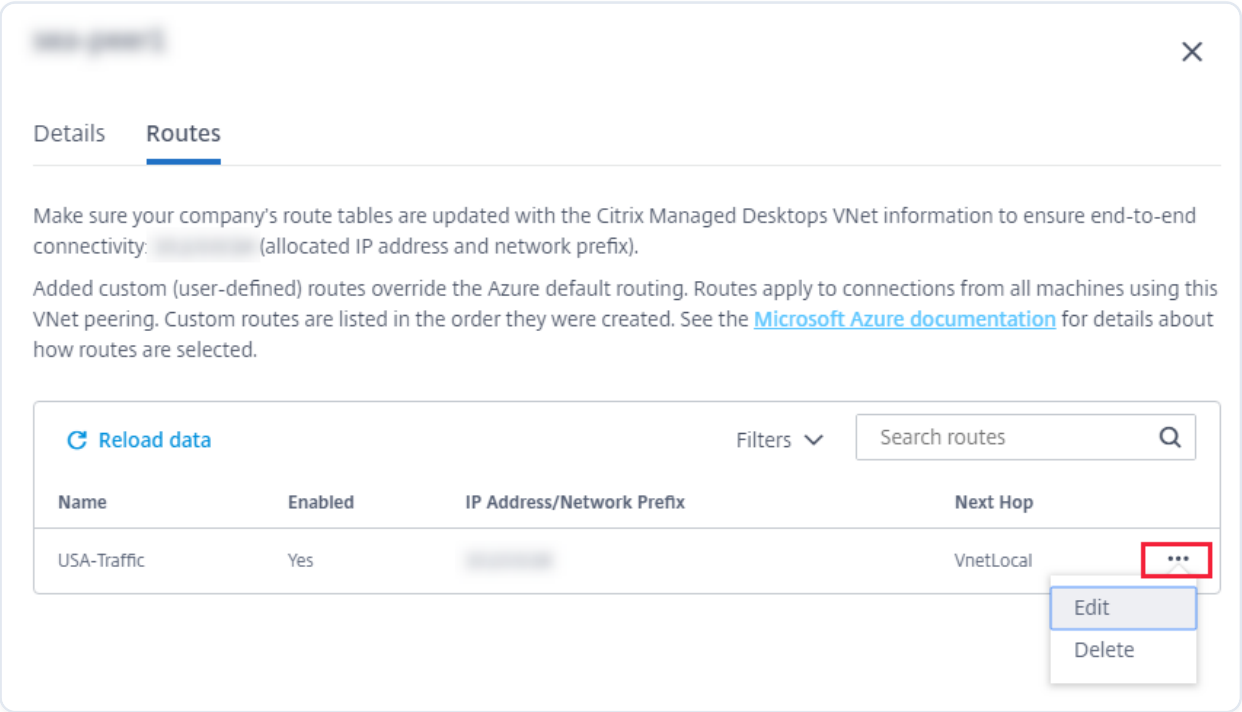
Para adicionar uma rota personalizada:

1. Nos detalhes da conexão de emparelhamento de VNet, selecione **Rotas** e clique em **Adicionar Rota**.
2. Insira um nome amigável, o endereço IP de destino e o prefixo, e o tipo de próximo salto que você deseja usar. Se você selecionar **Dispositivo Virtual** como o tipo de próximo salto, insira o endereço IP interno do dispositivo.
3. Indique se você deseja habilitar a rota personalizada. Por padrão, a rota personalizada está habilitada.
4. Clique em **Adicionar Rota**.

Para modificar ou desabilitar uma rota personalizada:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Faça as alterações necessárias no endereço IP de destino e prefixo 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 **Salvar**.

Para excluir uma rota personalizada:

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

Excluir uma conexão de emparelhamento de VNet do Azure

Antes de excluir um emparelhamento de VNet do Azure, remova todos os catálogos associados a ele. Consulte Excluir um catálogo.

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Selecione a conexão que você deseja excluir.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Nos detalhes da conexão, clique em **Excluir Conexão**.

Gateway VPN do Azure

O recurso 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 do Azure gerenciados pelo Citrix (desktops e aplicativos) e os recursos da sua empresa, como redes locais ou recursos em outros locais na nuvem. Isso é semelhante a configurar e conectar-se a um escritório remoto.

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

Durante o processo de criação da conexão:

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

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

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

Você também pode, opcionalmente, usar rotas personalizadas com este tipo de conexão.

Rotas personalizadas do gateway VPN do Azure

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 que os recursos do Citrix Virtual Apps and Desktops™ Standard devem acessar, mas que não estão diretamente conectadas por meio de um gateway VPN do Azure. Por exemplo, você pode criar uma rota personalizada que força o tráfego através de um dispositivo de rede para a Internet ou para uma sub-rede de rede local.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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.
- 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, revise 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

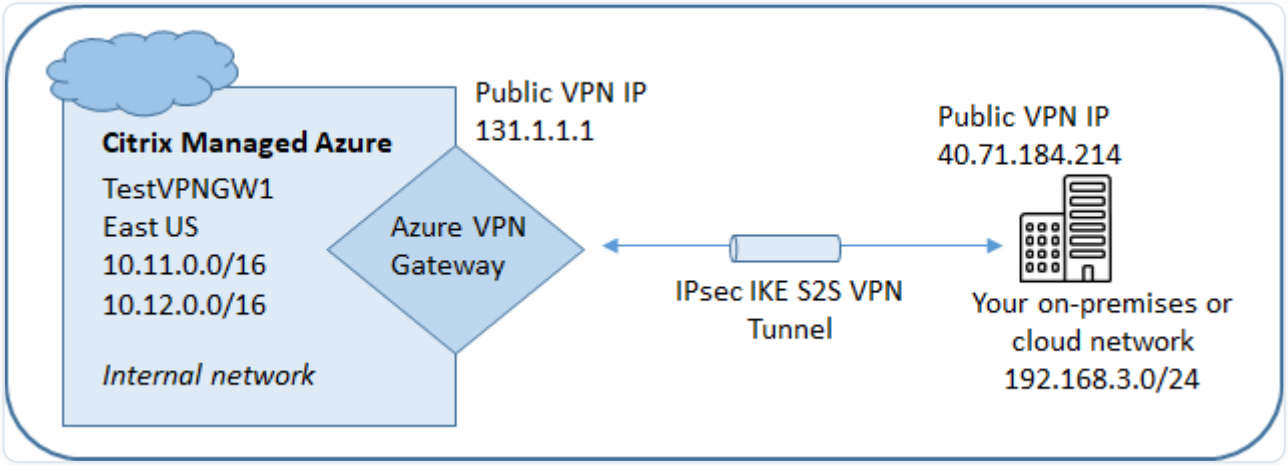
- Para saber mais sobre o Gateway VPN do Azure, consulte o artigo da Microsoft O que é o Gateway VPN?
- Revise os requisitos para todas as conexões de rede.
- Você deve ter uma VPN configurada. A rede virtual deve ser capaz de enviar e receber tráfego através do gateway VPN. Uma rede virtual não pode 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 de Gateway VPN do Azure antes de realmente iniciá-lo, para que você possa coletar as informações necessárias. Por exemplo, você precisará de endereços permitidos em sua rede, intervalos de IP para os VDAs e o gateway, taxa de transferência e nível de desempenho desejados e endereços de servidor DNS.

Criar uma conexão de gateway VPN do Azure

Certifique-se de revisar este procedimento antes de realmente iniciá-lo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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** do Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Clique em **Adicionar Conexão**.
3. Clique em qualquer lugar na caixa **Azure VPN Gateway**.
4. Revise as informações na página **Adicionar Conexão VPN** e, em seguida, 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 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. Geralmente, esse intervalo de endereços contém os recursos que seus 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 ao configurar sua VPN com as informações de conexão.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

- **Região:** Região do Azure onde o Citrix implanta máquinas que entregam desktops e aplicativos (VDAs), ao criar catálogos que usam esta conexão. Você não pode alterar esta seleção depois de criar a conexão. Se você decidir mais tarde usar uma região diferente, 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 este modo está habilitado, apenas um gateway está ativo por vez. Saiba mais sobre o gateway VPN ativo-ativo do Azure no documento da Microsoft Conectividade entre locais altamente disponível.

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

  - **Número do 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 exige que seus ASNs sejam diferentes. Se necessário, você pode alterar o ASN agora ou depois que o gateway for criado.
  - **Endereço IP de emparelhamento BGP:** O Azure oferece suporte a IP BGP no intervalo de 169.254.21.*x* a 169.254.22.*x*.

- **Sub-rede VDA:** O intervalo de endereços onde os VDAs Citrix (máquinas que entregam 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 esse 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 se sobrepor a nenhum endereço que você usa em suas redes locais ou em outras redes de nuvem. Se os endereços se sobrepuserem, a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

conexão poderá não ser criada com êxito. Além disso, um endereço sobreposto não funcionará corretamente para tarefas de administração do site.

- O intervalo da sub-rede VDA deve ser diferente do endereço da 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 onde o gateway VPN do Azure residirá quando você criar um catálogo que usa essa conexão.

  - O intervalo de IP não deve se sobrepor a 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 da sub-rede do gateway deve ser diferente do endereço da sub-rede 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 deseja adicionar rotas personalizadas, forneça as seguintes informações:

  - Digite um nome amigável para a rota personalizada.
  - Insira o endereço IP de destino e o prefixo de rede. O prefixo de 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 **Dispositivo virtual, insira o endereço IP interno do dispositivo. Para obter mais informações sobre os tipos de próximo 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 preferencial. Embora você possa alterar as entradas do servidor DNS posteriormente, lembre-se de que alterá-las pode causar problemas de conectividade para as máquinas nos catálogos que usam essa conexão.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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** do Citrix DaaS para Azure. O cartão de conexão contém um endereço IP público. (No diagrama, o endereço é 131.1.1.1.)

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

  Por exemplo, permita exceções em seu firewall para os intervalos de endereços IP da sub-rede 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 sucesso, a entrada da conexão em **Conexões de Rede > Gateway VPN do Azure** indica **Pronto para usar**.

Visualizar uma conexão de gateway VPN do Azure

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

   Exibe:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gerenciar rotas personalizadas para uma conexão de gateway VPN do Azure

Em uma conexão de gateway VPN do Azure existente, você pode adicionar, modificar, desabilitar 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, desabilitar ou excluir rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper sessões de usuário ativas.

1. No painel **Gerenciar** do Citrix DaaS para 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. Insira um nome amigável, o endereço IP de destino e o prefixo, e o tipo de próximo salto que você deseja usar. Se você selecionar **Dispositivo Virtual** como o tipo de próximo salto, insira o endereço IP interno do dispositivo.
     c. Indique se você deseja habilitar a rota personalizada. Por padrão, a rota personalizada está habilitada.
     d. Clique em **Adicionar Rota**.
   - Para modificar ou habilitar/desabilitar 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 de destino e o prefixo, ou o tipo de próximo salto, conforme necessário.
     d. Indique se você deseja habilitar a rota.
     e. Clique em **Salvar**.
   - 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Selecione **A exclusão de uma rota pode interromper 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:

- Redefinir uma conexão faz com que a conexão atual seja perdida, e ambas as extremidades devem restabelecê-la. Uma redefinição interrompe as sessões de usuário ativas.
- Antes de excluir uma conexão, exclua todos os catálogos que a utilizam. Consulte Excluir um catálogo.

Para redefinir ou excluir uma conexão:

1. No painel **Gerenciar** no Citrix DaaS para 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.

Criar um endereço IP estático público

Se você deseja 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 são ingressados no domínio ou não ingressados no domínio.

Para habilitar um gateway NAT para uma conexão:

1. No painel **Implantação Rápida > Microsoft Azure** no Citrix DaaS para Azure, expanda **Conexões de Rede** à direita.
2. Em **Conexões de Rede**, selecione uma conexão em **GERENCIADO PELA CITRIX** ou **PEERINGS DE VNET DO AZURE**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. No cartão de detalhes da conexão, clique em **Habilitar Gateway NAT**.
4. Na página Habilitar NAT Gateway, mova o controle deslizante para **Sim** e configure um tempo de inatividade.
5. Clique em **Confirmar Alterações**.

Ao habilitar um gateway NAT:

- O Azure atribui automaticamente um endereço IP estático público ao gateway. (Você não pode especificar este endereço.) Todos os VDAs em todos os catálogos que usam esta conexão usarão esse endereço para conectividade de saída.
- Você pode especificar um valor de tempo limite de inatividade. 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 ao cartão de detalhes da conexão para habilitar ou desabilitar o gateway NAT e alterar o valor do tempo limite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Imagens

Ao criar um catálogo para entregar desktops 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)
- Windows 11 Enterprise Virtual Desktop (multissessão)
- Windows 11 Enterprise Virtual Desktop (multissessão) com Office 365 ProPlus
- Windows 10 Pro (sessão única)
- Windows 10 Enterprise Virtual Desktop (multissessão)
- Windows 10 Enterprise Virtual Desktop (multissessão) com Office 365 ProPlus
- Windows Server 2019 (multissessão)
- Windows Server 2022 (multissessão)
- Windows Server 2025 (multissessão)
- Linux Ubuntu 22.04 LTS (sessão única)
- Linux Ubuntu 22.04 LTS (multissessão)

As imagens preparadas pela Citrix têm um Citrix Virtual Delivery Agent (VDA) atual e ferramentas de solução de problemas instalados. 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 anotadas como **CITRIX**.

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

Maneiras de usar imagens

Você pode:

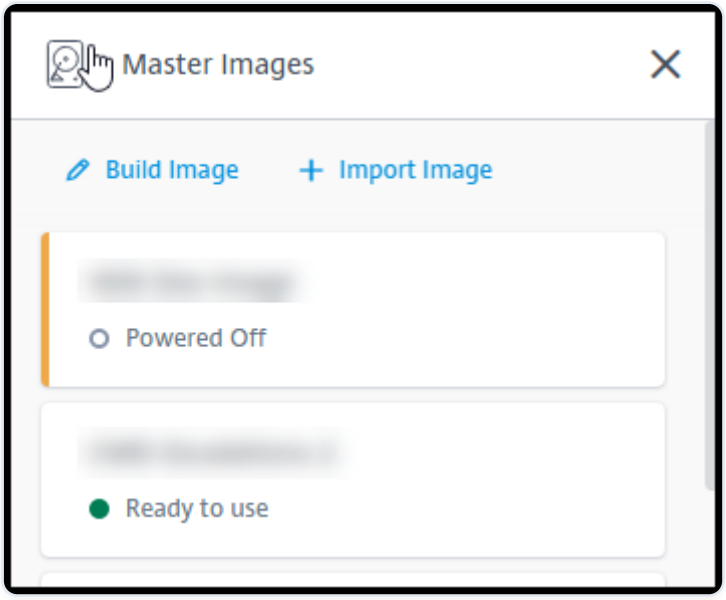
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Usar uma imagem preparada pela Citrix ao criar um catálogo.** Esta opção é recomendada apenas para implantações de prova de conceito.
- **Usar uma imagem preparada pela Citrix para criar outra imagem.** Depois que a nova imagem for criada, você a personaliza adicionando aplicativos e outros softwares que seus usuários precisam. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.
- **Importar uma imagem do Azure.** Depois de importar uma imagem do Azure, você pode usá-la ao criar um catálogo. Ou, você pode usar essa imagem para criar uma nova imagem e, em seguida, personalizá-la adicionando aplicativos. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.

Ao criar um catálogo, o Citrix DaaS™ para Azure verifica se a imagem usa um sistema operacional válido e se tem um Citrix VDA e ferramentas de solução de problemas instalados (juntamente com outras verificações).

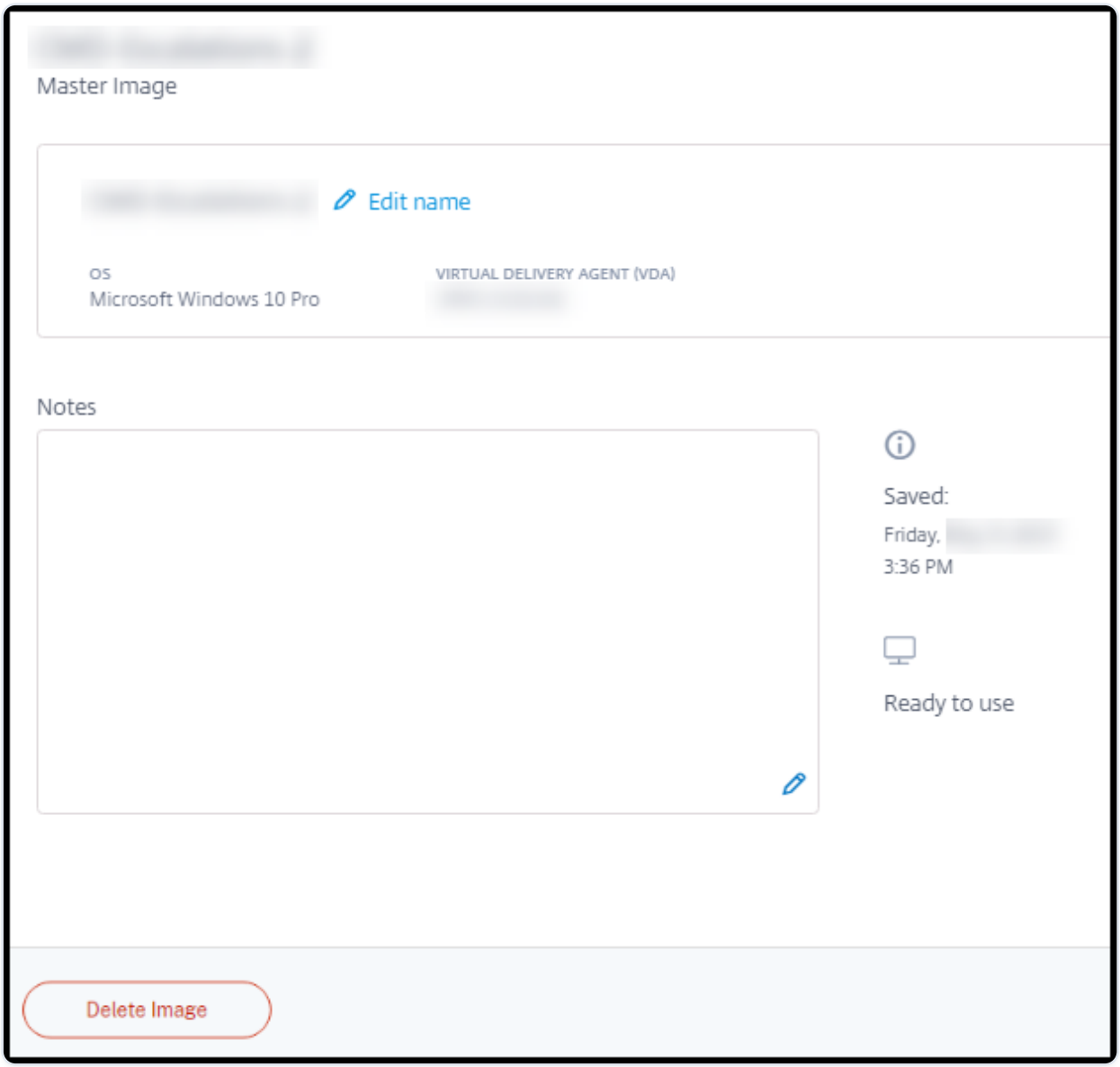
Exibir informações da imagem

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Master Images** à direita. A exibição lista as imagens fornecidas pela Citrix e as imagens que você criou e importou.



2. Clique em uma imagem para exibir seus detalhes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



No cartão de detalhes, você pode:

- Alterar (editar) o nome da imagem.
- Adicionar e editar notas (Disponível apenas para imagens que você preparou ou importou, não para imagens fornecidas pela Citrix).
- Excluir a imagem.

Preparar uma nova imagem

Preparar uma nova imagem inclui criar a imagem e depois personalizá-la. Ao criar uma imagem, uma nova VM é criada para carregar a nova imagem.

Requisitos:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Conheça as características de desempenho que as máquinas precisam. Por exemplo, a execução de aplicativos CAD pode exigir CPU, RAM e armazenamento diferentes dos de 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 Conexões de rede.

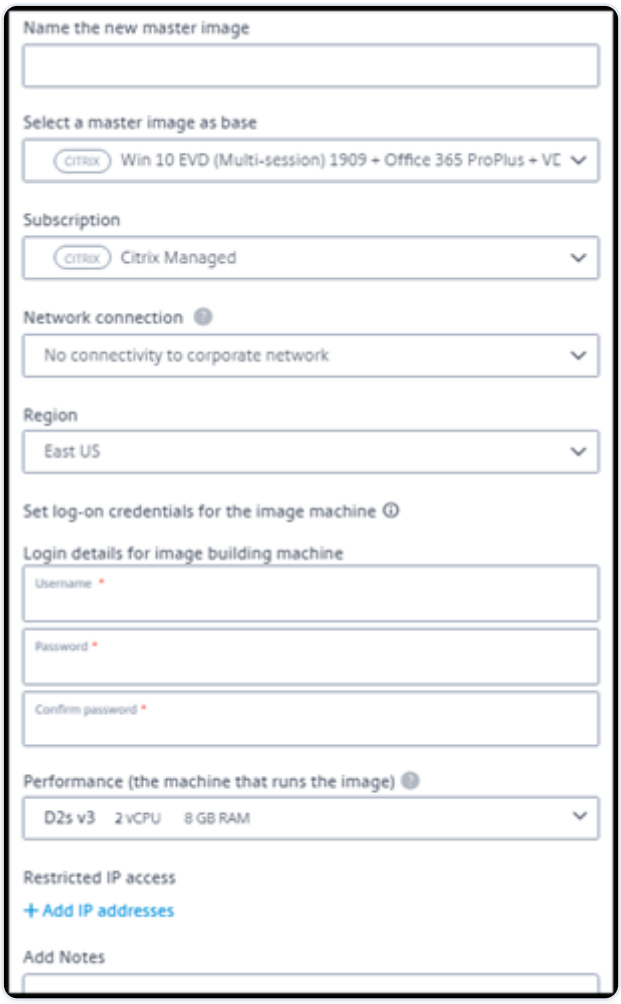
Ao usar uma imagem Ubuntu preparada pela Citrix para criar uma nova imagem, uma senha de root é criada para a nova imagem. Você pode alterar essa senha de root, mas apenas durante o processo de criação e personalização da imagem. (Você não pode alterar a senha de root depois que a imagem é usada em um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

- Quando a imagem é criada, a conta de administrador que você especificou (**Detalhes de login para a máquina de criação de imagem**) é adicionada ao grupo `sudoers`.
- Depois de fazer RDP na máquina que contém a nova imagem, inicie o aplicativo de terminal e digite `sudo passwd root`. Quando solicitado, forneça a senha que você especificou 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 **Quick Deploy > Microsoft Azure**, expanda **Imagens Mestre** à direita.
2. Clique em **Criar Imagem**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Insira valores nos seguintes campos:

   - **Nome:** Insira um nome para a nova imagem.
   - **Imagem mestre:** Selecione uma imagem existente. Esta 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 Azure gerenciada pela Citrix, selecione **Sem conectividade** 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 de domínio:** Selecione o tipo de domínio: Active Directory ou não associado ao domínio.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - 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 associado ao 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.
- **Credenciais de logon para a máquina da imagem:** Você usará essas credenciais mais tarde ao se conectar (RDP) à máquina que contém a nova imagem, para que possa instalar aplicativos e outros softwares.
- **Desempenho da máquina:** São informações de CPU, RAM e armazenamento para a 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, em seguida, 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 for criada, você poderá atualizar as notas na exibição de detalhes da imagem.
- **Associação de domínio local:** Indique se você deseja ingressar no domínio Active Directory local.

    - 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 para a máquina host.

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

Uma imagem pode levar até 30 minutos para ser criada. No painel **Quick Deploy > Microsoft Azure**, expanda **Imagens Mestre** à direita para ver o estado atual (como **Criando imagem** ou **Pronto para personalizar**).

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

Conectar-se a uma nova imagem e personalizá-la

Depois que uma nova imagem é criada, seu nome é adicionado à lista de imagens, com um status de **Pronto para personalizar** (ou redação semelhante). Para personalizar essa imagem, primeiro

© 1997–2026 Citrix Systems, Inc. All rights reserved.

você baixa um arquivo RDP. Ao usar esse arquivo para se conectar à imagem, você pode adicionar aplicativos e outros softwares à imagem.

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Imagens Mestre** à direita. Clique na imagem à qual você deseja se conectar.
2. Clique em **Baixar arquivo RDP**. Um cliente RDP é baixado.

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

   NÃO execute o Sysprep na imagem.
5. Quando terminar de personalizar a nova imagem, retorne à caixa **Imagens Mestre** e clique em **Concluir compilação**. A nova imagem passa automaticamente por testes de validação.

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

No painel **Quick Deploy > Microsoft Azure**, a exibição das imagens à direita indica quantos catálogos e máquinas usam cada imagem.

NOTA:

Depois de finalizar uma imagem, você não pode 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 os aplicativos de que seus usuários precisam, você pode usá-la para criar um catálogo ou substituir a imagem em um catálogo existente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requisitos da imagem importada

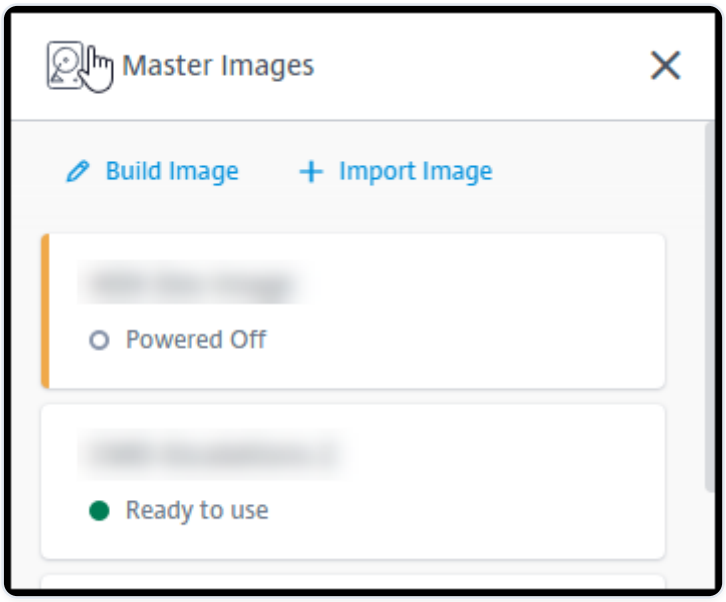
A Citrix executa testes de validação na imagem importada. Certifique-se de que os seguintes requisitos sejam atendidos ao preparar a imagem que você importará para o Citrix DaaS para Azure.

- **SO compatível:** A imagem deve ser um SO compatível. Para verificar uma versão do SO Windows, execute `Get-WmiObject Win32_OperatingSystem`.
- **Geração compatível:** As máquinas virtuais de Geração 1 suportam a maioria dos sistemas operacionais convidados. As máquinas virtuais de Geração 2 suportam a maioria das versões de 64 bits do Windows e versões mais recentes de sistemas operacionais Linux.
- **Não generalizada:** A imagem não deve ser generalizada.
- **Nenhum Delivery Controller configurado:** Certifique-se de que nenhum Citrix Delivery Controller esteja configurado na imagem. Certifique-se de que as seguintes chaves de registro sejam limpas.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Arquivo Personality.ini:** O `personality.ini` arquivo deve existir na unidade do sistema.
- **VDA válido:** 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 orientação sobre a instalação, consulte Instalar um VDA do Windows em uma imagem.
  - Red Hat Enterprise Linux e Ubuntu: Para obter orientação sobre a instalação, consulte a documentação do produto.
- **Agente de Máquina Virtual do Azure:** Antes de importar uma imagem, certifique-se de que o Agente de Máquina Virtual do Azure esteja instalado na imagem. Para obter mais informações, consulte o artigo da Microsoft Visão geral do Agente de Máquina Virtual do Azure.

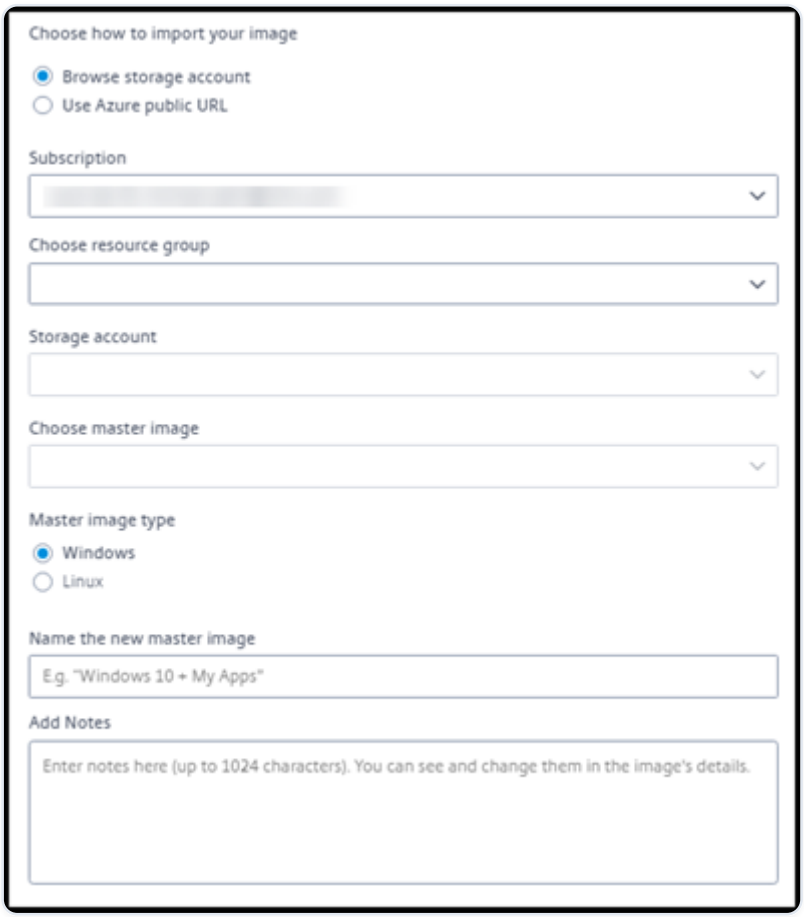
Importar a imagem

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Imagens Mestre** à direita.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Clique em **Importar Imagem**.



3. Escolha como importar a imagem.

   - Para discos gerenciados, use o recurso de exportação para gerar uma URL SAS. Defina o tempo de expiração para 7200 segundos ou mais.
   - Para VHDs em uma conta de armazenamento, escolha uma das seguintes opções:
     - Gere uma URL SAS para o arquivo VHD.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Atualize o nível de acesso de um contêiner de armazenamento de blocos para blob ou contêiner. Em seguida, obtenha a URL do arquivo.

4. Se você selecionou **Procurar conta de armazenamento**:
   a. Selecione sequencialmente uma assinatura > grupo de recursos > conta de armazenamento > imagem.
   b. Nomeie a imagem.
5. Se você selecionou **URL pública do Azure**:
   a. Insira a URL gerada 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 Linux pode ser importada somente se você selecionar uma assinatura gerenciada pelo cliente.)
   c. Nomeie a imagem.
6. Quando terminar, clique em **Importar Imagem**.

Atualizar um catálogo com uma nova imagem

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

- Para um catálogo aleatório, todas as máquinas atualmente no catálogo são atualizadas com a imagem mais recente. Se você adicionar mais desktops a esse catálogo, eles serão baseados na imagem mais recente.
- Para um catálogo estático, as máquinas atualmente no catálogo não são atualizadas com a imagem mais recente. As máquinas atualmente no catálogo continuam a usar a imagem 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 suportarem gen1.

Para atualizar um catálogo com uma nova imagem:

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Detalhes**, clique em **Atualizar Imagem**.

   Atualizar uma imagem em um catálogo(/en-us/citrix-daas-azure/media/image-update.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Excluir uma imagem

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Imagens Mestre** à direita.
2. Clique na imagem que você deseja excluir.
3. Clique em **Excluir Imagem** na parte inferior do cartão. Confirme a exclusão.

Instalar um VDA do Windows em uma imagem

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

1. No seu ambiente Azure, conecte-se à VM da 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 para Azure.

   Baixe um VDA para a VM. Existem pacotes de download de VDA separados para um SO de desktop (sessão única) e um SO de servidor (várias sessões).
3. Inicie o instalador do VDA clicando duas vezes no arquivo baixado. O assistente de instalação será iniciado.
4. Na página **Ambiente**, selecione a opção para criar uma imagem usando MCS e clique em **Avançar**.
5. Na página **Componentes Principais**, clique em **Avançar**.
6. Na página **Delivery Controller**, selecione **Deixar o Machine Creation Services™ fazer isso automaticamente** e clique em **Avançar**.
7. Deixe as configurações padrão nas páginas **Componentes Adicionais**, **Recursos** e **Firewall**, a menos que a Citrix o instrua de outra forma. Clique em **Avançar** em cada página.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 dos pré-requisitos é concluída e, em seguida, os componentes e recursos são instalados. Na página **Call Home**, deixe a configuração padrão (a menos que a Citrix o instrua de outra forma). Depois de se conectar, clique em **Avançar**.
10. Clique em **Concluir**. 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 execute o Sysprep na imagem.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usuários e autenticação

Métodos de autenticação de usuário

Os usuários devem autenticar ao fazer login no Citrix Workspace™ para iniciar seu desktop ou aplicativos.

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

- **Managed Microsoft Entra ID:** O Managed Microsoft Entra ID é um Microsoft Entra ID fornecido e gerenciado pela Citrix. Você não precisa fornecer sua própria estrutura de 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 apenas o Active Directory. Para obter detalhes, consulte Remote PC Access.
- Se você usa o Microsoft Entra Domain Services: os UPNs de logon do Workspace devem conter o nome de domínio que foi especificado ao habilitar o Microsoft Entra Domain Services. Os logons não podem usar UPNs para um domínio personalizado que você criar, mesmo que esse domínio personalizado seja designado como primário.

A configuração da autenticação de usuário inclui os seguintes procedimentos:

1. Configurar o método de autenticação de usuário no Citrix Cloud e na Configuração do Workspace.
2. Se você estiver usando o Managed Microsoft Entra ID para autenticação de usuário, adicione usuários ao diretório.
3. Adicionar usuários a um catálogo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurar a autenticação de usuário no Citrix Cloud

Para configurar a autenticação de usuário no Citrix Cloud:

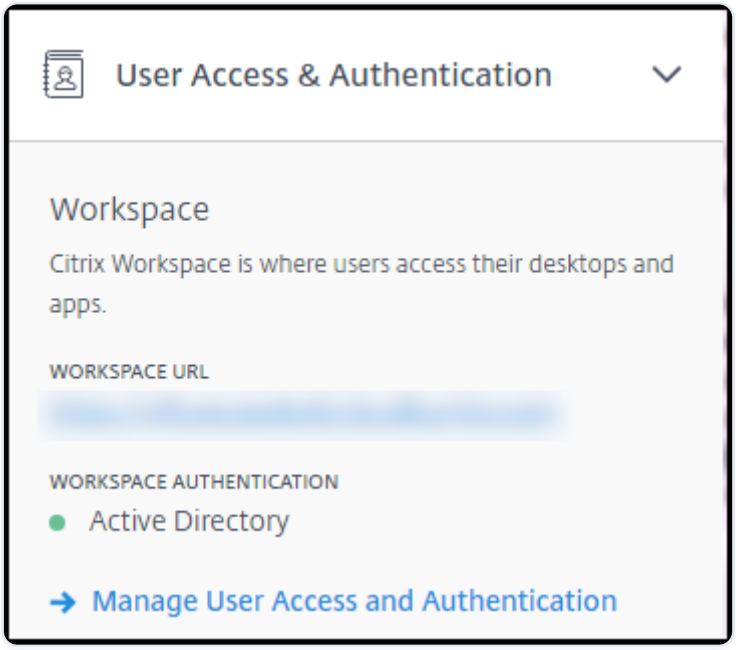
- Conecte-se ao método de autenticação de usuário que você deseja usar. (No Citrix Cloud, você se "conecta" ou "desconecta" de um método de autenticação.)
- No Citrix Cloud, defina a autenticação do Workspace para usar o método conectado.

NOTA:

O método de autenticação Managed Microsoft Entra 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 Microsoft Entra ID para Citrix DaaS para Azure. Se você quiser usar este método (e não tiver configurado um método diferente anteriormente), continue com Adicionar e excluir usuários no Managed Microsoft Entra ID. Se o Managed Microsoft Entra ID for desconectado, a autenticação do Workspace será alterada para Active Directory. Se você quiser usar um método de autenticação diferente, siga as etapas abaixo.

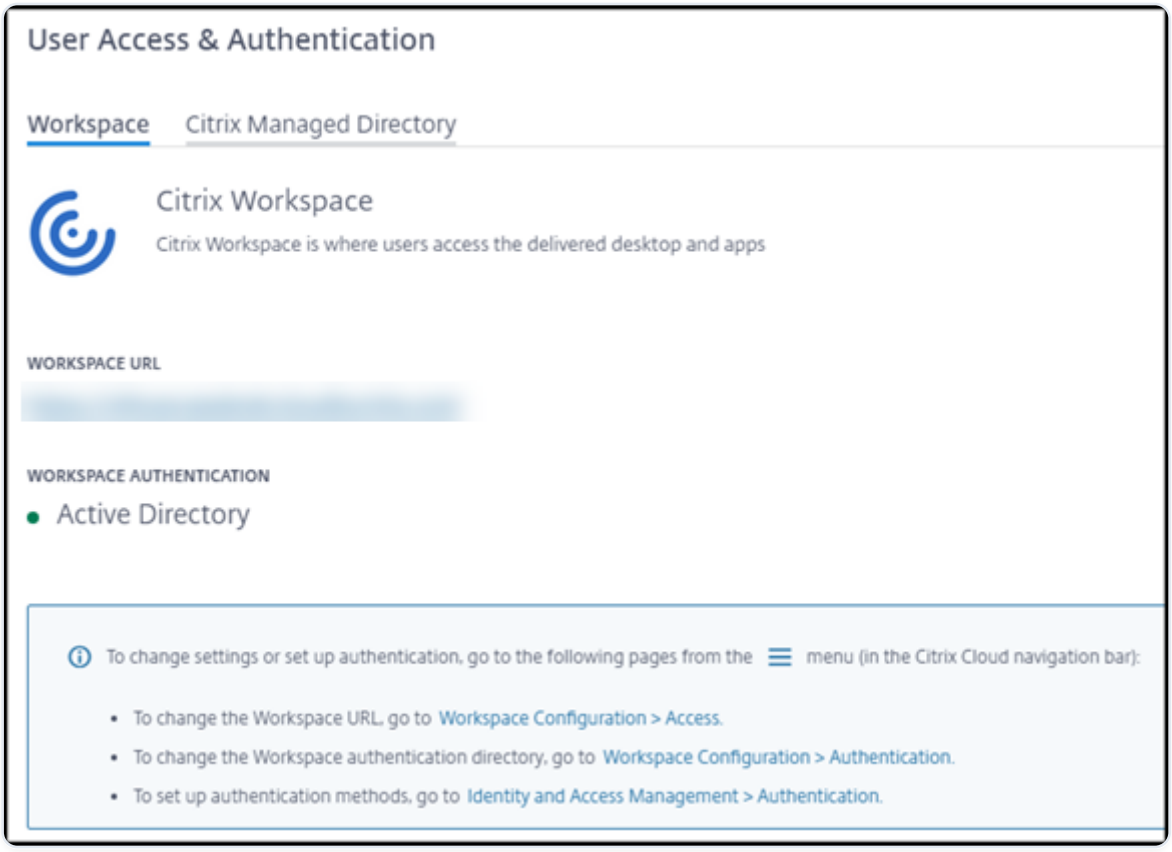
Para alterar o método de autenticação:

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, clique em **User Access & Authentication** à direita.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Clique em **Manage User Access and Authentication**. Selecione a guia **Workspace**, se ainda não estiver selecionada. (A outra guia indica qual método de autenticação de usuário está configurado atualmente.)



3. Siga o link **To set up authentication methods**. Esse link o levará ao Citrix Cloud. Selecione **Connect** no menu de reticências para o método desejado.
4. Ainda no Citrix Cloud, selecione **Workspace Configuration** no menu superior esquerdo. Na guia **Authentication**, selecione o método desejado.

O que fazer a seguir:

- Se você estiver usando o Managed Microsoft Entra ID, adicione usuários ao diretório.
- Para todos os métodos de autenticação, adicione usuários ao catálogo.

Adicionar e excluir usuários no Managed Microsoft Entra ID

Conclua este procedimento somente se você estiver usando o Managed Microsoft Entra ID para autenticação de usuário no Citrix Workspace.

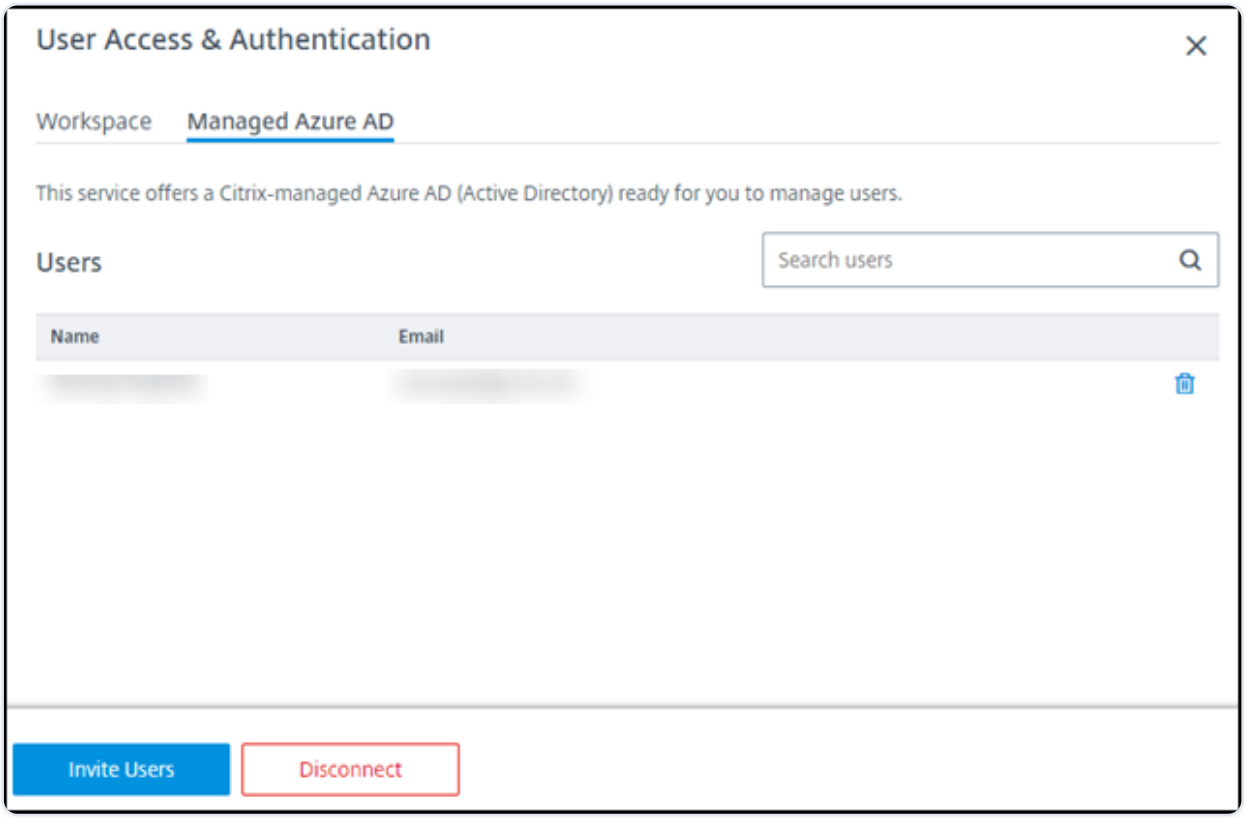
Você fornece o nome e os endereços de e-mail dos seus usuários. A Citrix envia um convite por e-mail para cada um deles. O e-mail instrui os usuários a clicar em um link que os conecta ao Citrix Managed Microsoft Entra ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Se o usuário já tiver uma conta Microsoft com o endereço de e-mail fornecido, essa conta será usada.
- Se o usuário não tiver uma conta Microsoft com o endereço de e-mail, a Microsoft criará uma conta.

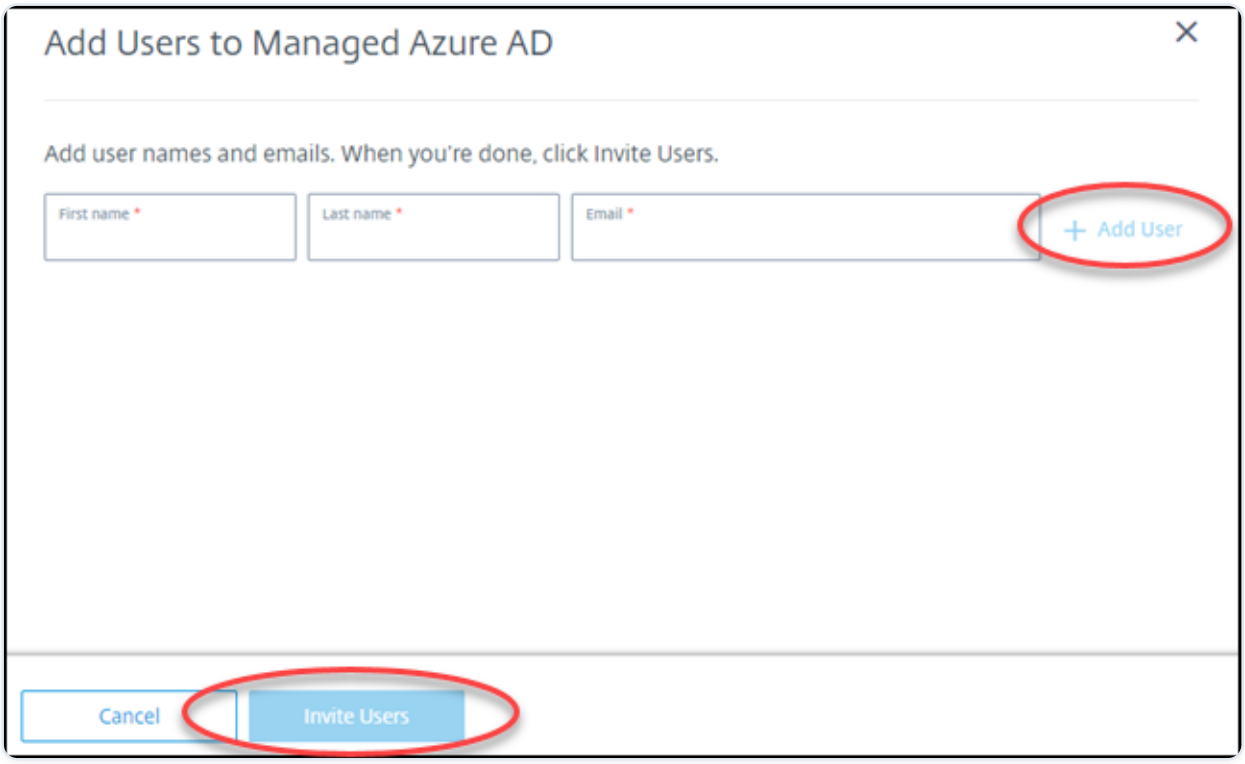
Para adicionar e convidar usuários para o Managed Microsoft Entra ID:

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **User Access & Authentication** à direita. Clique em **Manage User Access and Authentication**.
2. Clique na guia **Managed Microsoft Entra ID**.
3. Clique em **Invite Users**.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

Para excluir um usuário do Managed Microsoft Entra ID, clique no ícone da lixeira ao lado do nome do usuário que você deseja excluir do diretório. Confirme a exclusão.

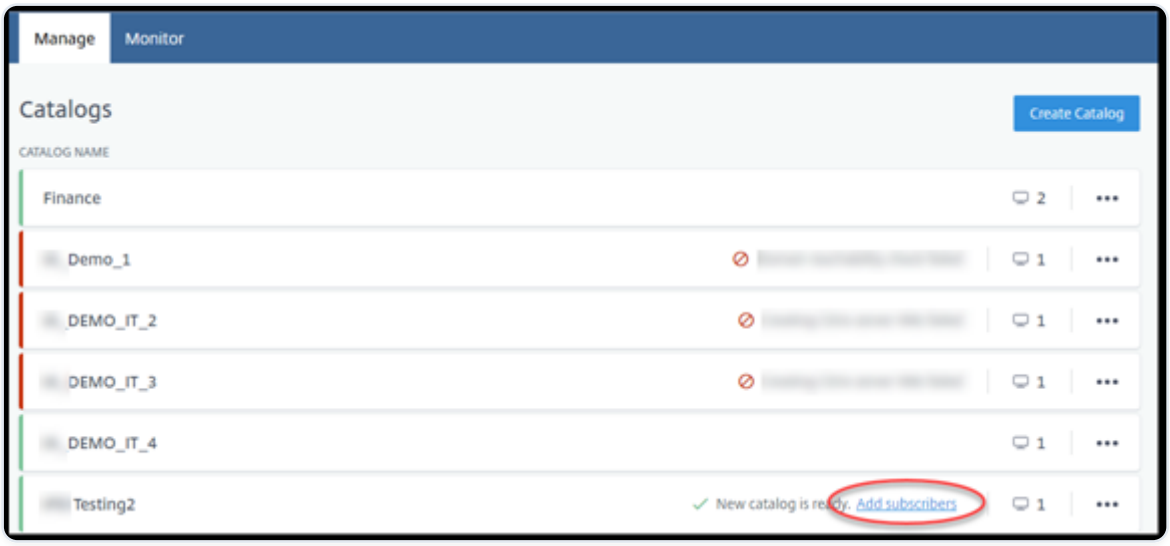
O que fazer a seguir: Adicionar usuários ao catálogo

Adicionar ou remover usuários em um catálogo

Conclua este procedimento independentemente do método de autenticação que você usa.

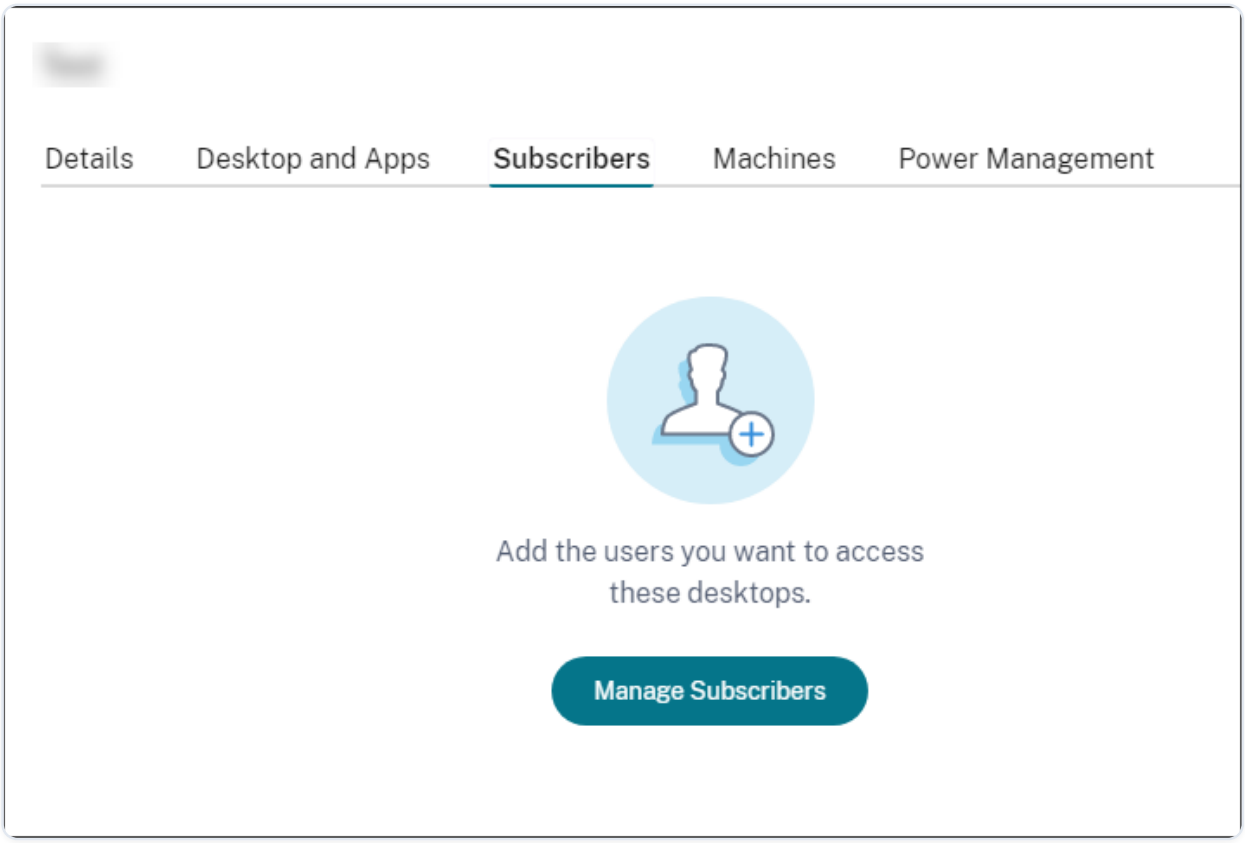
1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, se você ainda não adicionou nenhum usuário a um catálogo, clique em **Adicionar assinantes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



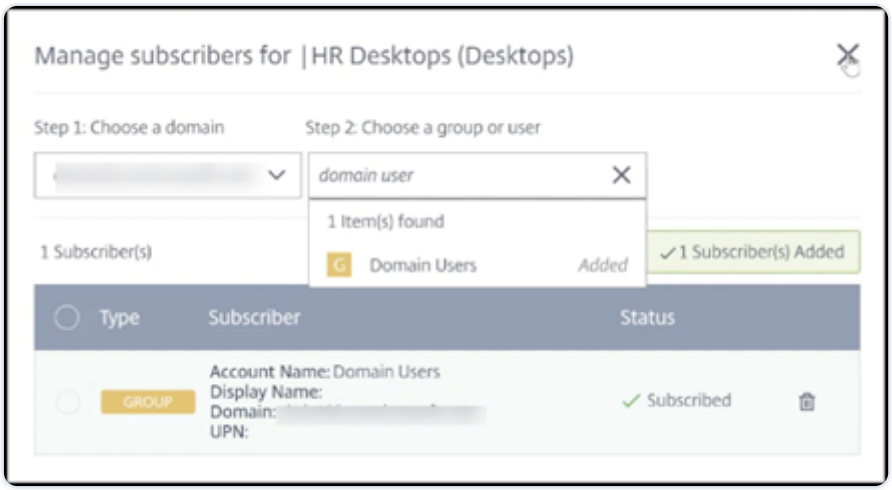
Para adicionar usuários a um catálogo que já possui usuários, clique em qualquer lugar na entrada do catálogo.

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



3. Selecione um domínio. (Se você estiver usando o Managed Microsoft Entra ID para autenticação de usuário, haverá apenas uma entrada no campo de domínio.) Em seguida, selecione um usuário.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

Para remover usuários de um catálogo, siga os passos 1 e 2. No passo 3, clique no ícone da lixeira ao lado do nome que você deseja excluir (em vez de selecionar um domínio e grupo/usuário). Esta ação remove o usuário do catálogo, não da origem (como Managed Microsoft Entra ID ou seu próprio AD ou AAD).

O que fazer a seguir:

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

Mais informações

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gerenciar catálogos

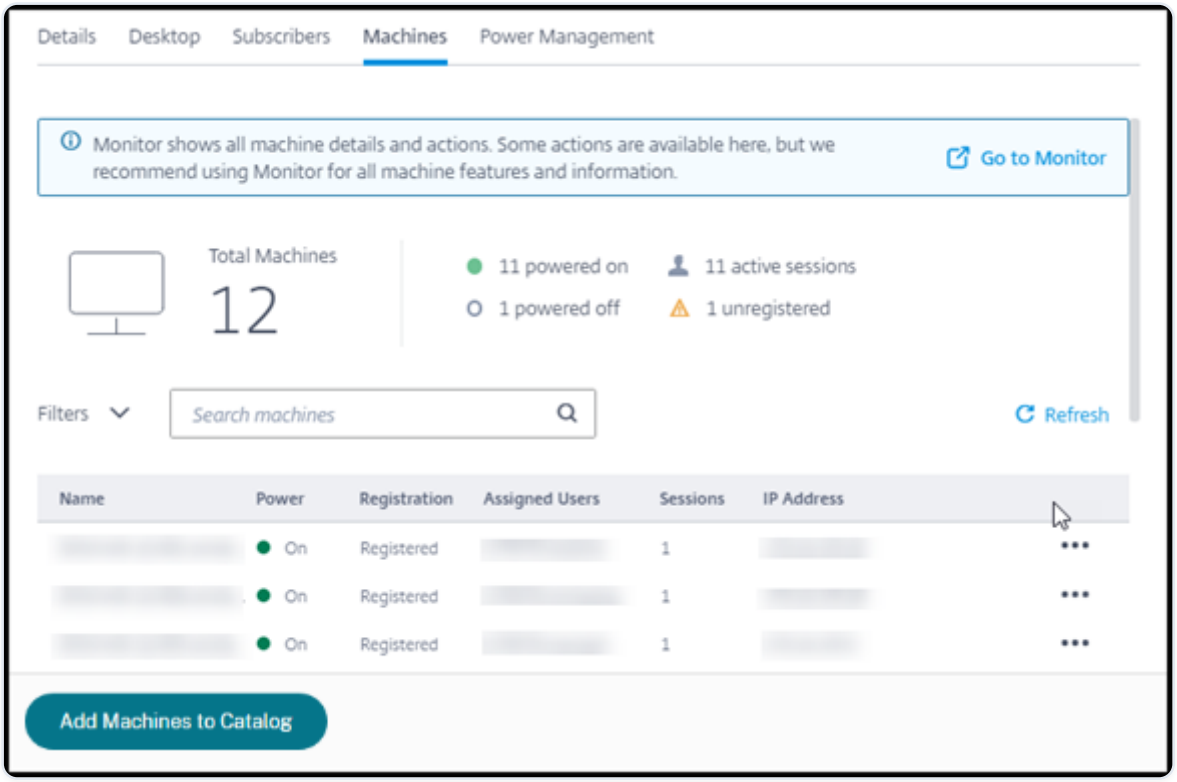
NOTA:

Este artigo descreve as tarefas que você pode usar para gerenciar catálogos criados na interface de Implantação Rápida. Para obter informações sobre o gerenciamento de catálogos usando a interface de gerenciamento do Web Studio, consulte Gerenciar catálogos de máquinas.

Adicionar máquinas a um catálogo

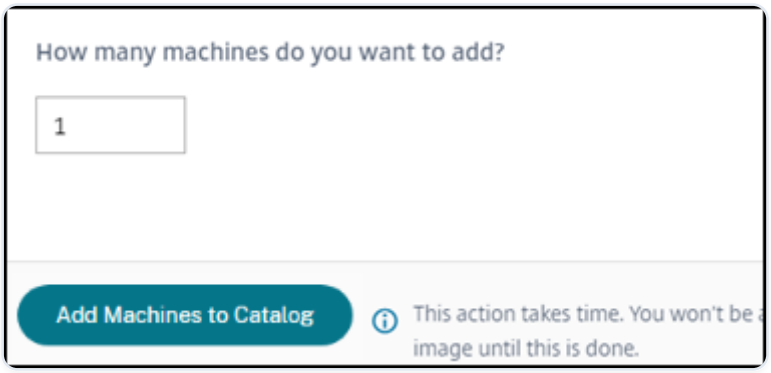
Enquanto as máquinas estão sendo adicionadas a um catálogo, você não pode fazer outras alterações nesse catálogo.

1. No painel **Implantação Rápida > Microsoft 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. (Válido somente se o catálogo estiver associado a um 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 agendamento de gerenciamento de energia para controlar quantas máquinas estão ligadas ou excluir máquinas individuais da guia **Máquinas**. Consulte Gerenciar máquinas em um catálogo para obter informações sobre como excluir máquinas da guia **Máquinas**.

Alterar o número de sessões por máquina

Alterar o número de sessões por máquina multissessão pode afetar a experiência dos usuários. Aumentar esse valor pode reduzir os recursos de computação alocados para sessões simultâneas. Recomendação: Observe seus dados de uso para determinar o equilíbrio apropriado entre a experiência do usuário e o custo.

1. No painel **Quick Deploy > Microsoft Azure**, selecione um catálogo que contenha máquinas multissessão.
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. Ao alterar o número máximo de sessões para um valor inferior às sessões ativas atuais de uma máquina, o novo valor é implementado por meio da redução normal das sessões ativas.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gerenciar máquinas em um catálogo

NOTA:

Muitas das ações disponíveis no painel **Quick Deploy > Microsoft Azure** também estão disponíveis no painel **Monitor** no Citrix DaaS Standard for Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard for Azure).

Para selecionar ações no painel **Quick Deploy > Microsoft Azure**:

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada de um catálogo.
2. Na guia **Máquinas**, localize a máquina que você deseja gerenciar. No menu de reticências dessa máquina, selecione a ação desejada:

   - **Reiniciar:** Reinicia a máquina selecionada.
   - **Iniciar:** Inicia a máquina selecionada. Esta ação está disponível somente se a máquina estiver desligada.
   - **Desligar:** Desliga a máquina selecionada. Esta ação está disponível apenas se a máquina estiver ligada.
   - **Ativar/desativar modo de manutenção:** Ativa o modo de manutenção (se estiver desativado) ou desativa (se estiver ativado) para a máquina selecionada.

     Por padrão, o modo de manutenção é desativado para uma máquina. Ativar o modo de manutenção para uma máquina impede que novas conexões sejam feitas a essa máquina. Os usuários podem se conectar a sessões existentes nessa máquina, mas não podem iniciar novas sessões nela. Você pode colocar uma máquina em modo de manutenção antes de aplicar patches ou para solucionar problemas.
   - **Excluir:** Exclui a máquina selecionada. Esta ação está disponível apenas quando a contagem de sessões da máquina é zero. Confirme a exclusão.

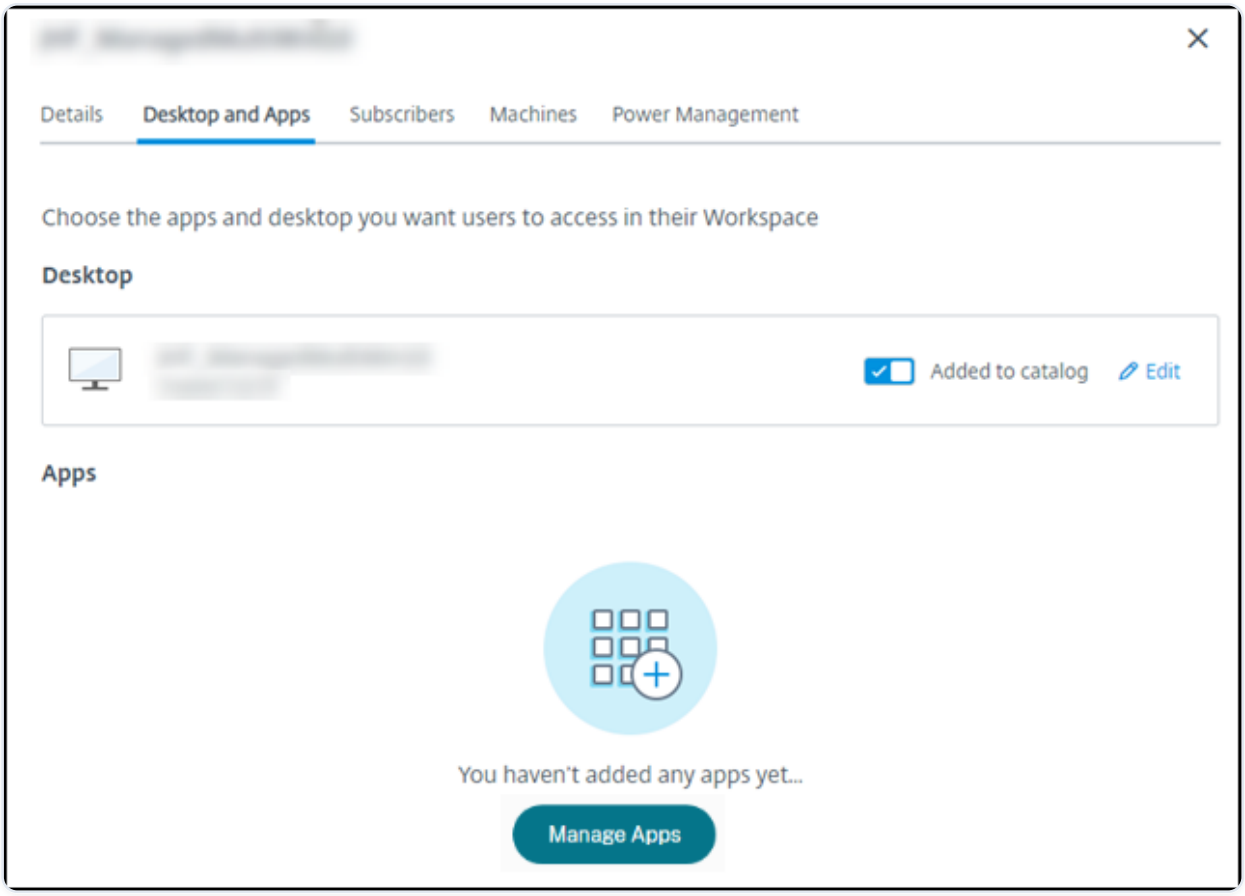
     Quando uma máquina é excluída, todos os dados nela são removidos.
   - **Forçar reinício:** Força a reinicialização da máquina selecionada. Selecione esta ação apenas se uma ação de **Reiniciar** para a máquina falhou.

Adicionar aplicativos a um catálogo

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo.

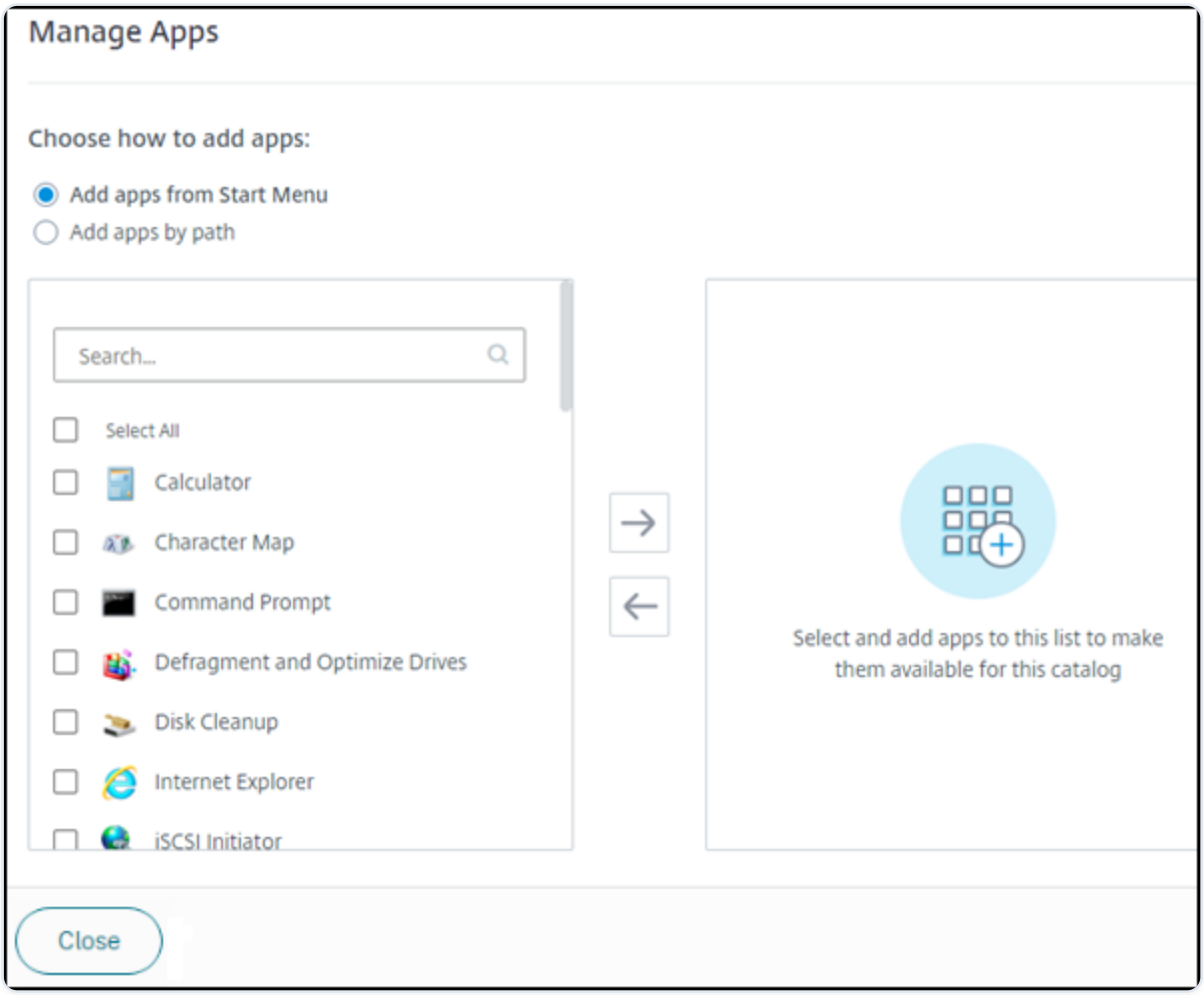
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Na guia **Desktop and Apps**, clique em **Gerenciar Aplicativos**.



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

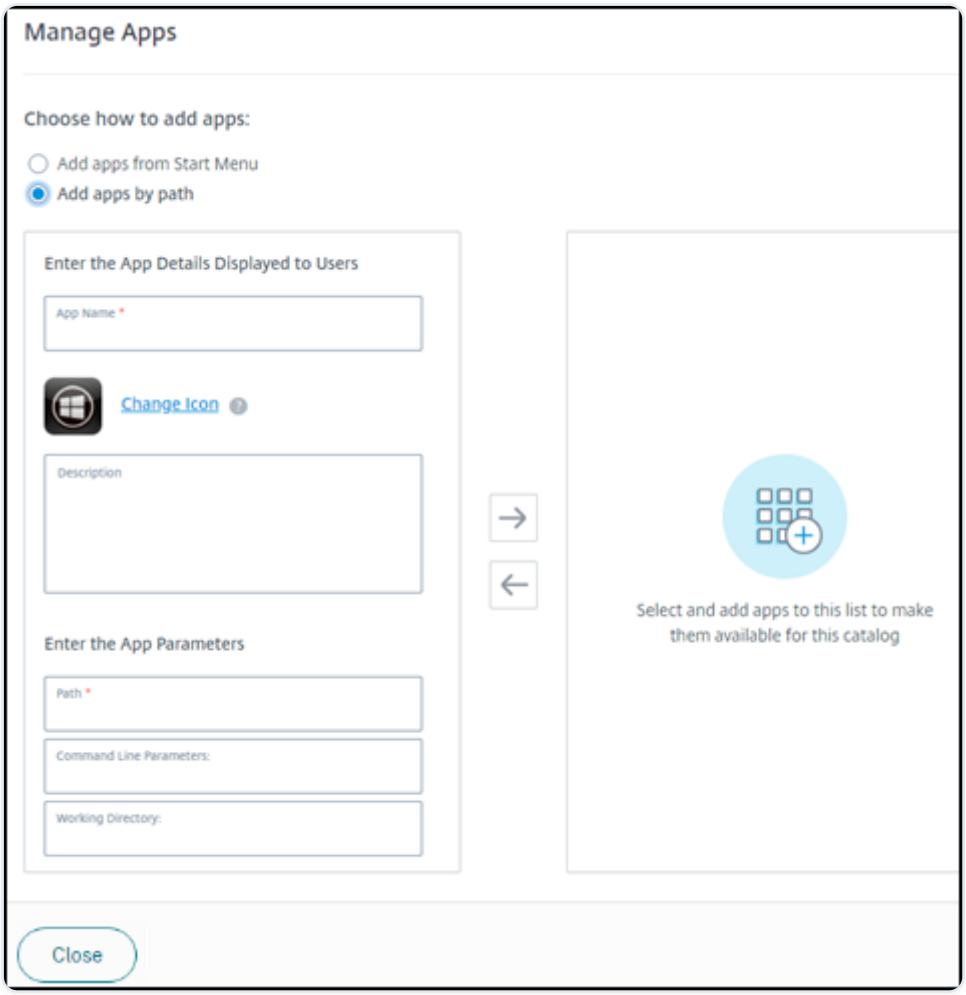
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Selecione os aplicativos disponíveis na coluna esquerda. (Use **Pesquisar** para personalizar a lista de aplicativos.) Clique na seta para a direita entre as colunas. Os aplicativos selecionados são movidos para a coluna direita.
- Da mesma forma, para remover aplicativos, selecione-os na coluna 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 poderá adicionar essa versão do aplicativo.

5. Para adicionar aplicativos por caminho:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Insira o nome do aplicativo. Este 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 em **Alterar ícone** e navegar até o ícone que você deseja exibir.
- (Opcional) Insira uma descrição do aplicativo.
- Insira o caminho para o aplicativo. Este campo é obrigatório. Opcionalmente, adicione parâmetros de linha de comando e o diretório de trabalho. Para obter detalhes sobre parâmetros de linha de comando, consulte Passar parâmetros para aplicativos publicados.

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

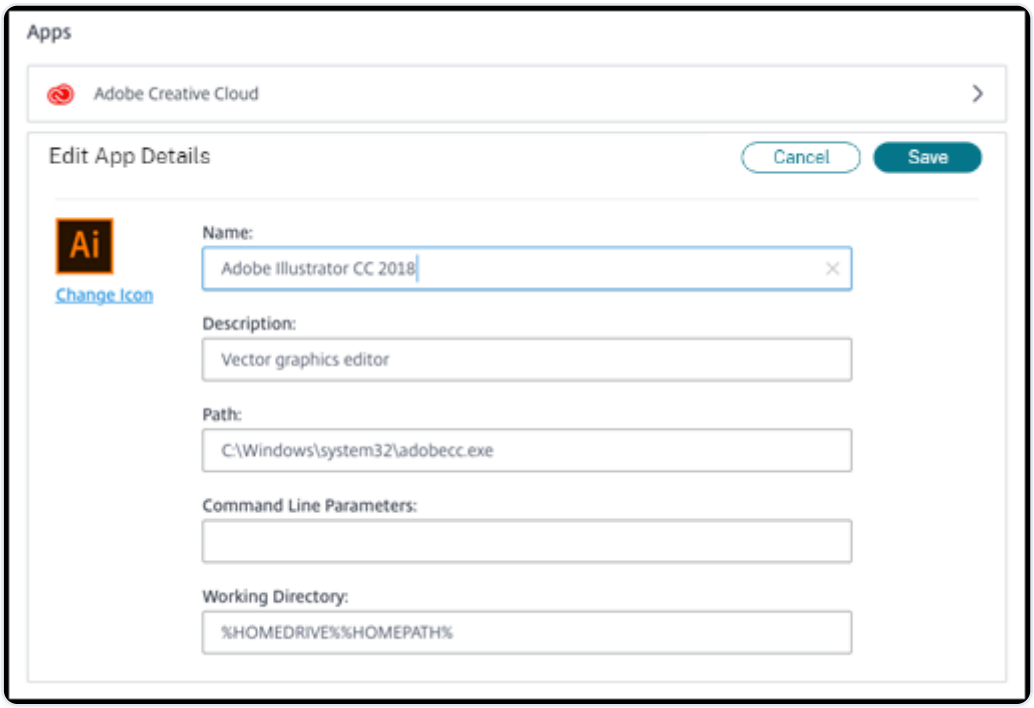
O que fazer a seguir (se você estiver concluindo o fluxo de criação e entrega do catálogo): Envie a URL do Citrix Workspace para seus usuários, se ainda não o fez.

Em VDAs do Windows Server 2019, alguns ícones de aplicativo 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 **Alterar ícone** para atribuir um ícone diferente que seja exibido corretamente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Editar um aplicativo em um catálogo

1. No painel **Quick Deploy > Microsoft 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:
   - **Nome:** O nome que os usuários veem no Citrix Workspace.
   - **Descrição**
   - **Caminho:** O caminho para o executável.
   - **Parâmetros da linha de comando:** 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 em **Alterar ícone** e navegar até o ícone que deseja exibir.
6. Quando terminar, clique em **Salvar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Passar parâmetros para aplicativos publicados

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

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

  Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo 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”), coloque 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 ao redor dos símbolos de porcentagem e asterisco. Adicione um espaço entre as aspas de fechamento do caminho e as aspas de abertura dos 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. Apenas impede que ele apareça no Citrix Workspace.

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, clique no ícone da lixeira ao lado dos aplicativos que você deseja remover.

Excluir um catálogo

Ao excluir um catálogo, todas as máquinas no catálogo são permanentemente destruídas. A exclusão de um catálogo não pode ser revertida.

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Details**, clique em **Delete Catalog** na parte inferior da janela.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Confirme a exclusão selecionando as caixas de seleção de reconhecimento 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 máquinas e de Cloud Connector.

Gerenciar agendamentos de gerenciamento de energia

Um agendamento de gerenciamento de energia afeta todas as máquinas em um catálogo. Um agendamento fornece:

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

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

Você não pode selecionar ou configurar um agendamento de energia ao criar um catálogo com criação rápida. Por padrão, os catálogos de criação rápida usam o agendamento predefinido Economia de Custos. Você pode selecionar ou configurar um agendamento diferente mais tarde para esse catálogo.

O gerenciamento de agendamentos inclui:

- Saber quais informações um agendamento contém
- Criar um agendamento

Informações em um agendamento

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Um agendamento de gerenciamento de energia contém as seguintes informações.

Agendamentos predefinidos

O Citrix DaaS™ para Azure oferece vários agendamentos predefinidos. Você também pode configurar e salvar agendamentos personalizados. Embora você possa excluir predefinições personalizadas, não pode excluir as predefinições fornecidas pela Citrix.

Fuso horário

Usado com a configuração de ligar máquinas para estabelecer o horário de trabalho e o horário pós-expediente, com base no fuso horário selecionado.

Essa configuração é válida para todos os tipos de máquina.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ligar máquinas: Horário de trabalho e horário pós-expediente

Os dias da semana e os horários de início e término do dia que formam seu horário de trabalho. Isso geralmente indica os intervalos em que você deseja que as máquinas estejam ligadas. Qualquer horário fora desses intervalos é considerado pós-expediente. Várias configurações de agendamento permitem que você insira valores separados para o horário de trabalho e o horário pós-expediente. Outras configurações se aplicam o tempo todo.

Esta configuração é válida para todos os tipos de máquina.

Hibernar máquinas: Horário de trabalho e após o expediente

Você pode hibernar máquinas. Enquanto uma máquina está hibernando, você não é cobrado pelo seu uso e economiza no consumo de energia. 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.

Esta configuração está disponível quando todos os seguintes critérios são atendidos:

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

Desligar máquinas quando não houver reconexão

Especifique por quanto tempo uma máquina permanece suspensa antes de ser desligada. Insira um valor maior do que o valor especificado no campo Quando desconectado.

Esta configuração é válida apenas para máquinas aleatórias.

Desconectar sessões de desktop quando ociosas

Por quanto tempo um desktop pode permanecer ocioso (não utilizado) antes que a sessão seja desconectada. Após uma sessão ser desconectada, o usuário deve ir para o Workspace e iniciar um desktop novamente. Esta é uma configuração de segurança.

Esta configuração é válida para todos os tipos de máquina. Uma configuração se aplica o tempo todo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desligar desktops ociosos

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 um desktop novamente. Esta 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. Em seguida, desligue as máquinas se elas permanecerem desconectadas por mais 15 minutos.

Se Tom parar de usar seu desktop e se afastar para uma reunião de uma hora, o desktop será desconectado após 10 minutos. Após mais 15 minutos, a máquina será desligada (25 minutos no total).

Do ponto de vista do usuário, as duas configurações de ociosidade (desconexão e desligamento) têm o mesmo efeito. Se Tom ficar longe de seu desktop por 12 minutos ou uma hora, ele deve iniciar um desktop novamente no Workspace. A diferença nos dois temporizadores afeta o estado da máquina virtual que fornece o desktop.

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

Fazer logoff de sessões desconectadas

Por quanto tempo uma máquina pode permanecer desconectada antes que a sessão seja encerrada.

Esta configuração é válida para máquinas multi-sessão. Uma configuração se aplica o tempo todo.

Atraso de desligamento

A quantidade mínima de tempo que uma máquina deve permanecer ligada antes de ser elegível para desligamento (juntamente com outros critérios). Essa configuração evita que as máquinas fiquem "ligando e desligando" durante demandas de sessão voláteis.

Esta configuração é válida para máquinas multi-sessão e se aplica o tempo todo.

Mínimo de máquinas em execução

Quantas máquinas devem permanecer ligadas, independentemente de quanto tempo estejam ociosas ou desconectadas.

Esta configuração é válida para máquinas aleatórias e multi-sessão. Você pode inserir valores para horário de trabalho e após o expediente.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Buffer de capacidade

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

Um valor mais baixo 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 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 a inicialização.
- 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 está ligada há 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 no ligar ou desligar as máquinas.

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

Criar um agendamento de gerenciamento de energia

1. No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Gerenciamento de Energia**, determine se algum dos agendamentos predefinidos (no menu 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, horários ou intervalos), a seleção predefinida mudará para **Personalizado** automaticamente. Um asterisco indica que as configurações personalizadas não foram salvas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Defina os valores desejados para o agendamento personalizado.
5. Clique em **Personalizado** na parte superior e salve as configurações atuais como uma nova predefinição. Insira um nome para a nova predefinição e clique na marca de seleção.
6. Quando terminar, clique em **Salvar Alterações**.

Mais tarde, 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 de VDA

Os recursos de instantâneo e restauração do Citrix DaaS para 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. Mais tarde, uma operação de restauração usa um instantâneo que você seleciona.

- Você pode configurar agendamentos de instantâneos diários 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 máquina única.)

IMPORTANTE:

Os recursos de instantâneo e restauração do Citrix DaaS para Azure são suportados apenas para máquinas em catálogos estáticos e atribuídas a usuários.

Agendamentos de instantâneos

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

Por padrão, não há agendamentos de instantâneos.

Para gerenciar agendamentos de instantâneos:

1. No painel **Gerenciar**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Detalhes**, clique em **Agendar Instantâneos**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Na página **Agendar Snapshots**, configure agendamentos para snapshots automáticos semanais ou diários, ou ambos:

    - Para adicionar ou alterar snapshots semanais, mova o controle deslizante para **Snapshots automáticos semanais** até que uma marca de seleção apareça. Selecione o dia da semana e a hora de início.
    - Para adicionar ou alterar snapshots diários, mova o controle deslizante para **Snapshots automáticos diários** até que uma marca de seleção apareça. Selecione a hora de início.
    - Para remover snapshots semanais, mova o controle deslizante para **Snapshots automáticos semanais** até que um **X** apareça.
    - Para remover snapshots diários, mova o controle deslizante para **Snapshots automáticos diários** até que um **X** apareça.

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

Snapshots manuais

Um snapshot manual é para uma única máquina em um catálogo. (Não é possível criar um agendamento para tirar um snapshot 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 snapshot. Selecione **Snapshots** no menu de reticências para essa máquina.
3. Na página **Snapshots para *nome-VDA***, clique em **Criar Snapshot Manual**.
4. Forneça um nome para o snapshot. Recomendado: Escolha um nome que você possa identificar facilmente mais tarde.
5. Confirme sua solicitação.

Visualizar e gerenciar snapshots

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 para essa máquina.
3. Na página **Backups para *nome-VDA***:

    - Se não houver instantâneos para a máquina, uma mensagem o orienta a criar um instantâneo manual para esta máquina ou a criar instantâneos agendados para todas as máquinas no catálogo que contém esta máquina.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Você pode selecionar um dos instantâneos e restaurar a máquina. Consulte Restaurar.
- Você pode excluir instantâneos. Selecione as caixas de seleção para um ou mais instantâneos e, em seguida, clique em **Excluir** no cabeçalho da tabela. Confirme sua solicitação.

Dica: Ao excluir 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 para essa máquina.
3. Na página **Instantâneos para *nome-VDA***, selecione 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 falhar ao restaurar um instantâneo, tente novamente.

Informações relacionadas

- Atualizar um catálogo com uma nova imagem
- Adicionar e remover usuários em um catálogo
- Associado ao domínio e não associado ao domínio

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoramento

No painel **Monitor**, você pode visualizar o uso da área de trabalho, sessões e máquinas em sua implantação do Citrix DaaS Standard for Azure (anteriormente Citrix Virtual Apps and Desktops Standard for Azure). Você também pode controlar sessões, gerenciar o consumo de energia das máquinas, 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 **Soluções > DaaS Standard for Azure**.
2. Clique na guia **Monitor**.

Monitorar o uso da área de trabalho

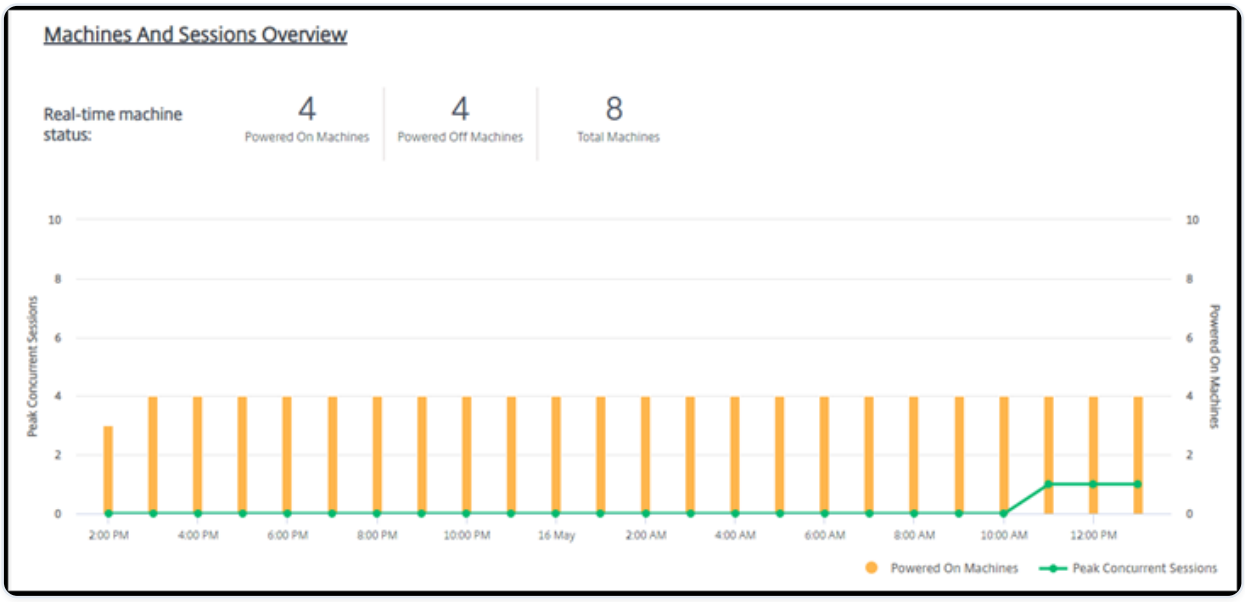
As exibições nesta página são atualizadas a cada cinco minutos.

- **Visão geral de máquinas e 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 da exibição 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 multissessão.

  O gráfico abaixo das contagens mostra o número de máquinas ligadas e o pico de sessões simultâneas em pontos regulares durante o período selecionado. Passe o mouse sobre um ponto no gráfico para exibir as contagens naquele ponto.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Os 10 principais:** Para personalizar uma exibição dos 10 principais, selecione um período: a última semana (padrão), mês ou três meses. Você também pode personalizar a exibição para mostrar apenas informações sobre atividades envolvendo máquinas de sessão única, máquinas multissessão ou aplicativos.
    - **Os 10 principais usuários ativos:** Lista os usuários que iniciaram áreas de trabalho com mais frequência durante o período. Passar o mouse sobre uma linha exibe o total de inicializações.
    - **Os 10 principais catálogos ativos:** Lista os catálogos com a maior duração durante o período selecionado. A duração é a soma de todas as sessões de usuário desse catálogo.

Relatório de uso da área de trabalho

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

Filtrar e pesquisar para monitorar máquinas e sessões

Ao monitorar informações de sessão e máquina, todas as máquinas ou sessões são exibidas por padrão. Você pode:

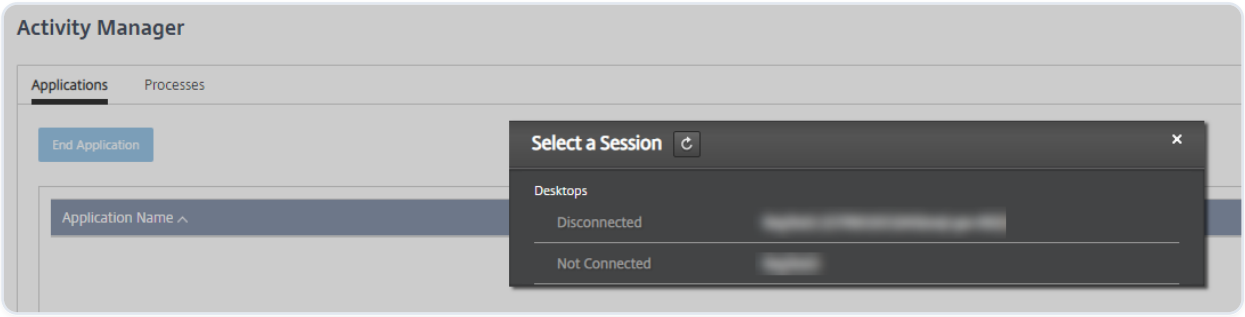
- Filtrar a exibição por máquinas, sessões, conexões ou aplicativos.
- Refinar a exibição de sessões ou máquinas escolhendo os critérios desejados, construindo um filtro usando expressões.
- Salvar os filtros que você constrói, para reutilização.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Controlar os aplicativos de um usuário

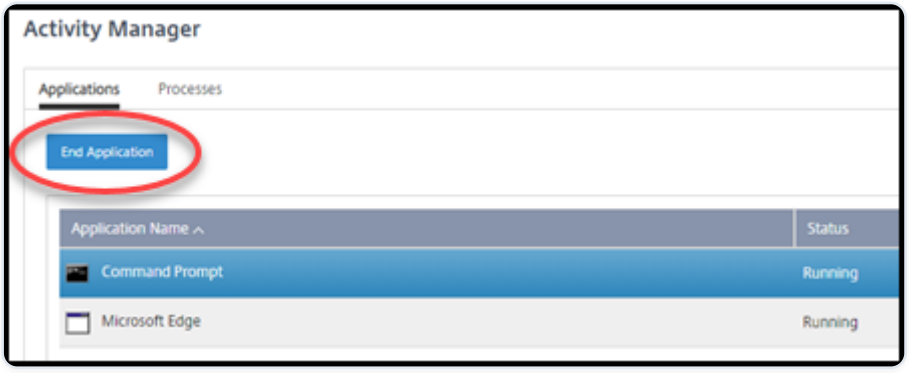
Você pode exibir e gerenciar aplicativos e processos para um usuário que tenha uma sessão em execução ou uma área de trabalho atribuída.

1. No painel **Monitor**, clique em **Pesquisar** e insira o nome de usuário (ou os caracteres iniciais do nome de usuário), máquina ou endpoint. 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 Gerenciador de Atividades lista os aplicativos e processos para a sessão do usuário.

3. Para encerrar um aplicativo, na guia **Aplicativos** no Gerenciador de Atividades, clique na linha do aplicativo para selecioná-lo e, em seguida, clique em **Encerrar Aplicativo**.



4. Para encerrar um processo, na guia **Processos** no Gerenciador de Atividades, clique na linha do processo para selecioná-lo e, em seguida, clique em **Encerrar 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Espelhar usuários

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

O espelhamento é iniciado em uma nova guia do navegador. Certifique-se de que seu navegador permita pop-ups da URL do Citrix Cloud™.

Em uma assinatura do Azure gerenciada pela Citrix, o espelhamento é suportado apenas para catálogos que usam uma conexão de rede. O espelhamento de um catálogo sem conectividade não é suportado.

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

Habilitar espelhamento

1. No painel do **Monitor**, vá para a exibição **Detalhes do Usuário**.
2. Selecione a sessão do usuário e, em seguida, clique em **Espelhar** na exibição **Gerenciador de Atividades** ou no painel **Detalhes da Sessão**.

Espelhar VDAs Linux

O espelhamento está disponível para VDAs Linux Versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu Versão 16.04.

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

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

Siga as instruções em Espelhamento de Sessão para configurar seu VDA Linux para espelhamento.

1. Depois de habilitar o espelhamento, a conexão de espelhamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou da sessão.
3. O administrador pode visualizar apenas a sessão espelhada.

Espelhar VDAs Windows

As sessões de VDA Windows são espelhadas usando o Assistência Remota do Windows. Habilite o recurso `Use Windows Remote Assistance` ao instalar o VDA.

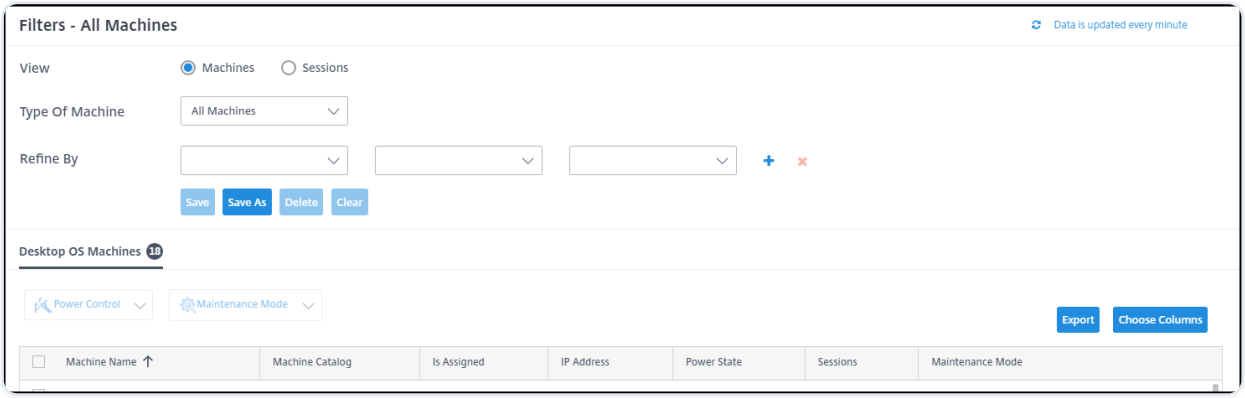
1. Depois de habilitar o espelhamento, a conexão de espelhamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo `.msrc incident`.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ele já não estiver selecionado por padrão. Um prompt de confirmação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

Monitorar e controlar sessões

As exibições da sessão são atualizadas a cada minuto.

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

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

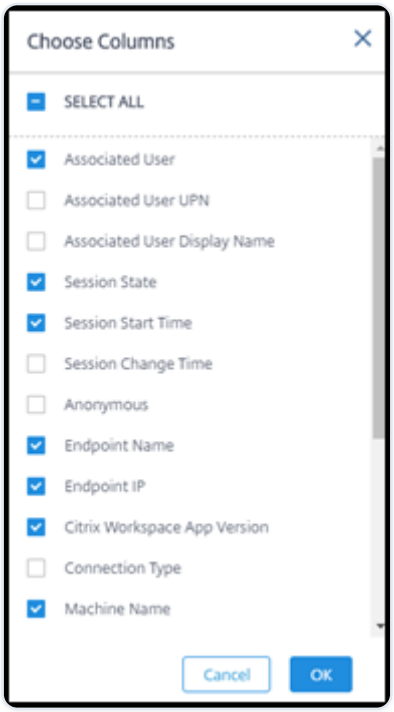


2. Selecione a exibição **Sessões**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Para personalizar a exibição, clique em **Escolher Colunas** e selecione as caixas de seleção dos itens que você deseja que apareçam. Quando terminar, clique em **OK**. A exibição de 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, escolha **Controle de Sessão > Logoff** ou **Controle de Sessão > Desconectar**.

Lembre-se de que o agendamento 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. As opções de logoff e desconexão também estão disponíveis lá.

Relatório de informações da sessão

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

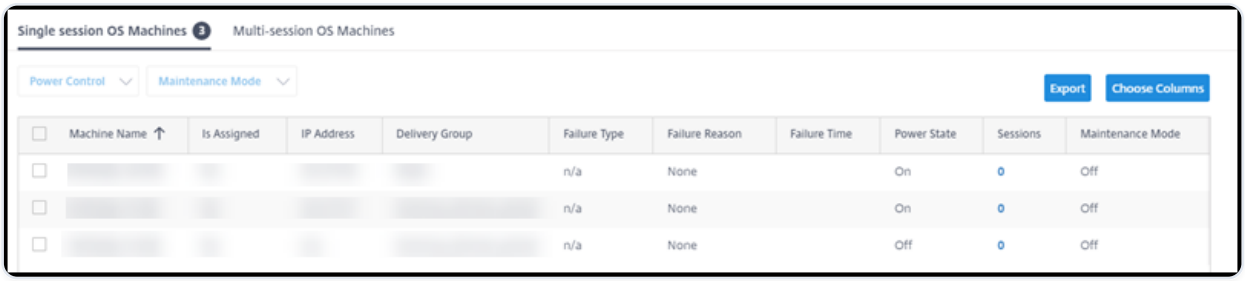
Monitorar e controlar a energia das máquinas

As exibições da máquina são atualizadas a cada minuto.

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

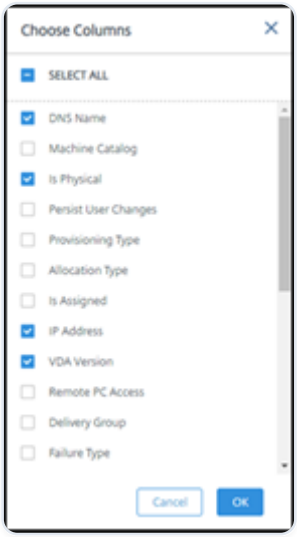
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Selecione a exibição **Máquinas**.

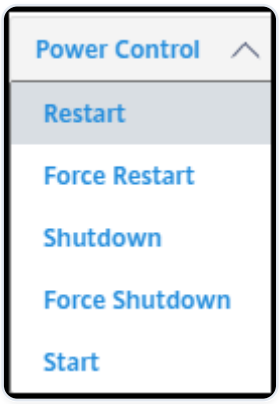


Por padrão, a exibição lista máquinas de SO de sessão única. Alternativamente, você pode exibir máquinas de várias sessões.

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



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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Para colocar as máquinas selecionadas em modo de manutenção ou retirá-las, clique em **Modo de Manutenção > LIGADO** ou **Modo de Manutenção > DESLIGADO**.

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

Relatório de informações da máquina

Para baixar informações da sessão, clique em **Exportar** na exibição 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.

Verificando a integridade de aplicativos e desktops

A sondagem automatiza o processo de verificação da integridade de aplicativos e desktops publicados. Os resultados da verificação de integridade estão disponíveis através do painel **Monitor**. Para obter detalhes, consulte:

- Sondagem de aplicativos
- Sondagem de desktops

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix DaaS™ para Azure para Provedores de Serviços Citrix

Este artigo descreve como os Provedores de Serviços Citrix (CSPs) podem configurar o Citrix DaaS Standard para Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard para Azure) para clientes (locatários) no Citrix Cloud.

Para uma visão geral dos recursos disponíveis para Parceiros Citrix, consulte Citrix Cloud para Parceiros.

Requisitos

- Você é um parceiro Provedor de Serviços Citrix.
- Você tem uma conta Citrix Cloud™.
- Você tem uma assinatura do Citrix DaaS para Azure.

Limitações

- As alterações de nome de 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 um usuário de cliente é atribuído a um recurso, você não pode removê-lo ou desatribuí-lo.
- O console de gerenciamento não impõe a separação de usuários por cliente. Você é responsável por adicionar usuários aos catálogos e recursos apropriados.

Adicionar um cliente

1. Faça login no Citrix Cloud com suas credenciais de CSP. Clique em **Clientes** no menu superior esquerdo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. No painel **Customer**, clique em **Invite or Add**. Forneça as informações solicitadas.

   Se o cliente não tiver uma conta Citrix Cloud, adicionar o cliente criará uma conta de cliente. Adicionar o cliente também o adiciona automaticamente como administrador de acesso total da conta desse cliente.

3. Se o cliente tiver uma conta Citrix Cloud:

   a. Uma URL do Citrix Cloud é exibida, que você copia e envia ao cliente. Para obter detalhes sobre esse processo, consulte Convidar um cliente para se conectar.

   b. O cliente deve adicioná-lo como administrador de acesso total à sua conta. Consulte Adicionar administradores a uma conta Citrix Cloud.

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

Adicionar Citrix DaaS for Azure a um cliente

1. Faça login no Citrix Cloud com suas credenciais de CSP. Clique em **Customers** no menu superior esquerdo.
2. No painel **Customer**, selecione **Add Service** no menu de reticências para o cliente.
3. Em **Select a Service to Add**, clique em **Citrix DaaS Standard for Azure**.
4. Clique em **Continue**.

Após concluir este procedimento, o cliente é integrado à sua assinatura do Citrix DaaS for Azure.

Quando a integração for concluída, um novo cliente será criado automaticamente no Citrix DaaS for Azure. O cliente fica visível em **Quick Deploy > Microsoft Azure**.

Filtrar recursos por cliente

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Criar catálogos para entregar aplicativos e desktops

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

Domínios federados

Domínios federados permitem que os usuários do cliente usem credenciais de um domínio anexado ao seu local de recurso para fazer login em seu workspace. Você pode fornecer workspaces dedicados aos seus clientes que seus usuários podem acessar por meio de uma URL de workspace personalizada (por exemplo, `customer.cloud.com`), enquanto o local de recurso permanece em sua conta do Citrix Cloud.

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

Após configurar o workspace por meio de Configuração do Workspace, os usuários dos clientes podem fazer login em seu workspace e acessar os aplicativos e desktops que você disponibilizou.

Adicionar um cliente a um domínio

1. Faça login no Citrix Cloud com suas credenciais CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel **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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remover um cliente de um domínio

Ao remover um cliente de um domínio que você gerencia, os usuários do cliente não podem mais acessar seus workspaces usando 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 para o 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 todos**.

   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 de CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel **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 **Acesso personalizado**, 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 para Azure, conforme necessário.
7. Quando terminar, clique em **Enviar Convite**.

Quando o administrador aceita o convite, ele tem o acesso que você atribuiu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Acesso do parceiro ao provedor de identidade do cliente

Você pode gerenciar usuários no painel **Quick Deploy > Microsoft Azure** do Citrix DaaS for Azure ou no console do Citrix Cloud.

Ao usar um provedor de identidade não-AD para usuários (como o Citrix Managed Microsoft Entra ID), você deve ser um administrador de Identidade e Espaço de Trabalho do Citrix Cloud para o cliente antes de poder gerenciar usuários para esse cliente. Se você não for um administrador para um cliente, não poderá adicionar ou excluir usuários para esse cliente.

Para gerenciar usuários para um cliente no painel **Quick Deploy > Microsoft 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. Ao selecionar um catálogo, você 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 para esse cliente).
- **Exemplo 2:** Você seleciona a entrada do parceiro em **Mostrar itens para**. O painel agora mostra apenas os itens do parceiro. Na guia **Assinantes**, você vê apenas os usuários criados para o parceiro. Nenhuma entrada de cliente aparece. Você pode adicionar ou remover usuários para esse parceiro (supondo que você seja um administrador desse parceiro), mas não pode gerenciar nenhum usuário de cliente a partir deste local.

Para gerenciar usuários para um cliente no console do Citrix Cloud, selecione o cliente quando solicitado após o login (ou mais tarde, usando **Alterar Cliente** 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 de CSP. Clique em **Clientes** no menu superior esquerdo.
2. No painel **Cliente**, selecione **Gerenciamento de Identidade e Acesso** no menu superior esquerdo.
3. Na guia **Administradores**, selecione **Editar Acesso** no menu de reticências para o administrador.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Selecione ou desmarque os pares de função e escopo para o Citrix DaaS for Azure, conforme necessário. Certifique-se de habilitar apenas as entradas que contêm o escopo exclusivo que foi criado para o cliente.
5. Clique em **Salvar**.

Acessar e configurar espaços de trabalho

Cada cliente obtém seu próprio workspace com uma URL `customer.cloud.com` exclusiva. Esta URL é onde os usuários do cliente acessam seus aplicativos e desktops publicados.

- **Do Citrix DaaS Standard para Azure:** No painel **Quick Deploy > Microsoft Azure**, visualize a URL expandindo **User Access & Authentication** à direita.
- **Do Citrix Cloud:** No painel **Customer**, selecione **Workspace Configuration** no menu superior esquerdo. Visualize a URL na guia **Access**.

Você pode alterar o acesso e a autenticação a um workspace. Você também pode personalizar a aparência e as preferências do workspace. Para obter detalhes, consulte os seguintes artigos:

- Configurar workspaces
- Proteger workspaces

Monitorar o serviço de um cliente

O painel **Monitor** do Citrix DaaS para Azure em um ambiente CSP é essencialmente o mesmo que em 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**.

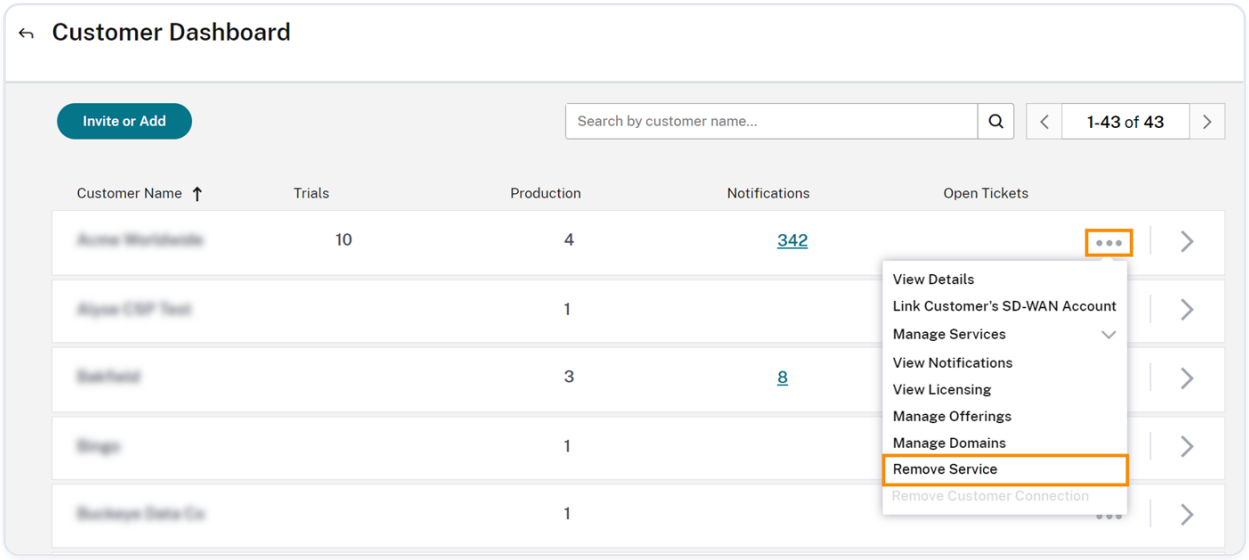
Lembre-se de que a capacidade de ver as exibições do **Monitor** para um cliente é controlada pelo acesso configurado do administrador.

Remover um Serviço

Antes de começar, certifique-se de que o escopo do seu cliente não esteja vinculado a nenhum objeto do Citrix DaaS Standard para Azure. Se estiverem vinculados, você não poderá 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 escopo.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Faça login no Citrix Cloud com suas credenciais de Citrix Service Providers.
2. No painel **Customer**, clique no menu de reticências (**...**) do cliente de onde você deseja remover um serviço e selecione **Remove Service**.



A página **Serviço a Remover** é exibida.

3. Clique em **Remover** para remover o serviço.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solução de problemas

Introdução

Os locais de recursos contêm as máquinas que fornecem desktops 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 de recursos. A Citrix instala e atualiza os Cloud Connectors.

Opcionalmente, você pode iniciar várias ações de Cloud Connector e de local de recursos. Consulte:

- Ações de local de recursos
- Configurações de local de recursos ao criar um catálogo

O Citrix DaaS™ para Azure possui 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 seus desktops ou aplicativos.

Esta solução de problemas inclui obter acesso à sua assinatura do Azure gerenciada pela Citrix 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 via Bastion
- Acesso RDP direto

Solução de problemas de VDA usando um bastion ou RDP direto

Os recursos de suporte são para pessoas que têm experiência em solucionar problemas da Citrix. Isso inclui:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Provedores de Serviços Citrix (CSPs) e outros que possuem conhecimento técnico e experiência em solução de problemas com produtos Citrix DaaS.
- Pessoal de Suporte da Citrix.

Se você não está familiarizado ou confortável com a solução de problemas de componentes Citrix, você pode solicitar ajuda do Suporte Citrix. Os representantes do Suporte Citrix podem pedir para você configurar um dos métodos de acesso descritos nesta seção. No entanto, os representantes Citrix fazem a solução de problemas real, usando ferramentas e tecnologias Citrix.

IMPORTANTE:

Esses recursos de suporte são válidos apenas para máquinas ingressadas no domínio. Se as máquinas em seus catálogos não estiverem ingressadas no domínio, você será orientado a solicitar ajuda para solução de problemas do Suporte Citrix.

Métodos de acesso

Esses métodos de acesso são válidos apenas para a assinatura Citrix Managed Azure. Para obter mais informações, consulte Assinaturas do Azure.

Dois métodos de acesso para suporte são fornecidos.

- Acesse seus recursos por meio de uma máquina bastion na assinatura Citrix Managed Azure dedicada do cliente. O bastion é um único ponto de entrada que permite o acesso às máquinas na assinatura. Ele fornece uma conexão segura a esses recursos, permitindo o tráfego remoto de endereços IP em um intervalo especificado.

  As etapas neste método incluem:

  - Criar a máquina bastion
  - Baixar um agente RDP
  - RDP para a máquina bastion
  - Conectar da máquina bastion às outras máquinas Citrix em sua assinatura

  A máquina bastion destina-se a uso de curto prazo. Este método é destinado a problemas que envolvem a criação de catálogos ou máquinas de imagem.
- Acesso RDP direto às máquinas na assinatura Citrix Managed Azure dedicada do cliente. Para permitir o tráfego RDP, a porta 3389 deve ser definida no Grupo de Segurança de Rede.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Este método é destinado a problemas de catálogo que não sejam de criação, como usuários incapazes de iniciar seus desktops.

Lembre-se: Como alternativa a esses dois métodos de acesso, entre em contato com o Suporte Citrix para obter ajuda.

Acesso Bastion

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Troubleshoot & Support** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione um dos dois primeiros tipos de problema e, em seguida, 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 você quiser restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, selecione a caixa de seleção **Restrict RDP access to only computers in IP address range** e, em seguida, insira o intervalo desejado.
6. Digite um nome de usuário e uma senha que você usará para fazer login ao acessar a máquina bastion via RDP. Requisitos de senha.

   Não use caracteres Unicode no nome de usuário.
7. Clique em **Create Bastion Machine**.

   Quando a máquina bastion for criada com sucesso, o título da página mudará para **Bastion – *connection***.

   Se a criação da máquina bastion falhar (ou se falhar durante a operação), clique em **Delete** na parte inferior da página de notificação de falha. Tente criar a máquina bastion novamente.

   Você pode alterar a restrição de intervalo RDP depois que a máquina bastion for criada. Clique em **Edit**. Insira o novo valor e, em seguida, clique na marca de seleção para salvar a alteração. (Clique em **X** para cancelar a alteração.)
8. Clique em **Baixar Arquivo RDP**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Conecte-se via RDP ao bastion, usando as credenciais que você especificou ao criar o bastion. (O endereço da máquina bastion está incorporado no arquivo RDP que você baixou.)
10. Conecte-se da máquina bastion às outras máquinas Citrix na assinatura. Você pode então 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 ou excluir uma máquina bastion, usando os botões na parte inferior da página. Se você optar por excluir uma máquina bastion, deverá reconhecer que todas as sessões ativas na máquina serão encerradas automaticamente. Além disso, quaisquer dados e arquivos que foram salvos na máquina serão excluídos.

Acesso RDP direto

1. No painel **Quick Deploy > Microsoft Azure** no Citrix DaaS para Azure, expanda **Troubleshoot & Support** à direita.
2. Clique em **Exibir opções de solução de problemas**.
3. Na página **Troubleshoot**, selecione **Outro problema de catálogo**.
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 você quiser restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, selecione a caixa de seleção **Restringir acesso RDP apenas a computadores no intervalo de endereços IP** e então insira o intervalo desejado.
6. Clique em **Habilitar Acesso RDP.**

   Quando o acesso RDP é habilitado com sucesso, o título da página muda para **RDP Access – *connection***.

   Se o acesso RDP não for habilitado com sucesso, clique em **Tentar Habilitar RDP Novamente** na parte inferior da página de notificação de falha.
7. Conecte-se às máquinas usando suas credenciais de administrador do Active Directory. Você pode então coletar logs e executar diagnósticos.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Obter ajuda

Se você ainda tiver problemas, abra um tíquete seguindo as instruções em Como Obter Ajuda e Suporte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Limites

Este artigo lista os limites para recursos em uma implantação do Citrix DaaS Standard for Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard for Azure).

NOTA:

Os limites são recomendados pela Citrix®.

Limites de configuração

RECURSO	LIMITE
Domínios do Active Directory	25
Catálogos	100
Locais de recursos	25
VDAs por assinatura	5.000

Limites de localização de recursos

A tabela a seguir lista os limites para cada localização de recurso. Se seus requisitos excederem esses limites, a Citrix recomenda usar mais localizações de recursos.

RECURSO	LIMITE
Domínios do Active Directory	1
VDAs de sessão única	10.000
VDAs de múltiplas sessões	1.000

Os Citrix Cloud Connectors são atribuídos a localizações de recursos e vinculam cargas de trabalho ao Citrix DaaS para Azure. Para obter informações sobre os limites do Cloud Connector e

© 1997–2026 Citrix Systems, Inc. All rights reserved.

recomendações de tamanho e escala, consulte Considerações de tamanho e escala para Cloud Connectors.

Limites de provisionamento

A tabela a seguir lista os máximos recomendados para uma única conta do Citrix Cloud™.

Para implantações em larga escala, a Citrix recomenda um modelo hub-and-spoke, onde os VDAs são distribuídos por várias assinaturas e conexões de rede.

RECURSO	LIMITE
VDAs multi-sessão por catálogo	500
VDAs de sessão única por catálogo	1.200
VDAs por assinatura do Microsoft Azure	5.000

Limites de uso

RECURSO	LIMITE
Administradores completos do Monitor simultâneos	5
Usuários finais simultâneos	100.000
Recursos publicados para um único usuário	250
Lançamentos de sessão por minuto	3.000

Limites de avaliação

A tabela a seguir lista os limites durante uma avaliação do Citrix DaaS™ para Azure.

ASSINATURA DO AZURE	RECURSO	LIMITE
Assinatura do Azure gerenciada pela Citrix	Número máximo de catálogos	3
	Número máximo de usuários	25

© 1997–2026 Citrix Systems, Inc. All rights reserved.

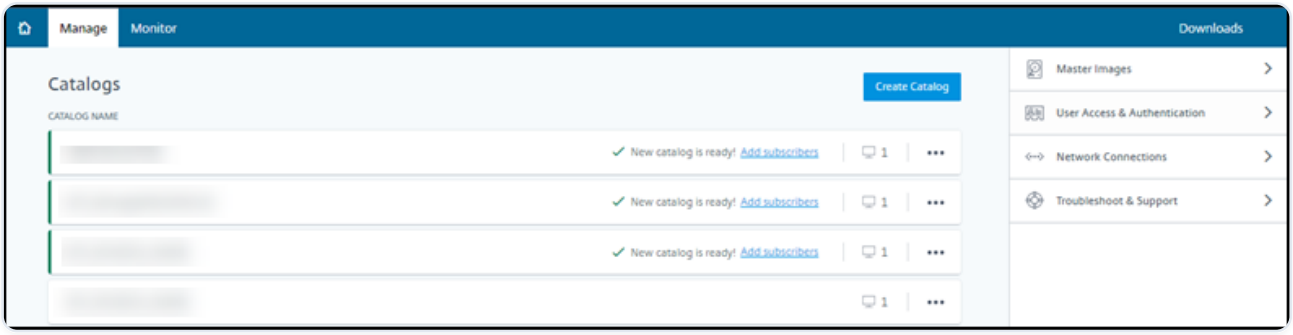
ASSINATURA DO AZURE	RECURSO	LIMITE
	Número máximo de VDAs por catálogo	3
Assinatura do Azure gerenciada pelo cliente	Número máximo de catálogos	10
	Número máximo de usuários	25
	Número máximo de VDAs por catálogo	10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Referência

Painéis

A maioria das atividades do administrador para o Citrix DaaS Standard for Azure (anteriormente serviço Citrix Virtual Apps and Desktops Standard for Azure) pode ser acessada pelos painéis **Gerenciar** e **Monitorar**.



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 **Soluções > DaaS Standard for Azure**. (Como alternativa, você pode clicar em **DaaS Standard for Azure** ou no bloco **Monitorar** na área principal da tela.)
3. navegar para **Quick Deploy > Microsoft Azure** para acessar o painel **Gerenciar**.
4. Para acessar o painel **Monitorar**, clique na guia **Monitorar**.

Para obter orientação no produto a partir do painel, clique no ícone no canto inferior direito.



Guias de catálogo no painel Gerenciar

No painel **Quick Deploy > Microsoft Azure**, clique em qualquer lugar na entrada do catálogo. As seguintes guias contêm informações sobre o catálogo:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Detalhes:** Lista as informações especificadas quando o catálogo foi criado (ou sua edição mais recente). Ele também contém informações sobre a imagem que foi usada para criar o catálogo.

  Nesta 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.

- **Área de trabalho:** Disponível apenas para catálogos que contêm máquinas de sessão única (estáticas ou aleatórias). Nesta guia, você pode alterar o nome e a descrição do catálogo.
- **Área de trabalho e aplicativos:** A guia **Áreas de trabalho e aplicativos** está disponível apenas para catálogos que contêm máquinas multissessão. Nesta guia, você pode:

  - Adicionar, editar ou remover aplicativos que os usuários do catálogo podem acessar no Citrix Workspace.
  - Alterar o nome e a descrição do catálogo.

- **Assinantes:** Lista todos os usuários, incluindo seu tipo (usuário ou grupo), nome da conta, nome de exibição, além do domínio do Active Directory e nome principal de usuário.

  Nesta guia, você pode adicionar ou remover usuários para um catálogo.

- **Máquinas:** Mostra o número total de máquinas no catálogo, além do número de máquinas registradas, máquinas não registradas e máquinas com o modo de manutenção ativado.

  Para cada máquina no catálogo, a exibição inclui o nome de cada máquina, estado de energia (ligada/desligada), estado de registro (registrada/não registrada), usuários atribuídos, contagem de sessões (0/1) e status do modo de manutenção (um ícone indicando ligado ou desligado).

  Nesta guia, você pode:

  - Adicionar ou excluir uma máquina
  - Iniciar, reiniciar, forçar reinício 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 a energia das máquinas.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Gerenciamento de energia:** Permite gerenciar quando as máquinas no catálogo são ligadas e desligadas. Um agendamento também indica quando as máquinas ociosas são desconectadas.

  Você pode configurar um agendamento de energia ao criar um catálogo personalizado ou posteriormente. Se nenhum agendamento for definido explicitamente, uma máquina será desligada quando uma sessão terminar.

  Ao criar um catálogo usando a criação rápida, você não pode selecionar ou configurar um agendamento de energia. Por padrão, os catálogos de criação rápida usam o agendamento predefinido Economia de Custos. No entanto, você pode editar esse catálogo posteriormente e alterar o agendamento.

  Para obter detalhes, consulte Gerenciar agendamentos 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 apenas máquinas não ingressadas no domínio.

1. Antes de criar um catálogo ingressado no domínio (ou uma conexão, se você estiver usando uma assinatura Citrix Managed Azure), verifique se você tem entradas de servidor DNS que podem resolver nomes de domínio públicos e privados.

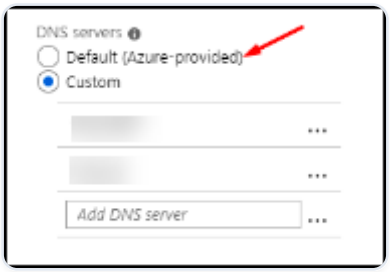
   Quando o Citrix DaaS™ para Azure cria um catálogo ou uma conexão, ele procura por pelo menos uma entrada de servidor DNS válida. Se nenhuma entrada válida for encontrada, a operação de criação falhará.

   Onde verificar:

   - Se você estiver usando sua própria assinatura do Azure, verifique a entrada **Servidores DNS** no seu Azure.
   - Se você estiver usando uma assinatura Citrix Managed Azure e criando uma conexão de emparelhamento de VNet do Azure, verifique a entrada **Servidores DNS** na VNet do Azure que você está emparelhando.

2. No Azure, a configuração **Personalizado** deve ter pelo menos uma entrada válida. O Citrix DaaS para Azure não pode ser usado com a configuração **Padrão (fornecido pelo Azure)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 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 você deseja usar com o Citrix DaaS para Azure podem resolver nomes IP de domínio públicos e privados.
- 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 essas capacidades.

3. Se você alterar alguma entrada de servidor DNS, reinicie todas as máquinas conectadas à rede virtual. A reinicialização atribui as novas configurações do servidor DNS. (As VMs continuam usando suas configurações DNS atuais até a reinicialização.)

Se você quiser alterar os endereços DNS mais tarde, depois que uma conexão for criada:

- Ao usar sua própria assinatura do Azure, você pode alterá-los no Azure (conforme descrito nas etapas anteriores). Ou, você pode alterá-los no Citrix DaaS para Azure.
- Ao usar uma assinatura do Azure gerenciada pela Citrix, o Citrix DaaS para 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 a alteração dos endereços do servidor DNS pode potencialmente causar problemas de conectividade para máquinas em catálogos que usam essa conexão.

Adicionando servidores DNS através do Citrix DaaS para Azure

Antes de adicionar um endereço de servidor DNS a uma conexão, certifique-se de que o servidor DNS possa 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 para uma conexão existente:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. No painel **Quick Deploy > Microsoft Azure**, expanda **Conexões de Rede** à direita.

b. Selecione a conexão que você deseja editar.

c. Clique em **Editar servidores DNS**.

3. Adicionar, alterar ou remover endereços.

a. Para adicionar um endereço, clique em **Adicionar servidor DNS** e, em seguida, 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 do endereço. Não é possível 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 VMs continuam usando suas configurações DNS atuais até a reinicialização.)

Políticas

Definir políticas de grupo para máquinas não associadas a domínio

1. Faça RDP para a máquina que está sendo usada para a imagem.
2. Instale o Citrix Group Policy Management:

a. Navegue até CTX220345. Baixe o anexo.

b. Clique duas vezes no arquivo baixado. Na pasta `Group Policy Templates 1912 > Group Policy Management`, clique duas vezes em `CitrixGroupPolicyManagement_x64.msi`.

3. Use o comando **Executar** para iniciar `gpedit.msc`, que abre o Editor de Política de Grupo.
4. Em `User Configuration Citrix Policies > Unfiltered`, clique em **Editar Política**.

   Se o Console de Gerenciamento de Política de Grupo falhar (conforme descrito em CTX225742), instale o Microsoft Visual C++ 2015 Runtime (ou uma versão posterior desse runtime).

5. Habilite as configurações de política conforme necessário. Por exemplo:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ao trabalhar em **Configuração do Computador** ou **Configuração do Usuário** (dependendo do que você deseja configurar) na guia **Configurações**, em `Category > ICA / Printing`, selecione **Auto-create PDF Universal Printer** e defina como `Enabled`.
- Se você deseja que os usuários logados sejam administradores de sua área de trabalho, adicione o grupo **Usuário Interativo** ao grupo de administradores internos.

6. Quando terminar, salve a imagem.
7. Ou atualize o catálogo existente ou crie um novo catálogo usando a nova imagem.

Definir políticas de grupo para máquinas ingressadas no domínio

1. Certifique-se de que o recurso Gerenciamento de Política de Grupo esteja instalado.
   - Em uma máquina Windows multi-sessão, 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 Windows de sessão única, instale as Ferramentas de Administração de Servidor Remoto para o SO apropriado. (Esta instalação requer uma conta de administrador de domínio.) Após essa instalação, o console de Gerenciamento de Política de Grupo estará disponível no menu **Iniciar**.
2. Baixe e instale o pacote de gerenciamento de Política de Grupo do Citrix na página de download do Citrix e, em seguida, configure as configurações de política conforme necessário. Siga o procedimento em Definir políticas de grupo para máquinas não ingressadas no domínio, da etapa 2 até o final.

Ações de localização de recursos

O Citrix cria automaticamente um local de recurso e dois Cloud Connectors quando você cria o primeiro catálogo para publicar desktops e aplicativos. Você pode especificar algumas informações relacionadas ao local de recurso ao criar um catálogo. Consulte Configurações de localização de recursos ao criar um catálogo.

(Para Acesso Remoto a PC, você cria o local de recurso e os Cloud Connectors.)

Esta seção descreve as ações disponíveis após a criação de um local de recurso.

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Assinaturas de Nuvem** à direita.
2. Clique na assinatura.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A guia **Detalhes** mostra o número e os nomes dos catálogos e imagens na assinatura. Ela também indica o número de máquinas que podem entregar desktops ou aplicativos. Essa contagem não inclui máquinas usadas para outros fins, como imagens, Cloud Connectors ou servidores de licença RDS.
- A guia **Locais de Recursos** lista cada local de recurso. Cada entrada de local de recurso inclui o status e o endereço de cada Cloud Connector no local de recurso.

O menu de reticências na entrada de um local de recurso contém as seguintes ações.

Executar Verificação de Integridade

A seleção de **Executar Verificação de Integridade** inicia a verificação de conectividade imediatamente. Se a verificação falhar, o estado do Cloud Connector será desconhecido, pois ele não está se comunicando com o Citrix Cloud. Você pode querer reiniciar o Cloud Connector.

Reiniciar Conectores

A Citrix recomenda reiniciar apenas um Cloud Connector por vez. A reinicialização coloca o Cloud Connector offline e interrompe o acesso do usuário e a conectividade da máquina.

Selecione a caixa de seleção do Cloud Connector que você deseja reiniciar. Clique em **Reiniciar**.

Adicionar Conectores

Adicionar um Cloud Connector geralmente leva 20 minutos para ser concluído.

Forneça as seguintes informações:

- Quantos Cloud Connectors adicionar.
- Credenciais da conta de serviço de domínio, que são usadas para unir as máquinas Cloud Connector ao domínio.
- Desempenho da máquina.
- Grupo de recursos do Azure. O padrão é o grupo de recursos usado pela última vez pelo local do recurso.
- Unidade Organizacional (OU). O padrão é a OU usada pela última vez pelo local do recurso.
- Se sua rede requer um servidor proxy para conectividade com a internet. Se você indicar **Sim**, forneça o FQDN ou endereço IP do servidor proxy e o número da porta.

Quando terminar, clique em **Adicionar Conectores**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Excluir Conectores

Se um Cloud Connector não conseguir se comunicar com o Citrix Cloud e uma reinicialização não resolver o problema, o Suporte Citrix poderá recomendar a exclusão desse Cloud Connector.

Selecione a caixa de seleção do Cloud Connector que você deseja excluir. Em seguida, clique em **Excluir**. Quando solicitado, confirme a exclusão.

Você também pode excluir um Cloud Connector disponível. No entanto, se a exclusão desse Cloud Connector resultar em menos de dois Cloud Connectors disponíveis no local do recurso, você não poderá excluir o Cloud Connector selecionado.

Selecionar Hora da Atualização

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 do recurso sejam atualizados. O melhor momento para iniciar as atualizações geralmente é fora do seu horário comercial típico.

Escolha a hora para iniciar as atualizações ou indique que você deseja que as atualizações comecem quando uma atualização estiver disponível. Quando terminar, clique em **Salvar**.

Renomear

Insira o novo nome para o local do recurso. Clique em **Salvar**.

Configurar Conectividade

Indique se os usuários podem acessar desktops e aplicativos por meio do serviço Citrix Gateway, ou apenas de dentro da sua rede corporativa.

Gerenciamento de Perfil

Gerenciamento de Perfil garante que as configurações pessoais se apliquem aos aplicativos virtuais dos usuários, independentemente da localização do dispositivo do usuário.

A configuração do Gerenciamento de Perfil é opcional.

Você pode habilitar o Gerenciamento de Perfil com o serviço de otimização de perfil. Este serviço oferece uma maneira confiável de gerenciar essas configurações no Windows. O gerenciamento de perfis garante uma experiência consistente, mantendo um único perfil que acompanha o

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 administração, suporte e infraestrutura mínimos. Além disso, a otimização de perfil oferece aos usuários uma experiência aprimorada de logon e logoff.

O serviço de otimização de perfil requer um compartilhamento de arquivos onde todas as configurações pessoais persistem. 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 de Gerenciamento de Perfil. Para saber mais sobre o formato da string de texto UNC, consulte Especificar o caminho para o armazenamento do usuário.

Ao habilitar o Gerenciamento de Perfil, considere otimizar ainda mais o perfil do usuário configurando o redirecionamento de pastas para minimizar os efeitos do tamanho do perfil do usuário. A aplicação do redirecionamento de pastas complementa a solução de Gerenciamento de Perfil. Para obter mais informações, consulte Redirecionamento de Pastas da Microsoft.

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

Este serviço acessa os recursos de sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2016. Isso geralmente requer uma licença de acesso para cliente dos Serviços de Área de Trabalho Remota (RDS CAL). A máquina Windows onde o Citrix VDA está instalado deve ser capaz de contatar um servidor de licenças RDS para solicitar RDS CALs. Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento da Microsoft Ativar o Servidor de Licenças dos Serviços de Área de Trabalho Remota. Para ambientes de prova de conceito, você pode usar o período de carência fornecido pela Microsoft.

Com este método, você pode fazer com que este serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações de Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft Licenciar sua implantação RDS com licenças de acesso para cliente (CALs).

Para configurar o servidor de licenças RDS usando as configurações de Política de Grupo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Instale um Servidor de Licenças dos Serviços de Área de Trabalho Remota em uma das VMs disponíveis. A VM deve estar sempre disponível. As cargas de trabalho do serviço Citrix devem ser capazes de alcançar este servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Especificar o Modo de Licenciamento da Área de Trabalho Remota para um Servidor Host de Sessão RD.

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

Uso do compromisso de consumo

NOTA:

Este recurso está em pré-visualização.

No cartão **Geral** no painel **Quick Deploy > Microsoft Azure**, o valor de **Consumo** indica quanto consumo foi usado no mês calendário atual. Esse valor inclui compromissos mensais e de prazo.

Quando você clica em **Geral**, a guia **Notificações** inclui:

- Consumo total usado no mês (mensal e de prazo).
- Número de unidades de compromisso de consumo mensal.
- Porcentagem do compromisso de consumo de prazo.

Os valores e as barras de progresso podem alertá-lo sobre excessos de uso potenciais ou reais.

Os dados reais podem levar 24 horas para aparecer. Os dados de uso e faturamento são considerados finais 72 horas após o fim de um mês calendário.

Para mais informações de uso, consulte Monitorar licenças e uso para Citrix DaaS Standard para Azure.

Opcionalmente, você pode solicitar que as notificações apareçam no painel **Gerenciar** quando o uso do consumo (para compromissos mensais, de prazo ou ambos) atingir um nível especificado. Por padrão, as notificações estão desabilitadas.

1. Na guia **Notificações**, clique em **Editar Preferências de Notificação**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Para habilitar 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 **Salvar**.

Para desabilitar as notificações, clique no controle deslizante para que a marca de seleção não apareça mais e, em seguida, clique em **Salvar**.

Monitorar o uso de licenças Citrix

Para visualizar as informações de uso da sua licença Citrix, siga as orientações em Monitorar licenças e uso para Citrix DaaS Standard para Azure. Você pode visualizar:

- Resumo de 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 multi-sessão, 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 prosseguir.

- Na interface de gerenciamento do Quick Deploy para Citrix DaaS para 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

O balanceamento de carga mede a carga da máquina e determina qual máquina multi-sessão selecionar para uma sessão de usuário de entrada sob as 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 de várias sessões) na 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, pois mais máquinas são mantidas ligadas e ocupadas.

  Este método é habilitado 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 para Azure calcula e, em seguida, atribui um índice de carga para cada máquina de várias sessões. O cálculo considera fatores como CPU, memória e simultaneidade.)

  Este 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 essas máquinas.

  Exemplo simples: Você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com as primeiras 10 sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

  Com o balanceamento de carga vertical, as sessões maximizam a capacidade da máquina ligada, o que pode economizar custos de máquina.

Para configurar o método de balanceamento de carga:

1. No painel **Quick Deploy > Microsoft Azure**, expanda **Geral** à direita.
2. Em **Configurações Globais**, clique em **Ver Tudo**.
3. Na página **Configurações Globais**, em **Balanceamento de Carga do Catálogo de Várias Sessões**, escolha o método de balanceamento de carga.
4. Clique em **Confirmar**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Criar um catálogo em uma rede que usa um servidor proxy

Siga este procedimento se 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 Azure gerenciada pela Citrix com uma rede que exige um servidor proxy não é compatível.)

1. No painel **Quick Deploy > Microsoft Azure**, inicie o processo de criação de catálogo fornecendo as informações necessárias e, em seguida, clicando em **Create Catalog** na parte inferior da página.
2. A criação do catálogo falha devido ao requisito de proxy. No entanto, um local de recurso 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 **Cloud Subscriptions**. Na guia **Resource Locations**, verifique se o local de recurso recém-criado possui algum Cloud Connector. Se tiver, exclua-os.
3. No Azure, crie duas VMs (consulte requisitos de sistema do Cloud Connector). Associe essas máquinas ao domínio.
4. No console do Citrix Cloud, instale um Cloud Connector em cada VM. Certifique-se de que os Cloud Connectors estejam no mesmo local de recurso que foi criado anteriormente. Siga as orientações em:
   - Configuração de proxy e firewall do Cloud Connector
   - Requisitos de sistema e conectividade
5. No painel **Quick Deploy > Microsoft Azure**, repita o processo de criação do catálogo. Quando o catálogo é criado, ele usa o local de recurso e os Cloud Connectors que você criou nas etapas anteriores.

Obter ajuda

- Revise 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.