

# Guia do portal do tenant do VMware Cloud Director

Modificado em 4 de abril de 2021  
VMware Cloud Director 10.2

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

<https://docs.vmware.com/br/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Brasil**  
Rua Surubim, 504 4º andar CEP 04571-050  
Cidade Monções  
São Paulo  
SÃO PAULO: 04571-050  
Brasil  
Tel: +55 11 55097200  
Fax: + 55. 11. 5509-7224  
[www.vmware.com/br](http://www.vmware.com/br)

Copyright © 2017-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

# Conteúdo

Guia do portal do tenant do VMware Cloud Director™ 11

## 1 Introdução ao portal do tenant do VMware Cloud Director 13

- Noções básicas do VMware Cloud Director™ 13
- Fazer login no portal do tenant do VMware Cloud Director 15
- Funções e direitos do portal de tenants do VMware Cloud Director 15
- Usando o portal de tenants do VMware Cloud Director 16
- Usar a pesquisa global do VMware Cloud Director 17
- Usar a pesquisa rápida do VMware Cloud Director 18
- Exibir tarefas 19
- Parar uma tarefa em andamento 20
- Exibir eventos 21
- Definir preferências do usuário 21

## 2 Trabalhando com máquinas virtuais 23

- Arquitetura da máquina virtual 24
- Criptografia da máquina virtual 25
- Exibir máquinas virtuais 26
- Criar uma nova máquina virtual independente 27
- Provisionamento rápido de máquinas virtuais 28
- Abrindo um console de máquina virtual 29
  - Instalar o VMware Remote Console num cliente 29
  - Abrir um console remoto de máquina virtual 30
  - Abrir o console Web 31
- Operações para ligar ou desligar em máquinas virtuais 32
  - Ligar uma máquina virtual 32
  - Desligar uma máquina virtual 32
  - Desligar um sistema operacional convidado 33
  - Redefinir uma máquina virtual 33
  - Suspender uma máquina virtual 33
  - Descartar o estado suspenso de uma máquina virtual 34
  - Ligar várias VMs 34
  - Desligar várias máquinas virtuais 35
  - Descartar o estado suspenso de várias máquinas virtuais 35
  - Redefinir várias máquinas virtuais 36
- Instalar o VMware Tools numa máquina virtual 36
- Atualizar a versão do hardware virtual de uma máquina virtual 37
- Editar as propriedades da máquina virtual 38

Alterar as propriedades gerais de uma máquina virtual	38
Alterar as propriedades de hardware de uma máquina virtual	39
Alterar as propriedades de personalização do SO convidado de uma máquina virtual	42
Alterar as propriedades avançadas de uma máquina virtual	46
Inserir Mídia	49
Ejetar Mídia	50
Copiar uma máquina virtual para um vApp diferente	50
Mover uma máquina virtual para um vApp diferente	51
Afinidade e antiafinidade da máquina virtual	52
Visualizar regras de afinidade e antiafinidade	52
Criar uma regra de afinidade	53
Criar uma regra de antiafinidade	53
Editar uma regra de afinidade ou antiafinidade	54
Excluir uma regra de afinidade ou antiafinidade	55
Monitorar máquinas virtuais	55
Como trabalhar com instantâneos	56
Tirar um snapshot de uma máquina virtual	57
Converter uma máquina virtual para um snapshot	58
Excluir um snapshot de uma máquina virtual	58
Renovar um lease de máquina virtual	59
Excluir uma máquina virtual	59
Grupos de Dimensionamento Automático	60
Criar um grupo de dimensionamento	60
Adicionar uma regra de dimensionamento automático	61

### 3 Trabalhando com vApps 63

Visualizar vApps	64
Criar um novo vApp	64
Criar um vApp a partir de um pacote OVF	67
Adicionar um vApp de um catálogo	69
Criar um vApp de um modelo de vApp	71
Importar uma máquina virtual do vCenter Server como vApp	72
Operações para ligar ou desligar em vApps	73
Ligar um vApp	73
Desligar um vApp	74
Redefinir um vApp	74
Suspender um vApp	74
Descartar o estado suspenso de um vApp	75
Ligar vários vApps	75
Desligar vários vApps	76
Descartar o estado suspenso de vários vApps	76

Redefinir vários vApps	77
Suspender vários vApps	77
Abrir um vApp	78
Editar Propriedades do vApp	78
Editar as propriedades gerais do vApp	78
Editar a ordem de início e interrupção de máquinas virtuais em um vApp	79
Editar as propriedades de guest de um vApp	80
Compartilhar um vApp	81
Exibir um diagrama de rede do vApp	81
Trabalhando com redes em um vApp	82
Exibir redes do vApp	83
Isolar uma rede de vApp	83
Adicionar uma rede a um vApp	84
Configurar serviços de rede para uma rede vApp	85
Excluir uma rede vApp	92
Como trabalhar com instantâneos	92
Tirar um snapshot de um vApp	93
Converter um vApp para um snapshot	94
Excluir um snapshot de um vApp	94
Tirar snapshots de vários vApps	95
Remover snapshots de vários vApps	95
Reverter vários vApps para snapshots	96
Alterar o proprietário de um vApp	96
Mover um vApp para outro data center virtual	97
Copiar um vApp interrompido para outro data center virtual	97
Copiar um vApp ligado	98
Adicionar uma máquina virtual a um vApp	99
Salvar um vApp como um modelo do vApp em um catálogo	100
Baixar um vApp como um pacote OVF	101
Renovar um lease de vApp	102
Excluir um vApp	103
Excluir vários vApps	103

## 4 Trabalhando com clusters Kubernetes 105

Adicionar uma política do Kubernetes do VDC de Organização	106
Editar uma política do Kubernetes do VDC de organização	108
Criar um cluster do Tanzu Kubernetes	109
Criar um cluster do Kubernetes nativo	111
Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition	112
Configurar o acesso externo a um serviço em um cluster Tanzu Kubernetes	114

## 5 Como trabalhar com redes 116

Gerenciando redes de centros de dados virtuais de organização	119
Visualizar as redes VDC da organização disponíveis	120
Adicionar uma rede isolada de data center virtual da organização	121
Adicionar uma rede roteada de VDC da organização	122
Adicionar uma rede direta de data center virtual da organização	124
Adicionar uma rede de VDC de organização com um comutador lógico do NSX-T Data Center importado	125
Editar as configurações gerais de uma rede de data center virtual da organização	126
Conectar uma rede de centro de dados virtual da organização a um edge gateway	126
Desconectar uma rede de VDC de organização de um edge gateway	127
Converter a interface de uma rede do VDC de organização roteada	128
Visualizar os endereços IP usados para uma rede de centros de dados virtuais da organização	128
Adicionar endereços IP a um pool de IPs de rede de data center virtual da organização	129
Editar ou remover intervalos de IP usados em uma rede de data center virtual da organização	129
Editar as configurações de DNS de uma rede de data center virtual da organização	130
Definir as configurações de DHCP para uma rede de data center virtual de organização isolada	130
Adicionar um pool DHCP a uma rede roteada de centro de dados virtual da organização com o suporte do NSX-T Data Center	131
Editar ou excluir um pool DHCP existente para uma rede isolada de centro de dados virtual da organização com o suporte do NSX Data Center for vSphere	132
Redefinir uma rede de data center virtual de organização	133
Excluir uma rede de data center virtual de organização	133
Gerenciamento de rede de grupo de centros de dados com o NSX-T Data Center	134
Gerenciamento de grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center	135
Usando o firewall distribuído em um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center	137
Gerenciamento de redes de grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center	142
Gerenciamento de pontos de saída para grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center	148
Gerenciamento de rede de grupo de centros de dados com o NSX Data Center for vSphere	150
Gerenciando grupos de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere	151
Gerenciamento de redes do grupo de centros de dados com suporte do NSX Data Center for vSphere	166
Gerenciando serviços de edge gateway do NSX Data Center for vSphere	168
Introdução ao recuso de Rede Avançada do VMware Cloud Director com NSX Data Center for vSphere	169
Configuração de firewall de tenant com NSX Data Center for vSphere	169
Gerenciando o DHCP do edge gateway do NSX Data Center for vSphere	181

Gerenciamento da conversão de endereços de rede (NAT) em um Edge Gateway do NSX Data Center for vSphere	186
Configuração de roteamento avançada para Edges Gateways do NSX Data Center for vSphere	190
Balanceamento de carga com o NSX Data Center for vSphere	198
Configurar o acesso seguro usando VPN em um edge gateway do NSX Data Center for vSphere	213
Gerenciamento de certificado SSL em um edge gateway do NSX Data Center for vSphere	239
Objetos de agrupamento personalizados para edge gateways do NSX Data Center for vSphere	246
Estatísticas e logs para um Edge Gateway do NSX Data Center for vSphere	250
Ativar o acesso pela linha de comando SSH a um edge gateway do NSX Data Center for vSphere	252
Trabalho com tags de segurança para edge gateways do NSX Data Center for vSphere	252
Trabalho com grupos de segurança para edge gateways do NSX Data Center for vSphere	257
Gerenciando Edge Gateways do NSX-T Data Center	260
Adicionar um conjunto de IPs a um edge gateway do NSX-T Data Center	261
Adicionar uma regra de firewall do edge gateway do NSX-T Data Center	262
Adicionar uma regra de SNAT ou DNAT a um edge gateway do NSX-T	263
Configurar um serviço de encaminhador de DNS em um edge gateway do NSX-T	266
Criar perfis de portas de aplicativos personalizados	267
VPN baseada em políticas IPsec para edge gateways do NSX-T Data Center	268
Configurar serviços de rede externa dedicada	271
Como trabalhar com o balanceamento de carga avançado do NSX	276
<b>6 Usando discos nomeados e revisando políticas de armazenamento</b>	<b>284</b>
Criando e usando discos nomeados	284
Criar um disco nomeado	285
Editar um disco nomeado	285
Anexar um disco nomeado a uma máquina virtual	286
Excluir um disco nomeado	286
Revisar propriedades de políticas de armazenamento	287
<b>7 Revisando e editando propriedades de centros de dados virtuais</b>	<b>288</b>
Revisar propriedades do data center virtual	288
Revisar os metadados do data center virtual	288
Limitar o acesso a um VDC de organização a usuários e grupos específicos na sua organização	289
<b>8 Como trabalhar com instâncias, endpoints e proxies dedicados do vCenter Server</b>	<b>291</b>
Usando o Chrome Browser Extension for VMware Cloud Director	292

- Configurar o navegador com as configurações de proxy 292
- Fazer login na interface de usuário de um componente usando um endpoint 293

## 9 Trabalhando com modelos de vApp 295

- Visualizar um modelo de vApp 295
- Criar um modelo de vApp de um arquivo OVF 296
- Importar uma máquina virtual do vCenter Server como modelo do vApp 297
- Atribuir uma política de posicionamento de VM e uma política de dimensionamento de VM a um modelo vApp 298
- Baixar um modelo de vApp 299
- Excluir um modelo de vApp 299

## 10 Trabalhando com arquivos de mídia 301

- Carregar arquivos de mídia 301
- Excluir um arquivo de mídia 302
- Baixar um arquivo de mídia 302

## 11 Trabalhando com catálogos 304

- Exibir catálogos 305
- Criar um catálogo 305
- Compartilhar um catálogo 306
- Excluir um catálogo 307
- Alterar o proprietário de um catálogo 308
- Gerenciar metadados para um catálogo 308
- Publicar um catálogo 309
- Assinar um catálogo externo 309
- Atualizar a URL do local e a senha para um catálogo assinado 310
- Sincronizar um catálogo assinado 311

## 12 Trabalhando com modelos de data center virtual de organização 312

- Visualizar modelos de centro de dados virtual disponíveis 312
- Instanciar um centro de dados virtual a partir de um modelo 313

## 13 Gerenciar usuários, grupos e funções 315

- Gerenciar usuários 315
  - Criar um usuário 315
  - Importar Usuários 317
  - Modificar um usuário 318
  - Desativar ou ativar uma conta de usuário 319
  - Excluir um usuário 319
  - Desbloquear uma conta de usuário bloqueada 320
  - Gerenciar as cotas de recursos de um usuário 320



Gerenciar grupos	321
Importar um grupo	321
Excluir um grupo	322
Editar um grupo	322
Gerenciar as cotas de recursos de um grupo	323
Funções e direitos	324
Funções predefinidas e seus direitos	324
Direitos em funções predefinidas de tenant global	326
Criar uma função de tenant personalizada	332
Editar uma função de tenant personalizada	333
Excluir uma função	333
<b>14 Configurar provedores de identidade</b>	<b>335</b>
Permitir que sua organização use um provedor de identidade SAML	335
Editar configurações LDAP para sua organização	337
Configurar, teste e sincronizar uma conexão LDAP	338
<b>15 Gerenciamento de certificados</b>	<b>341</b>
Importar certificados confiáveis	341
Importar certificados para a biblioteca de certificados	342
<b>16 Gerenciar a organização</b>	<b>344</b>
Editar nome e descrição da organização	344
Modificar suas configurações de e-mail	345
Testar configurações de SMTP	346
Modificar configurações de domínio das máquinas virtuais da organização	346
Trabalhando com vários sites	347
Configurar e gerenciar implantações multissite	347
Noções básicas sobre leases	348
Modificar as políticas de lease de modelos de vApp e vApps na sua organização	349
Modificar as políticas de senha e de conta de usuário da organização	350
Criar um painel de avisos	351
<b>17 Como trabalhar com a biblioteca de serviços</b>	<b>352</b>
Procurar um serviço	352
Executar um serviço	353
<b>18 Gerenciamento de entidades definidas</b>	<b>354</b>
Como trabalhar com definições de entidades personalizadas	357
Procurar uma entidade personalizada	357
Editar uma definição da entidade personalizada	357

Adicione uma definição da entidade personalizada	358
Instâncias de Entidades Personalizadas	359
Associar uma ação a uma entidade personalizada	359
Desassociar uma ação de uma definição de entidade personalizada	360
Publicar uma entidade personalizada	361
Excluir uma entidade personalizada	362

# Guia do portal do tenant do VMware Cloud Director™

O *Guia do Portal do Tenant do VMware Cloud Director™* fornece informações sobre como usar o portal do tenant do VMware Cloud Director. Nesta versão, você usa o portal do tenant para administrar sua organização, criar e configurar máquinas virtuais, vApps e redes dentro do vApps. Você também pode configurar os recursos de rede avançados fornecidos pelo VMware NSX® para o vSphere® em um ambiente do VMware Cloud Director. Com o portal do tenant do VMware Cloud Director, você também pode criar e gerenciar catálogos, modelos de vApp e VDC, e criar e gerenciar redes entre data centers virtuais.

## Público-alvo

Este guia destina-se a qualquer pessoa que deseja usar os recursos do portal do tenant do VMware Cloud Director. As informações são escritas principalmente para **administradores de organização** que usam o portal do tenant para administrar sua organização, gerenciar máquinas virtuais, vApps, redes e assim por diante.

## Glossário de publicações técnicas da VMware

As publicações técnicas da VMware fornecem um glossário dos termos que você pode não conhecer. Para saber as definições de termos como são usados na documentação técnica da VMware, consulte <http://www.vmware.com/support/pubs>.

## Termos e condições de uso

A VMware dá permissão a você para modificar este guia do usuário do tenant (o “Guia”) conforme razoavelmente necessário para personalizá-lo para refletir seus processos operacionais e, em seguida, reproduzir e distribuir o Guia modificado para seus clientes. Você não pode cobrar de seus clientes uma taxa de acesso ao Guia modificado. VOCÊ RECONHECE QUE O GUIA É FORNECIDO A VOCÊ SEM CUSTO, “COMO ESTÁ”, SEM GARANTIA DE QUALQUER TIPO E APENAS PARA O FIM DESCRITO ACIMA. ASSIM, A RESPONSABILIDADE TOTAL DA VMWARE E DE SEUS FORNECEDORES DECORRENTE DE OU RELACIONADA A FORNECER A VOCÊ ACESSO AO GUIA NÃO DEVERÁ EXCEDER \$ 100. EM NENHUMA CIRCUNSTÂNCIA A VMWARE OU SEUS FORNECEDORES TERÃO RESPONSABILIDADE POR QUAISQUER DANOS INDIRETOS, INCIDENTAIS, ESPECIAIS OU CONSEQUENCIAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS COMERCIAIS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES COMERCIAIS), INDEPENDENTEMENTE DA CAUSA E DE QUALQUER TEORIA

DE RESPONSABILIDADE, MESMO QUE A VMWARE OU SEUS FORNECEDORES TENHAM SIDO AVISADOS DA POSSIBILIDADE DE TAIS DANOS. ESSAS LIMITAÇÕES SERÃO APLICADAS NÃO OBSTANTE QUALQUER FALHA DO PROPÓSITO ESSENCIAL DE QUALQUER RECURSO LIMITADO.

# Introdução ao portal do tenant do VMware Cloud Director

# 1

Quando você faz login no portal do tenant, há uma série de tarefas que podem ser concluídas, desde a criação de máquinas virtuais e de vApps até a definição da configuração de rede avançada e a execução de fluxos de trabalho do vRealize Orchestrator.

Este capítulo inclui os seguintes tópicos:

- Noções básicas do VMware Cloud Director™
- Fazer login no portal do tenant do VMware Cloud Director
- Funções e direitos do portal de tenants do VMware Cloud Director
- Usando o portal de tenants do VMware Cloud Director
- Usar a pesquisa global do VMware Cloud Director
- Usar a pesquisa rápida do VMware Cloud Director
- Exibir tarefas
- Parar uma tarefa em andamento
- Exibir eventos
- Definir preferências do usuário

## Noções básicas do VMware Cloud Director™

O VMware Cloud Director™ fornece acesso baseado em função a um portal de tenants baseado na Web que permite aos membros de uma organização interagir com os recursos da organização para criar e trabalhar com vApps e máquinas virtuais.

Antes de você poder acessar sua organização, um VMware Cloud Director **administrador de sistema** precisa criar a organização, atribuir recursos a ela e fornecer a URL de acesso ao portal de tenants. Toda organização inclui um ou mais **administradores de organização**, que finalizam a configuração da organização adicionando membros e configurando políticas e preferências. Depois de configurada a organização, os usuários não administradores poderão fazer login para criar, usar e gerenciar máquinas virtuais e vApps.

## Organizações

Uma organização é uma unidade de administração para um conjunto de usuários, grupos e recursos de computação. Os usuários autenticam-se no nível da organização, fornecendo credenciais estabelecidas pelo **administrador da organização** quando o usuário foi criado ou importado. Os **administradores de sistema** criam e provisionam as organizações, enquanto os **administradores de organização** gerenciam catálogos, grupos e usuários da organização.

## Usuários e grupos

Uma organização pode conter um número arbitrário de usuários e grupos. Usuários podem ser criados localmente pelo administrador da organização ou importados de um serviço de diretório. Os grupos devem ser importados do serviço de diretório. Permissões dentro de uma organização são controladas por meio da atribuição de direitos e funções a usuários e grupos.

## Centros de dados virtuais

Um centro de dados virtual da organização fornece recursos a uma organização. Os centros de dados virtuais fornecem um ambiente onde os sistemas virtuais podem ser armazenados, implantados e operados. Eles também fornecem armazenamento para mídias virtuais de CD e DVD. Uma organização pode ter vários centros de dados virtuais.

## Redes de datacenters virtuais da organização

Uma rede de centros de dados virtuais da organização localiza-se em um centro de dados virtual da organização do VMware Cloud Director e está disponível para todos os vApps na organização. Uma rede de centros de dados virtuais da organização permite que os vApps em uma organização se comuniquem entre si. Uma rede de centros de dados virtuais da organização pode ser conectada a uma rede externa ou isolada e interna à organização. Apenas **administradores de sistema** podem criar redes de centros de dados virtuais da organização, mas os **administradores de organização** podem gerenciar as redes de centros de dados virtuais da organização, incluindo os serviços de rede que fornecem.

## Redes do vApp

Uma rede do vApp está localizada em um vApp e permite que as máquinas virtuais no vApp se comuniquem entre si. Você pode conectar uma rede do vApp a uma rede de centros de dados virtuais da organização para permitir que o vApp se comunique com outros vApps na organização e fora dela caso a rede de centros de dados virtuais da organização esteja conectada a uma rede externa.

## Catálogos

As organizações usam catálogos para armazenar os modelos do vApp e arquivos de mídia. Os membros de uma organização que têm acesso a um catálogo podem usar os arquivos de mídia e modelos do vApp dele para criar os próprios vApps. Os **administradores de organização** podem copiar itens de catálogos públicos para o catálogo da organização.

## Instâncias de dedicadas do vCenter Server (SDDCs) e proxies

Um SDDC (Centro de Dados Definido por Software) encapsula todo um ambiente vCenter Server. Uma instância dedicada do vCenter Server pode incluir um ou mais proxies que fornecem acesso a diferentes componentes do ambiente subjacente. O **administrador do sistema** pode publicar uma ou mais instâncias dedicadas do vCenter Server na sua organização. Você pode usar os proxies para acessar a interface do usuário ou a API dos componentes com proxy.

## Fazer login no portal do tenant do VMware Cloud Director

Você pode acessar o portal do tenant do VMware Cloud Director usando uma URL específica para sua organização.

Entre em contato com o **administrador da organização** se você não souber a URL da organização do portal do tenant. Consulte o *Notas da Versão do VMware Cloud Director* para obter informações sobre navegadores e configurações compatíveis.

### Procedimentos

- 1 Em um navegador da Web, navegue até a URL do portal do tenant da sua organização.  
Por exemplo, *https://cloud.example.com/tenant/myOrg*.
- 2 Insira seu nome de usuário e senha e clique em **Fazer Login**.

## Funções e direitos do portal de tenants do VMware Cloud Director

O VMware Cloud Director inclui um conjunto pré-configurado de funções de usuário e seus direitos. As funções que podem acessar o portal de tenants do VMware Cloud Director são as criadas por padrão em qualquer organização ou outras funções criadas pelo administrador de organização.

Os usuários que receberam as seguintes funções organizacionais poderão acessar o portal de tenants. Os itens que eles visualizam e as ações que eles podem realizar dependem dos direitos associados a uma função específica.

- **Administrador da organização**
- **Autor do catálogo**
- **Autor de vApp**
- **Usuário de vApp**
- **Somente acesso ao console**

Para obter informações sobre as funções predefinidas e seus direitos, consulte [Funções predefinidas e seus direitos](#).

## Usando o portal de tenants do VMware Cloud Director

Se você tiver mais de um centro de dados virtual, quando fizer login no portal de tenants do VMware Cloud Director, será direcionado para a tela do painel **Centros de Dados**. Se você tiver apenas um centro de dados virtual, quando fizer login no portal de tenants do VMware Cloud Director, será direcionado diretamente para o centro de dados.

A tela do painel **Centros de Dados** é parte do recurso multissite do VMware Cloud Director que permite aos tenants ver o ambiente de nuvem distribuído geograficamente deles como uma entidade única. Para obter mais informações sobre multissite, consulte [Trabalhando com vários sites](#).

O dashboard é uma visão unificada dos locais e centros de dados virtuais do VMware Cloud Director não apenas em uma única organização. Em um ambiente de várias células e várias organizações, você também pode ver os centros de dados virtuais de todas as outras organizações associadas.

---

**Observação** Dependendo dos direitos deles, os usuários do tenant poderão ver todos os sites membros de uma organização ou apenas um subconjunto de sites.

---

As informações sobre a organização são exibidas na parte superior na faixa de resumo.

Se você fizer login como **administrador de organização**, verá:

- O número de sites, organizações e centros de dados virtuais
- Número total de máquinas virtuais e vApps em execução
- Recursos de hardware usados, como CPU, memória e armazenamento

Os centros de dados virtuais são exibidos em um modo de exibição de cartão. Todo cartão contém informações sobre a organização à qual o centro virtual pertence, o número de vApps, o número total de máquinas virtuais e o número de máquinas virtuais que estão no estado de execução. O cartão também mostra o CPU, a memória e a capacidade de armazenamento disponíveis para o centro de dados e exibe métricas em tempo real sobre as alocações atuais e reservas de recursos.

Na navegação superior, você pode navegar para os diferentes itens de menu.

Item de menu	Descrição
Centros de Dados	Navega até os recursos de <b>Centro de Dados Virtual</b> , <b>Grupos de Centros de Dados</b> e <b>Centros de Dados Dedicados do vSphere</b> na sua organização
Datacenter Virtual	Navega até a tela <b>Centro de Dados Virtual</b> que exibe os centros de dados virtuais dentro da organização.
Centros de Dados Dedicados do vSphere	Navega até a tela que exibe os centros de dados dedicados do vSphere que seu provedor de serviços publicou na sua organização.
Aplicativos	Navega até os recursos <b>Aplicativos Virtuais</b> e <b>Máquinas Virtuais</b> na sua organização.



Item de menu	Descrição
Bibliotecas	Direciona você para uma visualização consolidada para modelos do vApp, catálogos, mídia e outros tipos de arquivos. Você usa esses modelos e arquivos para implantar máquinas virtuais ou vApps.
Rede	Leva você até as redes, edge gateways e grupos de centros de dados em sua organização.
Administração	Navega até as telas de configuração <b>Controle de Acesso</b> , <b>Provedor de Identidade</b> e às configurações gerais, e-mail, personalização de convidados, metadados, multissite e políticas da sua organização.
Monitorar	Navega até as telas <b>Tarefas</b> e <b>Eventos</b> . A tela <b>Tarefas</b> exibe as tarefas relatadas pelo VMware Cloud Director. A tela <b>Eventos</b> exibe os eventos relatados pelo VMware Cloud Director.

Você pode personalizar seu Portal do Tenant do VMware Cloud Director usando OpenAPIs do Cloud Director do **Branding**. Para obter informações sobre como usar o OpenAPI do Cloud Director, consulte o documento de *Guia de introdução do OpenAPI do Cloud Director* em <https://code.vmware.com>.

## Usar a pesquisa global do VMware Cloud Director

Você pode usar a pesquisa global do VMware Cloud Director para realizar uma busca por um nome ou parte de um nome entre os nomes dos objetos no seu ambiente. Você também poderá procurar uma máquina virtual por endereço IP se o endereço IP da máquina virtual for estático.

A lista de objetos predefinidos é:

- Centros de dados
- Modelos do vApp
- vApps
- Máquinas virtuais
- Redes do vApp
- Catálogos

Se uma máquina virtual usar um endereço IP atribuído pelo DHCP, a pesquisa não retornará o endereço IP dela. Se você quiser procurar uma máquina virtual com um endereço IP atribuído pelo DHCP, deverá procurar por nome.

Por padrão, você só pode procurar nos objetos em seu site local. Se você tiver um ambiente multissite, poderá pesquisar em vários sites.

### Procedimentos

- 1 No canto superior direito do portal de tenants do VMware Cloud Director, clique no ícone **Pesquisar**.
- 2 (Opcional) Fixe o painel de pesquisa clicando no ícone **Fixar**.

- 3 Na caixa de texto **Pesquisar**, insira um símbolo, parte de um nome ou um endereço IP pelo qual procurar nomes de objetos correspondentes ou endereços IP estáticos de máquinas virtuais.
- 4 Se você usar um ambiente multissite, selecione os sites nos quais deseja realizar a pesquisa.
- 5 Pressione **Enter**.

### Resultados

Os cinco principais resultados correspondentes por tipo de objeto aparecem. Os resultados são classificados em ordem alfabética.

### Próximo passo

- Para ver mais resultados, se houver algum, clique em **Carregar mais** sob cada tipo de objeto.
- Para ver mais informações sobre um objeto específico dos resultados da pesquisa, aponte para ele.
- Para gerenciar um objeto específico, por exemplo, para visualizar ou modificar as configurações de um objeto, clique nele. Os detalhes sobre o objeto aparecem à esquerda.

## Usar a pesquisa rápida do VMware Cloud Director

Você pode usar a pesquisa rápida do VMware Cloud Director para encontrar telas, entidades e ações. Os resultados dependem da sua localização na interface do usuário.

Os resultados dependem do contexto, de você ter ou não selecionado uma entidade e das ações disponíveis para uma entidade específica. Os resultados da pesquisa são agrupados em seções.

- Navegação Global – os resultados nesta seção não estão relacionados a uma entidade específica, por exemplo, Edge Gateways, LDAP, Tarefas, Certificados Confiáveis, Máquinas Virtuais e assim por diante. Você obterá esses resultados independentemente de onde estiver na interface do usuário.
- Navegação Contextual - os resultados nesta seção dependem da entidade selecionada na interface do usuário. Por exemplo, visualizações específicas de vApps, como VMs, Diagrama de Rede e assim por diante. Se você selecionar uma entidade, como um vApp, a pesquisa mostrará resultados de navegação global e contextual e quaisquer ações que possam ser aplicáveis à entidade.
- Ações Contextuais - os resultados nesta seção dependem da entidade selecionada na interface do usuário. Dependendo da sua localização na interface do usuário e da entidade que você selecionar, usando os resultados de pesquisa rápida, será possível realizar uma ação relacionada à entidade. Por exemplo, pesquisar a partir da exibição de detalhes de uma máquina virtual mostra os resultados das exibições globais, exibições contextuais e ações que você pode realizar na VM selecionada.

- Pesquisa de Entidade por Nome - se você estiver exibindo uma lista de entidades, os resultados da pesquisa poderão incluir também nomes de entidades do mesmo tipo que aquelas na lista. Por exemplo, se você estiver exibindo uma lista de VMs, os resultados da pesquisa incluirão correspondências de navegação global e nomes correspondentes de VMs. Se houver mais de uma página de entidades na lista que você está visualizando, a pesquisa verificará a lista completa de entidades e poderá exibir um nome que não esteja visível na página atual.

#### Procedimentos

- 1 Abra a janela **Pesquisa Rápida**.
  - Na barra de navegação superior, clique no menu **Ajuda** e selecione **Pesquisa Rápida**.
  - Pressione Ctrl +. ou Cmd +., dependendo do seu sistema operacional.
- 2 Insira critérios de pesquisa.
- 3 Navegue pelos resultados e selecione uma opção ou execute uma ação clicando ou pressionando Enter.
 

É possível usar as teclas de seta para cima e para baixo para navegar pelos resultados da pesquisa.

## Exibir tarefas


No portal de tenants, você pode ver a lista de tarefas recentes, junto com os detalhes e o status delas. Além disso, você também pode ver a lista de todas as tarefas.

Por padrão, o painel **Tarefas Recentes** aparece na parte inferior do portal de tenants e contém uma lista das tarefas que foram executadas recentemente. Quando você inicia uma operação, por exemplo, para criar uma máquina virtual, a tarefa é exibida no painel. Caso você minimize o painel **Tarefas Recentes**, ainda será possível ver o número de tarefas recentes em execução ou com falha. Você sempre poderá abrir o painel **Tarefas Recentes** novamente clicando nas setas duplas.

O modo de exibição de tarefas lista todas as tarefas, mostra quando as tarefas foram executadas e se foram concluídas com êxito. Esse modo de exibição é a primeira etapa para solucionar problemas no seu ambiente. O modo de exibição de tarefas contém operações de longa execução, como a criação de máquina virtual ou vApp.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Monitorar** e **Tarefas**.
 

A lista de todas as tarefas recentes é exibida, junto com o horário em que ela tarefa foi executada e o status dela.
- 2 Clique no ícone do editor (  ) para alterar os detalhes que você deseja visualizar sobre as tarefas.

### 3 (Opcional) Para visualizar os detalhes da tarefa, clique no nome dela.

Os detalhes da tarefa incluem informações como o motivo da falha, quando a tarefa falhou e assim por diante.

Detalhe	Descrição
Operação	Nome da operação realizada.
ID de Trabalho	O ID da tarefa.
Tipo	O objeto no qual a tarefa foi realizada. Por exemplo, se você criou uma máquina virtual, o tipo será VM.
Organização	Nome da organização.
Status	Status da tarefa, como Com êxito, Em execução ou Falhou.
Iniciador	O usuário que iniciou a operação.
Hora de início	A data e a hora em que a operação foi iniciada.
Hora de conclusão	A data e a hora em que a operação foi bem-sucedida ou falhou.
Namespace do serviço	Nome do serviço, como <i>com.vmware.cloud</i> .
Detalhes	Motivo da falha da tarefa. Por exemplo, se você tentar criar um instantâneo de uma máquina virtual, e a operação falhar, devido ao armazenamento é insuficiente, os detalhes da tarefa serão do tipo: A operação solicitada excederá a cota de armazenamento do VDC: a política de armazenamento "*" tem 8.693 MB restantes, e 41.472 MB são necessários.

## Parar uma tarefa em andamento

Se você iniciar acidentalmente uma operação antes de aplicar ou analisar todas as configurações necessárias, poderá interromper a tarefa em andamento.

Por padrão, o painel **Tarefas Recentes** é exibido na parte inferior do portal. Quando você inicia uma operação, por exemplo, para criar uma máquina virtual, a tarefa é exibida no painel.

### Pré-requisitos

O painel **Tarefas Recentes** deve estar aberto.

### Procedimentos

#### 1 Inicie uma operação de execução longa.

Operações de execução longa são operações como a criação de uma máquina virtual ou um vApp, operações de energia executadas em máquinas virtuais e vApps e assim por diante.

#### 2 No painel **Tarefas Recentes**, clique no ícone **Cancelar**.

#### 3 Na caixa de diálogo **Cancelar Tarefa**, confirme que você deseja cancelar a tarefa clicando em **OK**.

### Resultados

A operação é interrompida.

## Exibir eventos


A partir do portal, você pode ver a lista de todos os eventos, bem como seus detalhes e status.

A exibição de eventos é uma maneira de exibir o status dos eventos no seu portal. A exibição mostra quando os eventos aconteceram e se eles foram bem-sucedidos. A exibição de eventos contém ocorrências de uma vez, como logons de usuário e criação de objeto ou exclusão.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Monitorar** e **Eventos**.

A lista de todos os eventos é exibida, juntamente com a hora em que o evento ocorreu e o status do evento.

- 2 Clique no ícone do editor (  ) para alterar os detalhes que você deseja exibir sobre os eventos.
- 3 (Opcional) Clique em um evento para exibir os detalhes dele.

Detalhe	Descrição
Evento	Nome do evento. Por exemplo, se você modificar um vApp para incluir máquinas virtuais nele, o evento que inicia toda a operação será <i>Início da tarefa 'Modificar vApp'</i> .
ID do Evento	O ID da tarefa.
Tipo	O objeto no qual a tarefa foi realizada. Por exemplo, se você criou uma máquina virtual, o tipo será <i>VM</i> .
Destino	Objeto de destino do evento. Por exemplo, quando você modifica um vApp para incluir máquinas virtuais nele, o evento <i>Início da tarefa 'Modificar vApp'</i> é <i>vdcUpdateVapp</i> .
Status	Status do evento, como Com êxito ou Falhou.
Namespace do serviço	Nome do serviço, como <i>com.vmware.cloud</i> .
Organização	Nome da organização.
Proprietário	Usuário que acionou o evento.
Tempo de ocorrência	Data e hora em que o evento ocorreu.

## Definir preferências do usuário

Você pode definir determinadas preferências de exibição e alerta do sistema que terão efeito todas as vezes que fizer login no sistema.

Para saber mais sobre concessões, consulte [Noções básicas sobre leases](#).

### Procedimentos

- 1 Na barra de navegação superior, clique no seu nome de usuário e selecione **Preferências do usuário**.

- 2 Selecione a página a ser exibida quando você fizer login.
  - a Selecione o botão de opção ao lado de **Página Inicial** e clique em **Editar**.
  - b Selecione uma opção no menu suspenso e clique em **Salvar**.
- 3 Configure uma notificação por e-mail para expirações de concessão de tempo de execução.
  - a Selecione o botão de opção ao lado de **Tempo de Alerta de Locação de Implantação** e clique em **Editar**.
  - b Insira um valor em segundos e clique em **Salvar**.
- 4 Configure uma notificação por e-mail para expirações de locação de armazenamento.
  - a Selecione o botão de opção ao lado de **Tempo de Alerta de Locação de Armazenamento** e clique em **Editar**.
  - b Insira um valor em segundos e clique em **Salvar**.

# Trabalhando com máquinas virtuais

## 2

Uma máquina virtual é um computador de software que, como um computador físico, executa um sistema operacional e aplicativos. A máquina virtual consiste em um conjunto de arquivos de especificações e configurações, e tem o suporte dos recursos físicos de um host. Cada máquina virtual tem dispositivos virtuais que fornecem a mesma funcionalidade que o hardware físico, mas são mais portáteis, mais seguros e mais fáceis de gerenciar.

Além das operações que você pode executar em uma máquina física, as máquinas virtuais do VMware Cloud Director suportam operações de infraestrutura virtual, como tirar um instantâneo do estado da máquina virtual e mudar uma máquina virtual de um host para outro.

Começando com o VMware Cloud Director 9.5, as máquinas virtuais oferecem suporte para conectividade IPv6. Você pode atribuir endereços IPv6 a máquinas virtuais conectadas a redes IPv6.

---

**Importante** Todas as etapas para trabalhar com máquinas virtuais são documentadas com base no modo de exibição de cartão, pressupondo-se que você tenha mais de um centro de dados virtual. Também é possível concluir os mesmos procedimentos partindo do modo de exibição de grade, mas as etapas podem variar ligeiramente.

---

Este capítulo inclui os seguintes tópicos:

- [Arquitetura da máquina virtual](#)
- [Criptografia da máquina virtual](#)
- [Exibir máquinas virtuais](#)
- [Criar uma nova máquina virtual independente](#)
- [Provisionamento rápido de máquinas virtuais](#)
- [Abrindo um console de máquina virtual](#)
- [Operações para ligar ou desligar em máquinas virtuais](#)
- [Instalar o VMware Tools numa máquina virtual](#)
- [Atualizar a versão do hardware virtual de uma máquina virtual](#)
- [Editar as propriedades da máquina virtual](#)
- [Inserir Mídia](#)

- [Ejetar Mídia](#)
- [Copiar uma máquina virtual para um vApp diferente](#)
- [Mover uma máquina virtual para um vApp diferente](#)
- [Afinidade e antiafinidade da máquina virtual](#)
- [Monitorar máquinas virtuais](#)
- [Como trabalhar com instantâneos](#)
- [Renovar um lease de máquina virtual](#)
- [Excluir uma máquina virtual](#)
- [Grupos de Dimensionamento Automático](#)

## Arquitetura da máquina virtual

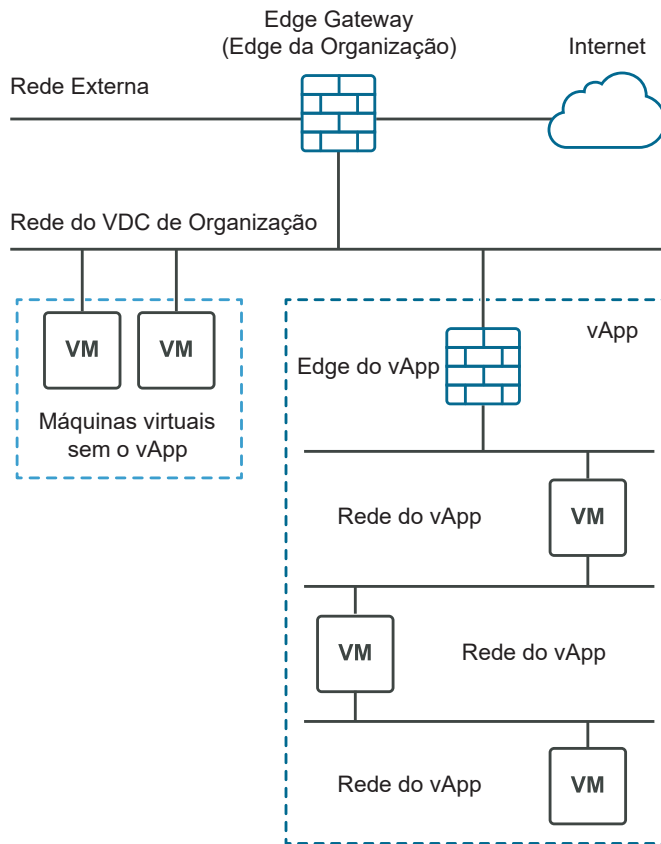
Uma máquina virtual pode existir como uma máquina independente ou pode existir num vApp.

Uma máquina virtual é um computador de software que, como um computador físico, executa um sistema operacional e aplicativos. A máquina virtual consiste em um conjunto de arquivos de especificações e configurações, e tem o suporte dos recursos físicos de um host. Cada máquina virtual tem dispositivos virtuais que fornecem a mesma funcionalidade que o hardware físico, mas são mais portáteis, mais seguros e mais fáceis de gerenciar. As máquinas virtuais podem ser autônomas ou podem existir num vApp. Um vApp é um objeto composto, por uma ou mais máquinas virtuais, bem como por uma ou mais redes.

A figura a seguir mostra as diferentes opções ao criar uma máquina virtual. Você pode criar uma máquina virtual independente ou uma máquina virtual num vApp. A máquina virtual independente está diretamente conectada ao datacenter virtual da organização. Você também pode criar uma máquina virtual num vApp. Ao criar uma máquina virtual dentro de um vApp, você pode agrupar várias máquinas virtuais e as respectivas redes associadas. Os vApps permitem que você crie aplicativos complexos e salve-os em um catálogo para uso no futuro.



Figura 2-1. As máquinas virtuais são independentes ou estão num vApp



## Criptografia da máquina virtual

A partir do VMware Cloud Director 10.1, você pode melhorar a segurança dos seus dados usando a criptografia da VM. Você pode criptografar VMs e discos associando-os a políticas de armazenamento que têm o recurso de Criptografia de VM.

A criptografia protege não apenas sua máquina virtual, mas também discos da máquina virtual e outros arquivos. Você pode visualizar os recursos das políticas de armazenamento e o status de criptografia de VMs e discos na API e na IU. Você pode realizar todas as operações em VMs e discos criptografados compatíveis na respectiva versão do vCenter Server.

Se o VDC de organização tiver uma política de armazenamento com criptografia de VM habilitada, você poderá criptografar VMs e discos. Consulte o tópico [Habilitando a criptografia de VM em políticas de armazenamento de um centro de dados virtual da organização](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*. Para criptografar uma VM ou um disco, associe-o a uma política de armazenamento habilitada para Criptografia de VM. Para máquinas virtuais, consulte [Criar uma nova máquina virtual independente](#) ou [Alterar as propriedades gerais de uma máquina virtual](#). Para discos nomeados, consulte [Criar um disco nomeado](#) ou [Editar um disco nomeado](#). Para descriptografar uma VM ou um disco, associe essa VM ou o disco a uma política de armazenamento que não tem criptografia habilitada.

## Limitações de criptografia da VM

As seguintes ações não são compatíveis com o VMware Cloud Director.

- Criptografe ou descriptografe uma VM ligada ou seus discos.
- Exporte um OVF de uma VM criptografada.
- Criptografe e descriptografe os discos de uma VM com um instantâneo se os discos fizerem parte do instantâneo.
- Descriptografe uma VM quando seu disco estiver em uma política criptografada.
- Adicione um disco criptografado a uma VM não criptografada.
- Criptografe um disco existente em uma VM não criptografada.
- Adicione um disco nomeado criptografado a uma VM descriptografada.
- Crie um clone vinculado criptografado.
- Criptografe uma VM de clone vinculado ou seus discos.
- Crie, mova ou clone VMs em instâncias do vCenter Server quando a VM de origem estiver criptografada.

---

**Observação** Em um VDC de organização com provisionamento rápido, se a VM de origem ou de destino estiver criptografada e você quiser criar um clone, o VMware Cloud Director sempre criará uma clonagem completa.

---

## Identificando um recurso de armazenamento de criptografia de VM


Por padrão, os **Administradores de sistema** e os **Administradores de organização** têm os direitos necessários para exibir os recursos de armazenamento do VDC de organização e se as VMs e os discos estão criptografados. Os **Autores do vApp** podem visualizar o status de criptografia de uma máquina virtual e seus discos na página **Detalhes** da máquina virtual. Para obter mais informações sobre funções e direitos, consulte [Funções predefinidas e seus direitos](#).


## Exibir máquinas virtuais

Você pode visualizar as máquinas virtuais que são autônomas ou que fazem parte de um vApp. Você pode visualizar máquinas virtuais no modo de exibição de grade ou no modo de exibição de cartão.


### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Escolha uma das opções a seguir.

- Para visualizar as máquinas virtuais em uma exibição de grade, clique no 

- Para exibir as máquinas virtuais em uma exibição de grade, clique no .


A lista de máquinas virtuais aparece em um modo de exibição de grade ou como uma lista de cartões.

- 3 (Opcional) Organize a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 4 (Opcional) No modo de exibição de grade, clique no  à esquerda de uma máquina virtual para visualizar as ações que podem ser executadas para a máquina virtual selecionada.  
Por exemplo, você pode encerrar uma máquina virtual.
- 5 Para acessar a interface do sistema operacional convidado da máquina virtual, clique no ícone da área de trabalho no canto superior direito do modo de exibição de cartão.
- 6 Para exibir e editar os detalhes de uma máquina virtual, clique em **Detalhes**.

## Criar uma nova máquina virtual independente

Você pode criar uma nova máquina virtual independente.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 Clique em **Nova VM**.
- 4 Insira o nome e o nome do computador da máquina virtual.

---

**Importante** O nome do computador pode conter apenas caracteres alfanuméricos e hifens. Um nome de computador não pode consistir somente em dígitos nem conter espaços.

---

- 5 (Opcional) Insira uma descrição significativa.
- 6 Selecione se deseja que a máquina virtual seja ligada imediatamente após sua criação.

## 7 Selecione como você deseja implantar a máquina virtual.

Opção	Ação
<b>Novo</b>	<p>Implante uma nova máquina virtual com configurações personalizáveis.</p> <ul style="list-style-type: none"> <li>a Selecione uma família de sistemas operacionais e um sistema operacional.</li> <li>b (Opcional) Selecione uma imagem de inicialização.</li> <li>c (Opcional) Selecione uma política de posicionamento de VM e uma política de dimensionamento de VM.</li> </ul> <p>Os menus suspensos de políticas de posicionamento e dimensionamento de VM são visíveis somente quando o provedor de serviços as publicou no VDC de organização.</p> <ul style="list-style-type: none"> <li>d (Opcional) Selecione o tamanho da máquina virtual nas opções de dimensionamento predefinidas ou clique em <b>Opções de Dimensionamento Personalizadas</b> para inserir o número de CPUs virtuais, os núcleos por soquete e as configurações de memória manualmente.</li> </ul> <p>Se você selecionar uma política de dimensionamento de VM que define o tamanho da VM, essa opção não estará visível.</p> <p>Os tamanhos predefinidos da máquina virtual são: <b>Pequeno, Médio e Grande</b>.</p> <ul style="list-style-type: none"> <li>e Especifique as configurações de armazenamento para a máquina virtual, como a política de armazenamento e o tamanho em GB.</li> <li>f Especifique as configurações de rede para a máquina virtual, como rede, modo de IP, endereço IP e NIC primário.</li> </ul>
<b>Modelo de origem</b>	<p>Implante uma máquina virtual de um modelo que você seleciona no catálogo de modelos.</p> <ul style="list-style-type: none"> <li>a Selecione um modelo da máquina virtual na lista de modelos disponíveis.</li> <li>b (Opcional) Selecione uma política de posicionamento de VM e uma política de dimensionamento de VM.</li> </ul> <p>Os menus suspensos de políticas de posicionamento e dimensionamento de VM são visíveis somente quando o provedor de serviços as publicou no VDC de organização. Se o modelo selecionado tiver políticas atribuídas, talvez você esteja limitado às políticas de modelo predefinidas.</p> <ul style="list-style-type: none"> <li>c (Opcional) Selecione para usar uma política de armazenamento personalizada e selecione a política de armazenamento a ser usada no menu suspenso <b>Política de armazenamento personalizada a ser usada</b>.</li> <li>d Leia e aceite o contrato de licença de usuário final, se houver algum.</li> </ul>

## 8 Clique em **OK** para salvar as configurações da máquina virtual e iniciar o processo de criação.

Você pode ver o cartão da máquina virtual no catálogo. Até que a máquina virtual seja criada, seu estado é exibido como Ocupada.

## Provisionamento rápido de máquinas virtuais

O provisionamento rápido economiza tempo ao usar clones vinculados em operações de provisionamento de máquinas virtuais.

Um clone vinculado é uma duplicata de uma máquina virtual que usa o mesmo disco virtual que o original com uma cadeia de discos delta para rastrear as diferenças entre o original e o clone. Se você desativar o provisionamento rápido, todas as operações de provisionamento resultarão em clones completos.

Um clone vinculado não pode existir em um centro de dados ou armazenamento de dados diferente do vCenter Server da máquina virtual original.

Quando você provisiona rapidamente uma VM, o VMware Cloud Director cria uma máquina virtual de sombra para oferecer suporte à criação de clones vinculados em centros de dados e armazenamentos de dados do vCenter Server para as máquinas virtuais que estão associadas a um modelo de vApp específico.

Uma máquina virtual de sombra é uma cópia exata da máquina virtual original. A máquina virtual de sombra é criada no centro de dados e no armazenamento de dados onde o clone vinculado é criado.

---

**Importante** A consolidação no local de uma VM com provisionamento rápido não é compatível com contêineres de armazenamento que empregam instantâneos nativos. Datastores ativados por VVOLs e VAAI usam instantâneos nativos, assim não é possível consolidar as VMs com provisionamento rápido implantadas em um desses contêineres de armazenamento. Se você precisa consolidar uma VM com provisionamento rápido implantada em um datastore ativado por VVOLs ou VAAI, é necessário realocá-la para um contêiner de armazenamento diferente.

---

## Abrindo um console de máquina virtual

Acessar seu console da máquina virtual permite que você visualize informações sobre a máquina virtual, trabalhe com o sistema operacional convidado e realize operações que afetam o sistema operacional convidado.

### Pré-requisitos

A máquina virtual está ligada.

## Instalar o VMware Remote Console num cliente

O VMware Remote Console fornece uma interação incorporada de convidado e usuário em todas as máquinas virtuais que são provisionadas e gerenciadas pelo VMware Cloud Director. Esta seção detalha as tarefas necessárias para instalar o VMware Remote Console no Windows, no Apple OS X e no Linux.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Usuário de vApp** ou um conjunto equivalente de direitos.

## Procedimentos

### 1 Baixe o instalador.

- Navegue até a página de download do VMware Remote Console e selecione o link para a sua plataforma.

[www.vmware.com/go/download-vmrc](http://www.vmware.com/go/download-vmrc)

- Na tela do painel **Centro de Dados Virtual** no VMware Cloud Director Tenant Portal, clique no cartão do centro de dados virtual que você deseja explorar. Selecione uma máquina virtual e, no menu **Ações**, selecione **Baixar VMRC**.

### 2 Execute a instalação da plataforma.

- Se você estiver usando o Windows, clique duas vezes no instalador do `.msi` e siga os prompts.
- Se você estiver usando o Linux, faça login com privilégios **raiz**, execute o instalador `.bundle` e siga os prompts.
- Se você estiver usando o SO Mac, clique duas vezes no `.dmg` para abri-lo e clique duas vezes no ícone do VMware Remote Console dentro para copiar para a pasta Aplicativos.

## Resultados

Após a instalação, o VMware Remote Console é aberto quando você clica em identificadores de recursos uniformes (URIs) que começam com o esquema `vmrc://`. O VMware Workstation, o Player e o Fusion também lidam com o esquema de URI `vmrc://`.

## Abrir um console remoto de máquina virtual

Você pode abrir um console da máquina virtual usando o VMware Remote Console por meio do portal do tenant do VMware Cloud Director.

### Pré-requisitos

- Verifique se o VMware Remote Console está instalado no seu sistema local.
- Verifique se a máquina virtual selecionada está em um estado ligado.
- Esta operação exige direitos incluídos na função predefinida de **Usuário de vApp** ou um conjunto equivalente de direitos.

## Procedimentos

### 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.

### 2 Clique em para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.

- 3 No menu **Ações** da máquina virtual, selecione **Iniciar Console Remoto da VM**.

---

**Observação** Se você não tiver o VMware Remote Console instalado, uma janela pop-up solicitará que você instale o VMware Remote Console ou use o console da Web.

---

#### Resultados

O console da máquina virtual é aberto como um console remoto virtual externo.

---

**Observação** Quando você se conecta a uma máquina virtual do VMware Cloud Director usando o VMware Remote Console, está limitado apenas à interação do console (enviando o Ctrl+Alt+Del). Não é possível executar operações do dispositivo, operações de ligar/desligar ou o gerenciamento de configurações.

---


## Abrir o console Web

Você pode se conectar ao console de uma máquina virtual mesmo se não tiver o VMware Remote Console instalado no sistema local.

#### Pré-requisitos

- Verifique se a máquina virtual está ligada.
- Esta operação exige direitos incluídos na função predefinida de **Usuário de vApp** ou um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual, selecione **Iniciar Console da Web**.

#### Resultados

O console da máquina virtual é aberto em uma nova guia do navegador usando o VMware HTML Console SDK.

#### Próximo passo

Clique em qualquer lugar na janela do console para começar a usar o mouse, o teclado e outros dispositivos de entrada no console.

---

**Observação** Para obter informações sobre os teclados internacionais compatíveis, consulte a Documentação do VMware HTML Console SDK, em <https://www.vmware.com/support/developer/html-console/>.

---

## Operações para ligar ou desligar em máquinas virtuais

Você pode realizar operações de energia em máquinas virtuais, como ligar ou desligar uma máquina virtual, suspender ou redefinir uma máquina virtual ou encerrar o sistema operacional convidado de uma máquina virtual.

### Ligar uma máquina virtual


Ligar uma máquina virtual é o equivalente a ligar uma máquina física.

Você não pode ligar uma máquina virtual que tenha a personalização de convidado habilitada, a menos que essa máquina virtual tenha uma versão atual do VMware Tools instalada.

#### Pré-requisitos

A máquina virtual está desligada.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja iniciar, selecione **Ligar**.

#### Resultados

Uma máquina virtual ligada exibe um status Ligado em verde.


### Desligar uma máquina virtual

Desligar uma máquina virtual é o equivalente a desligar uma máquina física.

#### Pré-requisitos

A máquina virtual está ligada.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja desligar, selecione **Desligar**.

#### Resultados

Uma máquina virtual desligada exibe um status Desligado em vermelho.




## Desligar um sistema operacional convidado

Desligar o sistema operacional convidado de uma máquina virtual é o equivalente a desligar uma máquina física.

### Pré-requisitos

A máquina virtual e o sistema operacional convidado devem estar ligados.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual, selecione **Encerrar SO Convidado**.

### Resultados

O SO convidado é desligado.


## Redefinir uma máquina virtual

A redefinição de uma máquina virtual limpa o estado (memória, cache e assim por diante), mas a máquina virtual continua a ser executada. A redefinição de uma máquina virtual é o equivalente a pressionar o botão redefinir de uma máquina física. Ele inicia uma reinicialização forçada do sistema operacional sem alterar o estado de energia da máquina virtual.

### Pré-requisitos

Sua máquina virtual deve estar ligada.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja redefinir, selecione **Redefinir**.

### Resultados

O estado é limpo para a máquina virtual.

## Suspender uma máquina virtual


Suspender uma máquina virtual preserva seu estado atual gravando a memória no disco.

O recurso de suspensão e reinício é útil quando você deseja salvar o estado atual da sua máquina virtual e continuar o trabalho mais tarde desse mesmo estado.

#### Pré-requisitos

A máquina virtual está ligada.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja suspender, selecione **Suspender**.

#### Resultados

A máquina virtual é suspensa, mas seu estado é preservado.


## Descartar o estado suspenso de uma máquina virtual

Se uma máquina virtual estiver em um estado suspenso e você não precisar mais retomar o uso da máquina, poderá descartar o estado suspenso. Descartar o estado suspenso remove a memória salva e retorna a máquina para um estado desligado.

#### Pré-requisitos

Uma máquina virtual suspensa.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual, selecione **Descartar estado suspenso**.

#### Resultados

O estado é descartado e a máquina virtual é desligada.

## Ligar várias VMs

É possível ligar várias VMs ao mesmo tempo.

Você não pode ligar uma máquina virtual que tenha a personalização de convidado habilitada, a menos que essa máquina virtual tenha uma versão atual do VMware Tools instalada.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione as VMs que você deseja ligar.
- 4 No menu **Ações**, selecione **Ligar**.
- 5 Clique em **OK** para confirmar.

## Desligar várias máquinas virtuais

É possível desligar várias VMs ao mesmo tempo.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione as VMs que você deseja desligar.
- 4 No menu **Ações**, selecione **Desligar**.
- 5 Clique em **OK** para confirmar.

## Descartar o estado suspenso de várias máquinas virtuais

Se várias VMs estiverem em estado suspenso e você não precisar mais retomar seu uso, poderá descartar esse estado suspenso de todas elas de uma só vez. Essa ação de descarte remove a memória salva e retorna as VMs para um estado desligado.

### Pré-requisitos

Verifique se as VMs estão em estado suspenso.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione as VMs das quais você deseja descartar o estado suspenso.
- 4 No menu **Ações**, selecione **Descartar Estado Suspenso**.
- 5 Clique em **OK** para confirmar.

## Redefinir várias máquinas virtuais

A redefinição de várias VMs limpa simultaneamente seu estado (memória, cache e assim por diante) enquanto as VMs continuam sendo executadas.

A redefinição de uma máquina virtual é o equivalente a pressionar o botão redefinir de uma máquina física. Ele inicia uma reinicialização forçada do sistema operacional sem alterar o estado de energia da máquina virtual.

### Pré-requisitos

Verifique se as VMs estão ligadas.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione as VMs que você deseja redefinir.
- 4 No menu **Ações**, selecione **Redefinir**.
- 5 Clique em **OK** para confirmar.

## Instalar o VMware Tools numa máquina virtual

O VMware Cloud Director depende do VMware Tools para personalizar o SO convidado.


O VMware Tools melhora o gerenciamento e o desempenho da máquina virtual, substituindo drivers genéricos do sistema operacional por drivers da VMware ajustados para o hardware virtual. Você instala o VMware Tools no sistema operacional convidado. Embora o sistema operacional convidado possa ser executado sem o VMware Tools, você perde recursos e conveniência importantes.

### Pré-requisitos

- Verifique se a máquina virtual está ligada.
- Se a máquina virtual recém-criada não tiver SO convidado, você deverá instalá-la antes de poder instalar o VMware Tools.
- A personalização do convidado deve ser desativada antes da instalação do VMware Tools.
- Se a versão do VMware Tools for anterior a 7299 em uma máquina virtual no seu vApp, você deverá atualizá-la.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.

- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual na qual você deseja instalar o VMware Tools, selecione **Instalar VMware Tools**.

O VMware Tools está instalado na sistema operacional convidado de destino. Se houver um erro durante a instalação, será exibida uma mensagem de erro. Você também pode exibir o progresso da operação de instalação na janela **Tarefas**.
- 4 Para abrir o console da Web da máquina virtual, no menu **Ações**, selecione **Iniciar Console da Web**.
- 5 Siga as instruções no artigo da [Base de dados de conhecimento da VMware 1014294](#) para configurar o VMware Tools para o seu sistema operacional específico.

#### Resultados

O VMware Tools está instalado e configurado no sistema operacional convidado.

## Atualizar a versão do hardware virtual de uma máquina virtual

Você pode fazer upgrade da versão do hardware virtual de uma máquina virtual. Versões mais recentes do hardware virtual oferecem suporte a mais recursos.

Não é possível fazer downgrade da versão de hardware das máquinas virtuais em um vApp.

O VMware Cloud Director é compatível com versões de hardware, dependendo dos recursos do vSphere de suporte. A versão do hardware compatível depende da versão mais recente do hardware virtual compatível no VDC do provedor de suporte. Um **administrador de organização** ou um **administrador de sistema** pode definir a versão do hardware como uma versão anterior à mais recente versão compatível pelo hardware subjacente. O portal de tenants do VMware Cloud Director define dinamicamente a lista de versões de hardware virtual selecionáveis com base no hardware de suporte do VDC da organização ou do provedor.


Para obter informações sobre os recursos de hardware disponíveis com configurações de compatibilidade de máquina virtual, consulte *vSphere Administração da máquina virtual*.

Para obter informações sobre os produtos VMware e suas versões de hardware virtual, consulte <https://kb.vmware.com/s/article/1003746>.

#### Pré-requisitos

- Pare a máquina virtual ou o vApp que contém a máquina virtual.
- Verifique se a versão mais recente do VMware Tools está instalada nela.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual de que você deseja fazer upgrade, selecione **Fazer upgrade da versão do hardware virtual**.
- 4 Clique em **OK**.

## Resultados

O upgrade da máquina virtual para a versão mais recente é realizado.

# Editar as propriedades da máquina virtual

Você pode editar as propriedades de uma máquina virtual, incluindo o nome e a descrição da máquina virtual, as configurações de hardware e de rede, as configurações do SO convidado e assim por diante.


## Alterar as propriedades gerais de uma máquina virtual

Você pode revisar e alterar o nome, a descrição e outras propriedades gerais de uma máquina virtual.

### Pré-requisitos

Alterar propriedades, como sistema operacional, exige que a máquina seja desligada.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No cartão da máquina virtual que você deseja editar, clique em **Detalhes**.

- 4 A lista de propriedades que você pode visualizar ou editar em **Geral** é expandida por padrão.


Opção	Ação
<b>Nome da Máquina Virtual</b>	<p>Editar o nome da máquina virtual</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está ligada.</p>
<b>Nome do Computador</b>	<p>Edita o nome do computador e do host definido no sistema operacional convidado que identifica a máquina virtual em uma rede. Este campo é restrito a 15 caracteres devido a uma limitação do sistema operacional do Windows em nomes de computador.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está ligada.</p>
<b>Descrição</b>	<p>Editar a descrição opcional da máquina virtual.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está ligada.</p>
<b>Família de Sistemas Operacionais</b>	<p>Selecione uma família de sistemas operacionais no menu suspenso.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está desligada. Além disso, você não poderá editar essa propriedade se um sistema operacional já estiver presente na máquina virtual.</p>
<b>Sistema Operacional</b>	<p>Selecione um sistema operacional no menu suspenso.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está desligada. Além disso, você não poderá editar essa propriedade se um sistema operacional já estiver presente na máquina virtual.</p>
<b>Atraso na Inicialização</b>	<p>Especifique o tempo em milissegundos para atrasar a operação de inicialização.</p> <p>O tempo entre o momento em que você liga a máquina virtual e quando ela sai do BIOS e inicializa o software sistema operacional convidado pode ser curto. Você pode alterar o atraso de inicialização para fornecer mais tempo.</p>
<b>Política de Armazenamento</b>	<p>Selecione uma política de armazenamento para usar na máquina virtual no menu suspenso.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está ligada.</p>
<b>Datacenter Virtual</b>	<p>Exibir o nome do datacenter virtual ao qual esta máquina virtual pertence.</p>
<b>VMware Tools</b>	<p>Verifique se o VMware Tools está instalado na máquina virtual.</p>
<b>Versão do Hardware Virtual</b>	<p>Verifique a versão de hardware virtual da máquina virtual.</p>
<b>Atualizar para:</b>	<p>Para atualizar, selecione uma versão no menu suspenso.</p>
<b>Sincronizar horário</b>	<p>Marque a caixa de seleção para habilitar a sincronização de horário entre a máquina virtual sistema operacional convidado e o datacenter virtual no qual está sendo executada.</p>
<b>Inserir Configuração do BIOS</b>	<p>Selecione se deseja forçar a entrada na tela de configuração do BIOS na próxima vez que a máquina virtual for inicializada.</p> <p>Você pode editar essa propriedade enquanto a máquina virtual está desligada.</p>

- 5 Clique em **Salvar** ao concluir suas alterações.

## Alterar as propriedades de hardware de uma máquina virtual

Você pode revisar e alterar as propriedades de hardware de uma máquina virtual.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No cartão da máquina virtual que você deseja editar, clique em **Detalhes**.
- 4 Clique em **Hardware** para expandir a lista de propriedades de hardware que você pode visualizar e editar.

Opção	Descrição
<b>Número de CPUs virtuais</b>	<p>Edite o número de CPUs.</p> <p>O número máximo de CPUs virtuais que você pode atribuir a uma máquina virtual depende do número de CPUs lógicas no host e do tipo de sistema operacional convidado que está instalado na máquina virtual.</p>
<b>Núcleos por soquete</b>	<p>Edite os núcleos por soquete.</p> <p>Você pode configurar como as CPUs virtuais são atribuídas em termos de núcleos e núcleos por soquete. Determine quantos núcleos de CPU você deseja na máquina virtual e, em seguida, selecione o número de núcleos desejado em cada soquete, dependendo se você deseja uma única CPU de núcleo, CPU de dois núcleos, CPU de três núcleos e assim por diante.</p>
<b>Expor virtualização de CPU assistida por hardware ao SO convidado</b>	<p>Você pode expor a virtualização de CPU total ao sistema operacional convidado para que os aplicativos que exigem a virtualização de hardware possam ser executados em máquinas virtuais sem conversão binária ou paravirtualização.</p>
<b>Total de Memória</b>	<p>Edite as configurações de recursos de memória de uma máquina virtual. O tamanho da memória da máquina virtual deve ser um múltiplo de 4 MB.</p> <p>Essa configuração determina o quanto da memória do host ESXi é alocada para a máquina virtual. O tamanho da memória de hardware virtual determina a quantidade de memória disponível para os aplicativos executados na máquina virtual. Uma máquina virtual não pode se beneficiar de mais recursos de memória do que o tamanho da memória do hardware virtual configurado.</p>
<b>Adição dinâmica de memória</b>	<p>Se você habilitar a inclusão automática de memória, poderá adicionar recursos de memória a uma máquina virtual enquanto a máquina estiver ligada. Este recurso só é suportado em determinados sistemas operacionais convidados e versões de hardware de máquina virtual superiores a 7.</p>
<b>Adição dinâmica de CPU virtual</b>	<p>Se você habilitar a inclusão automática da CPU virtual, poderá adicionar CPUs virtuais à máquina virtual enquanto ela estiver ligada. Você pode adicionar apenas múltiplos do número de núcleos por soquete. Este recurso só é suportado em determinados sistemas operacionais convidados e versões de hardware de máquina virtual.</p>



Opção	Descrição
Número de soquetes	Exibir o número de soquetes. O número de soquetes é determinado pelo número de CPUs virtuais disponíveis. O número muda quando você atualiza o número de CPUs virtuais.
Mídia Removível	Exibir a mídia removível disponível, como CD/DVD e unidade de disquete conectados.

5 Em **Discos rígidos**, clique em **Adicionar** para adicionar um disco rígido.

Opção	Descrição
Tamanho	Insira o tamanho do disco rígido em MB. Você poderá aumentar o tamanho do disco rígido mais tarde.  <b>Observação</b> Você poderá aumentar o tamanho de um disco rígido existente se a máquina virtual não for um clone vinculado e não tiver snapshots.
Política	A política de armazenamento para a máquina virtual é usada por padrão. Por padrão, todos os discos rígidos conectados a uma máquina virtual usam a política de armazenamento especificada para a máquina virtual. Você pode substituir esse padrão para qualquer um desses discos ao criar uma máquina virtual ou modificar suas propriedades. A coluna Tamanho para cada disco rígido inclui um menu suspenso que lista todas as políticas de armazenamento disponíveis para esta máquina virtual.
IOPS	Selecione um IOPS específico para o disco. Use essa opção para limitar as operações de E/S por disco por segundo.
Tipo de Barramento	Selecione o tipo de barramento. As opções são <b>Paravirtual (SCSI)</b> , <b>LSI Logic Parallel (SCSI)</b> , <b>LSI Logic SAS (SCSI)</b> , <b>IDE</b> e <b>SATA</b> . Para obter mais informações sobre tipos de controlador de armazenamento e compatibilidade, consulte <i>Guia de Administração de Máquinas Virtuais do vSphere</i> .
Número de Barramento	Insira o número de barramento.
Número de Unidade	Insira o LUN para a unidade de disco rígido.

6 Em **NICs**, clique em **Adicionar** para adicionar um novo NIC.

Você pode adicionar até 10 NICs. Para obter informações sobre a quantidade de número de NICs com suporte, dependendo da versão do hardware da máquina virtual, consulte:

<http://kb.vmware.com/s/article/2051652>. O VMware Cloud Director oferece suporte à modificação de NICs da máquina virtual enquanto a máquina virtual está em execução. Para obter informações sobre os tipos de adaptadores de rede compatíveis, consulte <http://kb.vmware.com/kb/1001805>.

Opção	Descrição
NIC Primária	Um sinalizador é exibido quando o NIC primário é selecionado. Selecione um NIC primário. A configuração do NIC primário determina o gateway padrão e único para a máquina virtual. A máquina virtual pode usar qualquer NIC para se conectar a máquinas virtuais e físicas que estejam diretamente conectadas à mesma rede que o NIC, mas ela só pode usar o NIC primário para se conectar a máquinas em redes que exigem uma conexão de gateway.
NIC	Número do NIC.
Conectado	Selecione a caixa de seleção para conectar um NIC.
Rede	Selecione uma rede no menu suspenso.
Modo de IP	Selecione um modo de IP.  <b>Cuidado</b> Não defina o modo de IP como <b>Nenhum</b> se você selecionou uma rede à qual conectar a NIC.  <ul style="list-style-type: none"> <li>■ <b>Pool estático de IPs</b> Recebe um endereço IP estático do pool de IPs de rede.</li> <li>■ <b>Estático – Manual</b> Permite que você especifique manualmente um endereço IP específico. Se você selecionar essa opção, deverá digitar um endereço IP na coluna <b>Endereço IP</b>.</li> <li>■ <b>DHCP</b> Recebe um endereço IP de um servidor DHCP.</li> </ul>
Endereço MAC	No menu suspenso, selecione se deseja manter ou redefinir o endereço MAC.

7 Clique em **Salvar**.

## Alterar as propriedades de personalização do SO convidado de uma máquina virtual


A personalização do SO convidado no VMware Cloud Director é opcional para todas as plataformas. É necessário para máquinas virtuais que devem ingressar em um domínio do Windows.

Algumas das informações solicitadas nesse menu se aplicam apenas às plataformas do Windows. O painel **Personalização do SO Convidado** inclui as informações necessárias para que a máquina virtual ingresse em um domínio do Windows. Um **administrador de organização** pode especificar valores padrão para um domínio que os convidados do Windows nessa organização podem participar. Nem todas as máquinas virtuais Windows devem ingressar em um domínio, mas, na maioria das instalações corporativas, uma máquina virtual que não é membro do domínio não pode acessar muitos dos recursos de rede disponíveis.

#### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Autor de vApp** ou um conjunto equivalente de direitos.
- A personalização de convidado exige que a máquina virtual esteja executando o VMware Tools.
- Antes de poder personalizar um SO convidado do Windows, o **administrador do sistema** deve instalar os arquivos Microsoft Sysprep apropriados no grupo do servidor VMware Cloud Director. Consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.
- A personalização de sistemas operacionais convidados Linux requer que o Perl esteja instalado no convidado.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No cartão da máquina virtual que você deseja editar, clique em **Detalhes**.
- 4 Clique em **Personalização e propriedades do SO convidado** para expandir a lista de configurações do sistema operacional convidado.

Opção	Descrição
<b>Permitir personalização do convidado</b>	Selecione essa opção para habilitar a personalização do convidado.
<b>Alterar SID</b>	Selecione essa opção para alterar a ID de segurança (SID) do Windows. Essa opção é específica para máquinas virtuais que executam um sistema operacional convidado Windows. A SID é usada em alguns sistemas operacionais Windows para identificar de forma exclusiva sistemas e usuários. Se você não selecionar essa opção, a nova máquina virtual terá a mesma SID que a máquina virtual ou o modelo no qual ela se baseia. As SIDs duplicadas não causam problemas quando os computadores fazem parte de um domínio e somente contas de usuário de domínio são usadas. No entanto, se as máquinas fizerem parte de um grupo de trabalho ou contas de usuário local forem usadas, as SIDs duplicadas poderão comprometer os controles de acesso aos arquivos. Para obter mais informações, consulte a documentação do seu sistema operacional Microsoft Windows.

Opção	Descrição
<b>Permitir senha de administrador local</b>	<p>Selecione essa opção para permitir a configuração de uma senha de administrador no sistema operacional convidado.</p> <p>a Especifique uma senha para o administrador local.</p> <p>Deixar a caixa de texto <b>Especificar senha</b> em branco gera uma senha automaticamente.</p> <p>b Especifique o número de vezes que o login automático será permitido.</p> <p>Inserir um valor zero desativa o login automático como <b>administrador</b>.</p>
<b>Exigir que o administrador altere a senha no primeiro login</b>	<p>Selecione essa opção para exigir que os administradores alterem a senha do sistema operacional convidado no primeiro login. Isso é recomendado por motivos de segurança.</p>
<b>Gerar senha automaticamente</b>	<p>Selecione essa opção para permitir a geração automática de senha.</p>
<b>Permitir que esta VM ingresse em um domínio</b>	<p>Você pode selecionar essa opção para ingressar a máquina virtual em um domínio do Windows. Você pode usar o domínio da organização ou substituir o domínio da organização e inserir as propriedades do domínio.</p> <p>a Insira o nome do domínio.</p> <p>b Insira o nome de usuário e a senha.</p> <p>c Insira a unidade organizacional da conta.</p>
<b>Script</b>	<p>Você pode usar um script de personalização para modificar o sistema operacional convidado da máquina virtual. Quando você adiciona um script de personalização a uma máquina virtual, o script é chamado apenas na personalização inicial e força a nova personalização. Se você definir o parâmetro de linha de comando <code>precustomization</code>, o script será chamado antes do início da personalização do convidado. Se você definir o parâmetro de linha de comando <code>postcustomization</code>, o script será chamado após a conclusão da personalização do convidado.</p> <ul style="list-style-type: none"> <li>■ Clique no botão carregar abaixo da caixa de texto do script para navegar até um script de personalização na máquina local.</li> <li>■ Digite o script de personalização diretamente na caixa de texto <b>Arquivo de script</b>.</li> </ul> <p>Um script de personalização que você insere diretamente na caixa de texto <b>Arquivo de script</b> não pode conter mais de 1.500 caracteres. Para obter mais informações, consulte o artigo da Base de Conhecimento da VMware <a href="https://kb.vmware.com/kb/1026614">https://kb.vmware.com/kb/1026614</a>.</p>

5 Clique em **Salvar** ao concluir suas alterações.

## Noções básicas sobre personalização de guests

Quando você personaliza seu sistema operacional convidado, há algumas configurações e opções que devem ser conhecidas.

### Caixa de seleção Habilitar personalização de guest

Essa caixa de seleção encontra-se na guia **Personalização do SO guest**, na página **Propriedades** da máquina virtual. O objetivo da personalização do guest é configurar com base nas opções selecionadas na página **Propriedades**. Se essa caixa de seleção estiver marcada, a personalização e a repersonalização dos guests são executadas quando necessárias.

Esse processo é necessário para o funcionamento de todos os recursos de personalização de guest, como o nome do computador, configurações de rede, configuração e expiração do administrador e senhas de raiz, alteração de SID para sistemas operacionais Windows e assim por diante. Essa opção deve ser selecionada para que o recurso **Ligar e forçar repersonalização** funcione.

Se a caixa de seleção estiver marcada e os parâmetros de configuração da máquina virtual no VMware Cloud Director estiverem fora de sincronia com as configurações no sistema operacional guest, a guia **Perfil** na página **Propriedades** das máquinas virtuais exibirá que a configuração está fora de sincronia com o sistema operacional guest e a máquina virtual precisa de personalização do guest.

### Comportamento de personalização de guest para vApps e máquinas virtuais

As caixas de seleção estão desmarcadas.

- **Habilitar personalização de guests**
- Em SOs guest do Windows, **Alterar SID**
- **Redefinição da senha**

Se você deseja realizar uma personalização (ou fez alterações nas configurações de rede que precisam ser refletidas no sistema operacional guest), pode marcar a caixa de seleção **Habilitar personalização de guest** e definir as opções na guia **Personalização do SO guest** da página **Propriedades** da máquina virtual. Quando máquinas virtuais de modelos vApp são usadas para criar um vApp e, em seguida, adicionar uma máquina virtual, os modelos vApp atuam como blocos de construção. Quando você adiciona máquinas virtuais do catálogo a um novo vApp, as máquinas virtuais são habilitadas para personalização de guest por padrão. Quando você salva um modelo vApp de um catálogo como um vApp, as máquinas virtuais serão habilitadas para personalização de guest somente se a caixa de seleção **Habilitar personalização de guest** estiver marcada.

Esses são os valores padrão das configurações de personalização do guest:

- A caixa de seleção **Habilitar personalização de guest** é a mesma que a máquina virtual de origem no seu catálogo.
- Para máquinas virtuais guest do Windows, **Alterar SID** é o mesmo que a máquina virtual de origem no seu catálogo.
- A configuração de redefinição de senha é igual à máquina virtual de origem no seu catálogo.

Você pode desmarcar a caixa de seleção **Habilitar personalização de guest** se necessário antes de iniciar o vApp.

Se máquinas virtuais em branco, que estão pendentes de instalação do sistema operacional guest, forem adicionadas a um vApp, a caixa de seleção **Habilitar personalização de guest** será desmarcada por padrão porque essas máquinas virtuais ainda não estão prontas para personalização.

Depois de instalar o sistema operacional guest e o VMware Tools, você pode desligar as máquinas virtuais, parar o vApp e marcar a caixa de seleção **Habilitar personalização de guest** e iniciar o vApp e as máquinas virtuais para realizar a personalização do guest.

Se o nome da máquina virtual e as configurações de rede forem atualizadas em uma máquina virtual que foi personalizada, da próxima vez em que você ligar a máquina virtual, ela será repersonalizada, o que ressincroniza a máquina virtual guest com o VMware Cloud Director.

## Ligar e forçar nova personalização de uma máquina virtual

Você pode ligar uma máquina virtual e forçar nova personalização dessa máquina.


Se as configurações em uma máquina virtual não estiverem sincronizadas com o VMware Cloud Director ou se uma tentativa de executar uma personalização de convidado falhar, você poderá forçar nova personalização da máquina virtual.

Verifique se o aplicativo que está em execução na máquina virtual oferece suporte a uma nova personalização. Se você alterar um controlador de domínio usando o Microsoft Sysprep e também alterar o SID, a máquina virtual pode estar danificada. Para reduzir o risco de danificar a máquina virtual, crie um snapshot antes de repersonalizá-la.

### Pré-requisitos

- Você deve ser um administrador da organização.
- A máquina virtual deve estar desligada.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Energia** da máquina virtual que você deseja ligar e personalizar, selecione **Ligar e Forçar Nova Personalização**.

### Resultados

A máquina virtual é repersonalizada e ligada.

## Alterar as propriedades avançadas de uma máquina virtual

Nas configurações **Avançadas**, você pode definir as configurações de alocação de recursos (compartilhamentos, reserva e limite) para determinar a quantidade de CPU, memória e recursos de armazenamento fornecidos para uma máquina virtual.

Use as configurações de alocação de recursos (compartilhamentos, reserva e limite) para determinar a quantidade de recursos de CPU, memória e armazenamento fornecidos para uma máquina virtual.

### **Compartilhamentos de alocação de recursos**

Compartilhamentos especificam a importância relativa de uma máquina virtual em um datacenter virtual. Se uma máquina virtual tiver duas vezes mais compartilhamentos de um recurso que outra máquina virtual, ela terá direito a consumir duas vezes mais desse recurso quando essas duas máquinas virtuais estiverem competindo por recursos. Os compartilhamentos são normalmente especificados como Alto, Normal ou Baixo, e esses valores especificam valores de compartilhamento com uma proporção de 4:2:1, respectivamente. Você também pode selecionar Personalizado para atribuir um número específico de compartilhamentos (que expressa um peso proporcional) a cada máquina virtual. Ao atribuir compartilhamentos a uma máquina virtual, você sempre especifica a prioridade para essa máquina virtual em relação a outras máquinas virtuais ligadas.

### **Reserva de alocação de recursos**

Especifica a alocação mínima garantida para uma máquina virtual. O VMware Cloud Director permite que você ligue uma máquina virtual somente se houver recursos não reservados suficientes para satisfazer a reserva da máquina virtual. O datacenter virtual garante essa quantidade, mesmo quando seus recursos estão muito carregados. A reserva é expressa em unidades concretas (megahertz ou megabytes).

Por exemplo, suponha que você tenha 2 GHz disponíveis e especifique uma reserva de alocação de recursos de 1 GHz para a máquina virtual 1 e 1 GHz para a máquina virtual 2. Agora, cada máquina virtual tem a garantia de obter 1 GHz se ela precisar. No entanto, se a máquina virtual 1 estiver usando apenas 500 MHz, a máquina virtual 2 poderá usar 1,5 GHz.

Padrões de reserva para 0. Você poderá especificar uma reserva se precisar garantir que as quantidades mínimas necessárias de CPU ou memória estejam sempre disponíveis para a máquina virtual.

### **Limite de alocação de recursos**

Especifica um limite superior para recursos de CPU e memória que podem ser alocados para uma máquina virtual. Um datacenter virtual pode alocar mais do que a reserva para uma máquina virtual, mas nunca aloca mais do que o limite, mesmo se houver recursos não utilizados no sistema. O limite é expresso em unidades concretas (megahertz ou megabytes).


Os limites de recursos de CPU e memória padrão são ilimitados. Quando o limite de memória é ilimitado, a quantidade de memória configurada para a máquina virtual quando ela foi criada torna-se seu limite efetivo na maioria dos casos.

Na maioria dos casos, não é necessário especificar um limite. Se você especificar um limite, poderá perder recursos ociosos. O sistema não permite que uma máquina virtual use mais recursos do que o limite, mesmo quando o sistema não está sendo completamente utilizado e recursos ociosos estão disponíveis. Especifique um limite somente se você tiver bons motivos para fazer isso.

### Pré-requisitos

- Um datacenter virtual do pool de reservas.
- Certifique-se de que uma determinada quantidade de memória para uma máquina virtual seja fornecida pelo datacenter virtual.
- Garanta que uma determinada máquina virtual sempre seja alocada uma porcentagem maior dos recursos do datacenter virtual do que outras máquinas virtuais.
- Defina um limite superior nos recursos que podem ser alocados para uma máquina virtual.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No cartão da máquina virtual que você deseja editar, clique em **Detalhes**.
- 4 Clique em **Avançado e Editar**.
- 5 Defina os compartilhamentos de alocações de recursos para as configurações de CPU selecionando uma opção no menu suspenso **Prioridade**.

Opção	Descrição
Baixo	Aloca compartilhamentos de 500 por CPU virtual.
Normal	Aloca compartilhamentos de 1000 por CPU virtual.
Alto	Aloca compartilhamentos de 2000 por CPU virtual.
Personalizado	<p>Permite atribuir um número específico de compartilhamentos inserindo o número de compartilhamentos (que expressa um peso proporcional) a cada máquina virtual.</p> <p>Ao atribuir compartilhamentos a uma máquina virtual, você sempre especifica a prioridade para essa máquina virtual em relação a outras máquinas virtuais ligadas.</p>



- 6 Especifique a reserva para as configurações de CPU inserindo a reserva em MHz e, opcionalmente, o limite para as configurações de CPU em MHz.

Opção	Descrição
Ilimitado	A opção de recurso de CPU padrão.
Máximo	Especifique um limite superior para os recursos da CPU que podem ser alocados para uma máquina virtual em MHz.

- 7 Defina os compartilhamentos de alocações de recursos para as configurações de memória selecionando uma opção no menu suspenso **Prioridade**.

Opção	Descrição
Baixo	Aloca cinco compartilhamentos por megabyte de memória de máquina virtual configurada.
Normal	Aloca 10 compartilhamentos por megabyte de memória de máquina virtual configurada.
Alto	Aloca 20 compartilhamentos por megabyte de memória de máquina virtual configurada.
Personalizado	Permite que você atribua um número específico de compartilhamentos inserindo o número de compartilhamentos.

- 8 Especifique a reserva para as configurações de memória em MB e, opcionalmente, o limite para as configurações de memória em MB.

Opção	Descrição
Ilimitado	A opção de recurso de memória padrão.
Máximo	Especifique um limite superior para a reserva de memória que pode ser alocada a uma máquina virtual.

- 9 Clique em **Salvar**.

## Inserir Mídia


Você pode inserir mídias, como imagens de CD/DVD de catálogos, para uso em um sistema operacional convidado de uma máquina virtual. Você pode usar esses arquivos de mídia para instalar um sistema operacional na máquina virtual, vários aplicativos, drivers e assim por diante.

### Pré-requisitos

Você tem acesso a um catálogo com arquivos de mídia.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.

- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 Selecione a máquina virtual à qual você deseja adicionar a mídia.
- 4 No menu **Ações**, selecione **Inserir Mídia**.
- 5 Na janela **Inserir CD**, selecione o arquivo de mídia a ser inserido na máquina virtual.
- 6 Clique em **Inserir**.


## Ejetar Mídia

Depois de concluir o uso de um CD ou DVD na máquina virtual, você pode ejetar o arquivo de mídia.

### Pré-requisitos

Um arquivo de mídia foi inserido anteriormente na máquina virtual.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 Selecione a máquina virtual da qual você deseja ejetar a mídia.
- 4 No menu **Ações**, selecione **Ejetar Mídia**.

### Resultados

O arquivo de mídia é ejetado.

## Copiar uma máquina virtual para um vApp diferente


É possível copiar uma máquina virtual para outro vApp. Quando você copia uma máquina virtual, a máquina virtual original permanece no vApp de origem.

Quando você copia uma máquina virtual, os snapshots não são incluídos na cópia.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Autor de vApp** ou um conjunto equivalente de direitos.
- Desligue a VM.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja copiar, selecione **Copiar para**.
- 4 Selecione o vApp de destino para o qual você deseja copiar a máquina virtual e clique em **Avançar**.
- 5 Configure os recursos, como o nome da máquina virtual e o nome do computador e, opcionalmente, a política de armazenamento e as NICs, e clique em **Avançar**.

---

**Importante** O nome do computador pode conter apenas caracteres alfanuméricos e hífens. Ele não pode consistir apenas em dígitos e não pode conter espaços.

---

- 6 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluído**.

## Mover uma máquina virtual para um vApp diferente

Você pode mover uma máquina virtual para outro vApp. Quando você move uma VM, o VMware Cloud Director remove a VM original do vApp de origem.

Quando você move uma máquina virtual para um vApp diferente, os snapshots que você tirou são perdidos.

Mover as VMs entre diferentes vApps baseia-se no VMware vSphere® vMotion® e no Enhanced vMotion Compatibility (EVC). Você pode mover uma VM para um vApp diferente que pertença ao mesmo ou a outro VDC de organização na mesma organização. O VDC de organização pode estar no mesmo VDC de provedor ou em um VDC de provedor diferente.

Enquanto você estiver movendo uma máquina virtual para um vApp diferente, poderá realizar reconfigurações como alterar a rede e o perfil de armazenamento.


**Tabela 2-1. Reconfigurações durante transferências de máquina virtual e estados de máquina Virtual**

Reconfiguração	O estado da VM se o vApp de destino estiver no mesmo VDC de organização	O estado da VM se o vApp de destino estiver no outro VDC de organização dentro do mesmo VDC de provedor
alterar a rede	desligada	N/A
remover a rede	ligada ou desligada	N/A
alterar o perfil de armazenamento	ligada ou desligada	desligada

### Pré-requisitos

- Verifique se você tem direitos de **Autor do vApp** ou um conjunto equivalente de direitos.
- Verifique se os recursos subjacentes do vSphere suportam vMotion e EVC. Para obter informações sobre os requisitos e as limitações de vMotion e EVC, consulte *vCenter Server e gerenciamento de host*.
- Se você quiser alterar a rede da VM ou o perfil de armazenamento, verifique se precisa desligar a VM. Consulte a tabela *Reconfigurações durante transferências da VM e estados da VM*.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina que você deseja mover, selecione **Mover para**.
- 4 Selecione o vApp de destino e clique em **Avançar**.
- 5 Configure os recursos, como o nome da VM e o nome do computador e, opcionalmente, a política de armazenamento e as NICs, e clique em **Avançar**.

---

**Importante** O nome do computador pode conter apenas caracteres alfanuméricos e hífens. Ele não pode consistir apenas em dígitos e não pode conter espaços.

---

- 6 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluído**.

## Afinidade e antiafinidade da máquina virtual

As regras de afinidade e antiafinidade permitem que você espalhe um grupo de máquinas virtuais em diferentes hosts ESXi ou mantenha um grupo de máquinas virtuais em um host ESXi específico.


Uma regra de afinidade coloca um grupo de máquinas virtuais em um host específico para que você possa facilmente auditar o uso dessas máquinas virtuais. Uma regra de antiafinidade coloca um grupo de máquinas virtuais em hosts diferentes, o que impede que todas as máquinas virtuais falhe ao mesmo tempo no caso de um único host falhar.

Se as regras de afinidade ou antiafinidade não puderem ser atendidas, isso impedirá que as máquinas virtuais adicionadas à regra sejam ligadas.

### Visualizar regras de afinidade e antiafinidade

Você pode visualizar as regras de afinidade e antiafinidade existentes e as propriedades delas, como as máquinas virtuais afetadas pelas regras e se as regras estão ativadas ou não.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Regras de Afinidade**.
- 2 (Opcional) Clique no ícone **Editor de grade** (  ) e selecione os detalhes sobre as regras que você deseja visualizar.

## Resultados

Você vê a lista das regras de afinidade e antiafinidade existentes, das máquinas virtuais e do status habilitado de cada regra.

## Criar uma regra de afinidade

Crie uma regra de afinidade para colocar um grupo específico de máquinas virtuais em um único host para que você possa auditar o uso dessas máquinas virtuais.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Regras de Afinidade**.
- 2 Em **Regras de Afinidade**, clique em **Novo**.
- 3 Insira um nome para a regra.
- 4 Desmarque **Habilitado** para criar a regra sem habilitá-la.  
Por padrão, a caixa de seleção é marcada, e as regras serão ativadas depois que você as criar.
- 5 Deixe a caixa de seleção **Obrigatório** selecionada.  
Por padrão, cada regra de afinidade é necessária. Isso significa que, se a regra não puder ser atendida, as máquinas virtuais adicionadas à regra não serão ligadas.
- 6 Selecione as máquinas virtuais que você deseja adicionar à regra de afinidade.
- 7 Clique em **Salvar**.

## Resultados

O VMware Cloud Director coloca as máquinas virtuais associadas à regra de afinidade em um único host.

## Criar uma regra de antiafinidade

Crie uma regra de antiafinidade para colocar um grupo específico de máquinas virtuais entre vários hosts para evitar falhas simultâneas dessas máquinas virtuais no caso de falha em um único host.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Regras de Afinidade**.
- 2 Em **Regras Antiafinidade**, clique em **Novo**.
- 3 Insira um nome para a regra.
- 4 Desmarque **Habilitado** para criar a regra sem habilitá-la.  
Por padrão, a caixa de seleção é marcada, e as regras serão ativadas depois que você as criar.
- 5 Deixe a caixa de seleção **Obrigatório** selecionada.  
Por padrão, cada regra de antiafinidade é necessária. Isso significa que, se a regra não puder ser atendida, as máquinas virtuais adicionadas à regra não serão ligadas.
- 6 Selecione as máquinas virtuais a serem adicionadas à regra de anti-afinidade.
- 7 Clique em **Salvar**.

## Resultados

O VMware Cloud Director coloca as máquinas virtuais associadas à regra de antiafinidade entre vários hosts.

## Editar uma regra de afinidade ou antiafinidade

Você pode editar uma regra de afinidade ou antiafinidade para ativar ou desativar a regra, adicionar ou remover máquinas virtuais, alterar o nome da regra ou a preferência da regra.

## Pré-requisitos

Esta operação requer o direito de `Organization vDC: VM-VM Affinity Edit`. Este direito está incluído nas funções predefinidas de **Autor do catálogo**, **Autor de vApp** e **Administrador da organização**.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Regras de Afinidade**.
- 2 Clique no botão de opção ao lado do nome da regra que você deseja editar e clique em **Editar**.
- 3 Edite as propriedades da regra.
  - a Altere o nome da regra conforme necessário.
  - b Selecione se deseja ativar ou desativar a regra.
  - c Deixe a caixa de seleção **Obrigatório** selecionada.
  - d Adicione mais máquinas virtuais ou remova máquinas virtuais.
- 4 Clique em **Salvar**.

## Excluir uma regra de afinidade ou antiafinidade

Se não quiser mais usar uma regra de afinidade ou antiafinidade, você poderá excluí-la.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Regras de Afinidade**.
- 2 Clique no botão de opção ao lado do nome da regra que você deseja excluir e clique em **Excluir**.
- 3 Para confirmar que você deseja excluir a regra, clique em **OK**.

### Resultados

O VMware Cloud Director exclui a regra de afinidade ou antiafinidade.

## Monitorar máquinas virtuais


Se o administrador do VMware Cloud Director tiver habilitado o recurso para monitorar máquinas virtuais, você poderá visualizar o gráfico de monitoramento no portal do tenant.

Use-o para compreender o status de uma determinada máquina virtual ao longo do tempo (dias, semanas ou meses).

### Pré-requisitos

Este recurso só estará disponível se o administrador do VMware Cloud Director o tiver habilitado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 Selecione a máquina virtual que você deseja monitorar e clique em **Detalhes**.
- 4 Clique em **Gráfico de monitoramento** para expandir a exibição de monitoramento.  
O gráfico de monitoramento é exibido.

5

## 6 Selecione uma opção de métrica para monitorar máquinas virtuais.

A lista no menu suspenso **Métrica** varia dependendo das opções do **administrador do sistema**. Você vê algumas ou todas as opções.

Métrica	Descrição
Disco provisionado mais recente	Especificado em KB. Escolha o modo de exibição de dia, semana ou mês.
Média de leitura do disco	Especificado como uma porcentagem. Escolha o modo de exibição de dia, semana ou mês.
Média de gravação em disco	Especificado como uma porcentagem. Escolha o modo de exibição de dia, semana ou mês.
Uso médio da CPU	Especificado como uma porcentagem. Escolha o modo de exibição de dia, semana ou mês.
Uso médio da CPU em MHz	Especificado em MHz. Escolha o modo de exibição de dia, semana ou mês.
Uso máximo da CPU	Especificado como uma porcentagem. Escolha o modo de exibição de dia, semana ou mês.
Média de uso de mems	Especificado como uma porcentagem. Escolha o modo de exibição de dia, semana ou mês.
Disco usado mais recente	Especificado em KB. Escolha o modo de exibição de dia, semana ou mês.

Um novo gráfico é exibido todas as vezes que você seleciona um valor diferente na lista.

## 7 (Opcional) Altere o intervalo de tempo para a coleção de métricas.

## 8 Clique em **Atualizar**.

## 9 Para salvar as alterações, clique em **Salvar**.

# Como trabalhar com instantâneos

Os instantâneos preservarão o estado e os dados de uma máquina virtual no momento em que o instantâneo for tirado. Quando você tira um instantâneo de uma máquina virtual, ela não é afetada, e apenas uma imagem dela em um determinado estado é copiada e armazenada. Os instantâneos são úteis quando você deve reverter repetidamente para o mesmo estado da máquina virtual, mas não deseja criar várias máquinas virtuais.

Os instantâneos são úteis como uma solução de curto prazo para teste de software com efeitos desconhecidos ou potencialmente prejudiciais. Por exemplo, você pode usar um instantâneo como um ponto de restauração durante um processo linear ou interativo, como a instalação de pacotes de atualização ou durante um processo de ramificação, como a instalação de versões diferentes de um programa.



Convém usar um instantâneo ao fazer upgrade do sistema operacional de uma máquina virtual. Por exemplo, antes de fazer upgrade da máquina virtual, você tira um instantâneo para preservar o point-in-time antes do upgrade. Se não houver problemas durante o upgrade, você poderá optar por remover o instantâneo, e isso confirmará as alterações feitas durante o upgrade. No entanto, se você tiver um problema, poderá reverter para o instantâneo, que voltará para o estado da máquina virtual salvo antes do upgrade.

Com VMware Cloud Director, você só pode ter um instantâneo de uma máquina virtual. Toda tentativa de tirar um novo instantâneo de uma máquina virtual exclui o anterior.

## Tirar um snapshot de uma máquina virtual

É possível tirar um snapshot de uma máquina virtual. Depois de tirar o snapshot, você pode reverter a máquina virtual para esse snapshot ou removê-lo.

### Pré-requisitos


Verifique se a máquina virtual não está conectada a um disco nomeado.

---

**Observação** Snapshots não capturam configurações de NIC.

---

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual da qual você deseja tirar um snapshot, selecione **Criar Snapshot**.

Tirar um snapshot de uma máquina virtual substitui o snapshot existente, se houver algum.

- 4 (Opcional) Selecione se deseja fazer o snapshot da memória da máquina virtual.

Quando você captura o estado de memória da máquina virtual, o snapshot mantém o estado ativo da máquina virtual. Snapshots de memória criam um snapshot em um momento preciso, por exemplo, para atualizar o software que ainda está funcionando. Se você tirar um snapshot de memória, e a atualização não for concluída conforme o esperado ou se o software não atender às suas expectativas, você poderá reverter a máquina virtual ao seu estado anterior.

Quando você captura o estado da memória, os arquivos da máquina virtual não exigem desativação. Se você não capturar o estado da memória, o snapshot não salvará o estado ativo da máquina virtual, e os discos terão uma falha consistente, a menos que você os desative.

- 5 (Opcional) Selecione se deseja desativar o sistema de arquivos convidado.

Essa operação requer que o VMware Tools esteja instalado na máquina virtual. Quando você desativa uma máquina virtual, o VMware Tools desativa o sistema de arquivos dessa

máquina virtual. Uma operação de desativação garante que um disco de snapshot represente um estado consistente dos sistemas de arquivos do convidado. Snapshots desativados são apropriados para backups automáticos ou periódicos. Por exemplo, se você não tem conhecimento das atividades da máquina virtual, mas deseja reverter vários backups recentes, é possível desativar os arquivos.

Não é possível desativar máquinas virtuais com discos de grande capacidade.

6 Clique em **OK**.

#### Resultados

O snapshot permite que você reverta sua máquina virtual para o snapshot mais recente.


## Converter uma máquina virtual para um snapshot

Você pode reverter uma máquina virtual para o estado em que ela estava quando o snapshot foi criado.

#### Pré-requisitos

A máquina virtual tem um snapshot.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja reverter para um snapshot, selecione **Reverter para Snapshot**.
- 4 Clique em **OK**.

#### Resultados

A máquina virtual é revertida para o snapshot salvo.

## Excluir um snapshot de uma máquina virtual


Você pode remover um snapshot de uma máquina virtual.

Ao remover um snapshot, você exclui o estado da máquina virtual que você removeu e não pode retornar a esse estado novamente. A remoção de um snapshot não afeta o estado atual da máquina virtual.

#### Pré-requisitos

Uma máquina virtual com um snapshot armazenado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual para a qual você deseja remover o snapshot, selecione **Remover Snapshot**.
- 4 Clique em **OK**.


## Renovar um lease de máquina virtual

Você pode renovar um lease de máquina virtual se ele for expirar em breve.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual com expiração do lease, selecione **Renovar Lease**.

### Resultados

O lease é renovado. Você pode ver o novo período de lease no campo **Lease**.

## Excluir uma máquina virtual


Você pode excluir uma máquina virtual da sua organização.

### Pré-requisitos

Sua máquina virtual deve ser desligada.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.

- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No menu **Ações** da máquina virtual que você deseja excluir, selecione **Excluir**.
- 4 Confirme a exclusão.

#### Resultados

A máquina virtual é excluída.

## Grupos de Dimensionamento Automático

Começando com o VMware Cloud Director 10.2.2, você pode dimensionar aplicativos automaticamente, dependendo do uso atual de CPU e memória.

Para obter informações sobre a configuração da solução de dimensionamento automático, consulte [Grupos de dimensionamento automática](#) no *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Dependendo de critérios predefinidos para o uso de CPU e memória, o VMware Cloud Director pode ampliar ou reduzir automaticamente o número de VMs em um grupo de dimensionamento selecionado. Para balancear a carga dos servidores configurados para executar o mesmo aplicativo, você pode usar o VMware NSX Advanced Load Balancer (Avi Networks).

As funções de **administrador do sistema** ou **administrador da organização** têm controle total sobre as VMs nos grupos de dimensionamento. As outras funções de tenant globais podem visualizar as VMs e acessar o Console Web de VMs, mas não podem excluir, editar, realizar operações de energia e assim por diante.

Se você excluir um grupo de dimensionamento, o VMware Cloud Director não excluirá as VMs existentes nesse grupo.

## Criar um grupo de dimensionamento

No VMware Cloud Director 10.2.2, seu provedor de serviços pode conceder direitos para criar grupos de dimensionamento. A quantidade de VMs em um grupo de dimensionamento muda automaticamente dependendo das condições que você definir.

Você também pode acessar grupos de dimensionamento em um centro de dados virtual (VDC) da organização selecionado.

#### Procedimentos

- 1 Na barra de navegação superior, selecione **Aplicativos** e escolha a guia **Grupos de Dimensionamento**.
- 2 Clique em **Novo Grupo de Dimensionamento**.
- 3 Selecione um VDC da organização para criar o grupo de dimensionamento.
- 4 Insira um nome e, opcionalmente, uma descrição do novo grupo de dimensionamento.

- 5 Selecione o número mínimo e máximo de VMs para o qual você deseja que o grupo se expanda e clique em **Avançar**.
- 6 Selecione um modelo de VM para as VMs no grupo de dimensionamento e uma política de armazenamento e clique em **Avançar**.
- 7 Selecione uma rede para o grupo de dimensionamento.
  - Se o seu VDC tiver o suporte do NSX-T Data Center, selecione um balanceador de carga.
  - Se quiser gerenciar o balanceador de carga sozinho ou se não houver necessidade de um balanceador de carga, selecione **Eu tenho uma rede totalmente configurada**.
- 8 Clique em **Criar Grupo e Adicionar Regras**.

#### Resultados

O VMware Cloud Director inicia a expansão inicial do grupo de dimensionamento para atingir o número mínimo de VMs.

#### Próximo passo

- [Adicionar uma regra de dimensionamento automático](#)
- Na visualização de detalhes de um grupo de dimensionamento, ao selecionar **Monitor**, você pode ver todas as tarefas relacionadas a esse grupo. Por exemplo, você pode ver o tempo de criação do grupo de dimensionamento, todas as tarefas em expansão ou redução para o grupo, as regras que iniciaram as tarefas e assim por diante.
- Exclua um grupo de dimensionamento. Quando você exclui um grupo de dimensionamento, o VMware Cloud Director não exclui as VMs existentes nesse grupo. Se quiser reduzir o número de VMs, você deverá excluí-las manualmente.

## Adicionar uma regra de dimensionamento automático

No VMware Cloud Director 10.2.2, seu provedor de serviços pode conceder direitos para criar e gerenciar grupos de dimensionamento. É possível adicionar regras que disparam a expansão ou a redução de grupos de dimensionamento.

#### Pré-requisitos

##### [Criar um grupo de dimensionamento](#)

#### Procedimentos

- 1 Na barra de navegação superior, selecione **Aplicativos** e escolha a guia **Grupos de Dimensionamento**.
- 2 Escolha um grupo de dimensionamento e selecione **Regras**.
- 3 Clique em **Adicionar Regra**.
- 4 Digite um nome para a regra.

- 5 Selecione se o grupo de dimensionamento deve ser expandido ou reduzido quando a regra entrar em vigor.
- 6 Selecione o número de VMs com base no qual você deseja que o grupo seja expandido ou reduzido quando a regra entrar em vigor.
- 7 Insira um período de resfriamento em minutos após cada dimensionamento automático no grupo.

As condições não poderão disparar outro dimensionamento até que o período de resfriamento expire. O período de resfriamento será redefinido quando qualquer uma das regras do grupo de dimensionamento entrar em vigor.

- 8 Adicione uma condição que dispare a regra.

A duração é o período no qual a condição deve ser válida para disparar a regra. Para que a regra seja disparada, todas as condições devem ser atendidas.

- 9 (Opcional) Para adicionar outra condição, clique em **Adicionar Condição**.
- 10 Clique em **Adicionar**.

# Trabalhando com vApps

# 3

Um vApp consiste em uma ou mais máquinas virtuais que se comunicam através de uma rede e usam recursos e serviços em um ambiente implantado. Um vApp pode conter várias máquinas virtuais.

Começando com o VMware Cloud Director 9.5, vApps são compatíveis com a conectividade IPv6. Você pode atribuir endereços IPv6 a máquinas virtuais conectadas a redes IPv6.

---

**Importante** Todas as etapas para trabalhar com vApps são documentadas com base no modo de exibição de cartão, pressupondo-se que você tenha mais de um centro de dados virtual. Também é possível concluir os mesmos procedimentos partindo do modo de exibição de grade, mas as etapas podem variar ligeiramente.

---

Este capítulo inclui os seguintes tópicos:



- Visualizar vApps
- Criar um novo vApp
- Criar um vApp a partir de um pacote OVF
- Adicionar um vApp de um catálogo
- Criar um vApp de um modelo de vApp
- Importar uma máquina virtual do vCenter Server como vApp
- Operações para ligar ou desligar em vApps
- Abrir um vApp
- Editar Propriedades do vApp
- Exibir um diagrama de rede do vApp
- Trabalhando com redes em um vApp
- Como trabalhar com instantâneos
- Alterar o proprietário de um vApp
- Mover um vApp para outro data center virtual
- Copiar um vApp interrompido para outro data center virtual
- Copiar um vApp ligado


- [Adicionar uma máquina virtual a um vApp](#)
- [Salvar um vApp como um modelo do vApp em um catálogo](#)
- [Baixar um vApp como um pacote OVF](#)
- [Renovar um lease de vApp](#)
- [Excluir um vApp](#)
- [Excluir vários vApps](#)


## Visualizar vApps

Você pode visualizar vApps em um modo de exibição de grade ou em um modo de exibição de cartão.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Para visualizar os vApps em um modo de exibição de grade, clique no . Para visualizá-los em um modo de exibição de cartão, clique no .
 

A lista de vApps aparece em uma grade ou como uma lista de cartões.
- 3 (Opcional) Configure o modo de exibição de grade para que ele mostre os detalhes que você deseja ver.
  - a No modo de exibição de grade, clique no ícone **Editor de grade** ().
  - b Selecione os detalhes do vApp que você deseja incluir no modo de exibição de grade marcando a caixa de seleção ao lado de cada detalhe que deseja ver.
  - c Para salvar as alterações, clique em **OK**.

Os detalhes selecionados aparecem como colunas para cada vApp.
- 4 (Opcional) No modo de exibição de grade, clique no  à esquerda de um vApp para visualizar as ações que podem ser executadas para o vApp selecionado.
 

Por exemplo, você pode encerrar um vApp.

## Criar um novo vApp

Em vez de criar um vApp com base em um modelo vApp, você pode decidir criar um vApp usando máquinas virtuais a partir de catálogos, novas máquinas virtuais ou uma combinação de ambos.



Criar um vApp exige que você forneça um nome e, opcionalmente, uma descrição do vApp. Você pode voltar e adicionar as máquinas virtuais ao vApp em uma etapa posterior.

### Pré-requisitos

Esta operação requer os direitos incluídos na função predefinida de **autor do vApp** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Selecione **Novo vApp**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo vApp.
- 4 (Opcional) Se você quiser que o vApp seja ligado durante a implantação, marque a caixa de seleção **Ligar**.

---

**Observação** O vApp poderá ser ligado somente se houver máquinas virtuais nele.

---

- 5 (Opcional) Pesquise o catálogo para que as máquinas virtuais adicionem a este vApp ou adicione uma nova máquina virtual em branco clicando em **Adicionar máquina virtual**.

Se não houver máquinas virtuais no catálogo, crie uma máquina virtual e adicione-a ao vApp.

- a Insira o nome e o nome do computador da máquina virtual.

---

**Importante** O nome do computador pode conter apenas caracteres alfanuméricos e hifens. Um nome de computador não pode consistir somente em dígitos nem conter espaços.

---

- b (Opcional) Insira uma descrição significativa.

- c Selecione como você deseja implantar a máquina virtual.

Opção	Ação
<b>Novo</b>	<p>Implante uma nova máquina virtual com configurações personalizáveis.</p> <ol style="list-style-type: none"> <li>1 Selecione uma família de sistemas operacionais e um sistema operacional.</li> <li>2 (Opcional) Selecione uma imagem de inicialização.</li> <li>3 (Opcional) Selecione uma política de posicionamento de VM e uma política de dimensionamento de VM.</li> </ol> <p>Os menus suspensos de políticas de posicionamento e dimensionamento de VM são visíveis somente quando o provedor de serviços as publicou no VDC de organização.</p> <ol style="list-style-type: none"> <li>4 Selecione o tamanho da máquina virtual ou clique em <b>Opções de Dimensionamento Personalizadas</b> para inserir manualmente as configurações de processamento, memória e armazenamento.</li> </ol> <p>Os tamanhos predefinidos da máquina virtual são pequeno, médio ou grande.</p> <ol style="list-style-type: none"> <li>5 Especifique as opções de armazenamento, como política de armazenamento e tamanho em GB.</li> <li>6 Especifique as configurações de rede para a máquina virtual, como rede, modo de IP, endereço IP e NIC primário.</li> </ol>
<b>Modelo de origem</b>	<p>Implante uma máquina virtual de um modelo que você seleciona no catálogo de modelos.</p> <ol style="list-style-type: none"> <li>1 Selecione o modelo da máquina virtual no catálogo.</li> <li>2 (Opcional) Selecione uma política de posicionamento de VM e uma política de dimensionamento de VM.</li> </ol> <p>Os menus suspensos de políticas de posicionamento e dimensionamento de VM são visíveis somente quando o provedor de serviços as publicou no VDC de organização. Se o modelo selecionado tiver políticas atribuídas, talvez você esteja limitado às políticas de modelo predefinidas.</p> <ol style="list-style-type: none"> <li>3 (Opcional) Selecione para usar uma política de armazenamento personalizada e selecione a política em <b>Política de armazenamento personalizada a ser usada</b>.</li> <li>4 Se houver um contrato de licença de usuário final disponível, você deverá revisá-lo e aceitá-lo.</li> </ol>

- d Para adicionar a máquina virtual ao vApp, clique em **OK**.

É possível ver a máquina virtual adicionada no catálogo.

- 6** (Opcional) Repita a [Etapa 5](#) para cada máquina virtual adicional que deseja criar no vApp.
- 7** Para concluir a criação do vApp, clique em **Criar**.

## Resultados

O vApp é criado. Quando o vApp é ligado, as máquinas virtuais nele são criadas e ligadas também.

## Criar um vApp a partir de um pacote OVF

Você pode criar e implantar um vApp diretamente de um pacote OVF sem criar um modelo de vApp e um item de catálogo correspondente.

O VMware Cloud Director tem suas próprias restrições para implantações do OVF que diferem das restrições no vCenter Server. Como resultado, uma implantação do OVF bem-sucedida no vCenter Server pode falhar no VMware Cloud Director.

O VMware Cloud Director oferece suporte ao OVF 1.1, mas não oferece suporte a todas as seções do esquema do OVF 1.1. Por exemplo, não há suporte para a seção `DeploymentOptions` no OVF.

Uma implantação do OVF no VMware Cloud Director envolve vários componentes, como o `TransferService`, a área de spool na montagem do NFS, a conexão NFC ao vCenter Server, a validação da soma de verificação, etc. Se algum desses componentes falhar, isso resultará em falha de carregamento do OVF.

Se você carregar um pacote do OVF com um arquivo de manifesto, o VMware Cloud Director validará o hash SHA-1 do arquivo descritor OVF e todos os arquivos VMDK para os valores no arquivo `manifest.mf`. Se algum hash não corresponder, o carregamento falhará. Um **administrador do sistema** pode desativar essa verificação definindo a propriedade `CONFIG` como `ovf.manifest.check.disabled`.

### Pré-requisitos

- Verifique se você tem um pacote OVF para carregar e se tem permissão para carregar pacotes OVF e implantar vApps.
- Verifique se a versão do OVF no arquivo descritor OVF não é 0,9.
- O tamanho máximo padrão com suporte de um arquivo descritor OVF no VMware Cloud Director é 12 MB. Você pode substituir isso editando a propriedade `CONFIG` `ovf.descriptor.size.max`.
- Verifique se o tamanho máximo padrão permitido do arquivo de manifesto (extensão `.mf`) é 1 MB.
- Verifique se o pacote OVF está em conformidade com o esquema XSD OVF.
- Se uma versão de hardware for fornecida no elemento `VirtualSystemType` do arquivo descritor OVF, verifique se ela é inferior à versão de hardware mais alta com suporte no VDC para o qual você carrega o OVF.
- Se o arquivo descritor OVF contiver elementos `ExtraConfig`, verifique se o **administrador do sistema** incluiu esses elementos em `AllowedList` de `extraConfigs`. Os elementos que não estão incluídos em `AllowedList` fazem com que o carregamento do OVF falhe com um erro de validação.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique em **Adicionar vApp do OVF**.
- 3 Clique no botão **Carregar** para navegar até um local acessível do seu computador e selecione o arquivo de modelo OVF/OVA.

O local pode ser seu disco rígido local, um compartilhamento de rede ou uma unidade de CD/DVD. As extensões de arquivo com suporte incluem `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` e `.strings`. Se você optar por carregar um arquivo OVF, que faz referência a mais arquivos do que você está tentando carregar, por exemplo, um arquivo VMDK, deverá procurar e selecionar todos os arquivos.

- 4 Clique em **Avançar**.
- 5 Verifique os detalhes do modelo OVF/OVA que você está prestes a implantar e clique em **Avançar**.
- 6 Insira um nome e, opcionalmente, uma descrição para o vApp e clique em **Avançar**.
- 7 (Opcional) Altere o nome do computador do vApp para que ele contenha apenas caracteres alfanuméricos.

Essa etapa será necessária apenas se o nome do vApp contiver espaços ou caracteres especiais. Por padrão, o nome do computador é preenchido com o nome da máquina virtual. No entanto, os nomes de computador devem conter apenas caracteres alfanuméricos.

- 8 No menu suspenso **Política de Armazenamento**, selecione uma política de armazenamento para cada uma das máquinas virtuais no vApp e clique em **Avançar**.
- 9 Selecione as redes às quais você deseja que cada máquina virtual se conecte.
  - Selecione uma rede para cada máquina virtual no menu suspenso **Rede**.
  - Você pode selecionar a opção **Alternar para o fluxo de trabalho de rede avançado** e inserir as configurações de rede, como a NIC primária, o tipo de adaptador de rede, a rede, a atribuição de IP e o endereço IP para cada máquina virtual no vApp manualmente.

É possível configurar propriedades adicionais para máquinas virtuais depois de concluir o assistente.

- 10 Clique em **Avançar**.

- 11 Personalize o hardware das máquinas virtuais no vApp e clique em **Avançar**.

Opção	Descrição
Número de CPUs virtuais	Insira o número de CPUs virtuais para cada máquina virtual no vApp. O número máximo de CPUs virtuais que você pode atribuir a uma máquina virtual depende do número de CPUs lógicas no host e do tipo de sistema operacional convidado que está instalado na máquina virtual.
Núcleos por soquete	Insira o número de núcleos por soquete para cada máquina virtual no vApp. Você pode configurar como as CPUs virtuais são atribuídas em termos de núcleos e núcleos por soquete. Determine quantos núcleos de CPU você deseja na máquina virtual e, em seguida, selecione o número de núcleos desejado em cada soquete, dependendo se você deseja uma única CPU de núcleo, CPU de dois núcleos, CPU de três núcleos e assim por diante.
Número de núcleos	Exiba o número de núcleos para cada máquina virtual no vApp. O número muda quando você atualiza o número de CPUs virtuais.
Memória total (MB)	Insira a memória em MB para cada máquina virtual no vApp. Essa configuração determina o quanto da memória do host ESXi é alocada para a máquina virtual. O tamanho da memória de hardware virtual determina a quantidade de memória disponível para os aplicativos executados na máquina virtual. Uma máquina virtual não pode se beneficiar de mais recursos de memória do que o tamanho da memória do hardware virtual configurado.

- 12 Na página Pronto para ser Concluído, reveja suas configurações e clique em **Concluir**.

### Resultados

O novo vApp aparece na exibição de cartão.

## Adicionar um vApp de um catálogo

Se você tiver acesso a um catálogo, poderá usar os modelos de vApp nesse catálogo para criar vApps.

Um modelo de vApp pode ser baseado em um arquivo OVF com propriedades para personalizar as máquinas virtuais do vApp. O vApp herda essas propriedades. Se qualquer uma dessas propriedades for configurável pelo usuário, você poderá especificar os valores delas.

### Pré-requisitos

- Para acessar modelos de vApp em catálogos públicos, verifique se você é um **administrador da organização** ou um **autor de vApp**.
- Para acessar modelos de vApp em catálogos de organização compartilhados com você, verifique se você é pelo menos um **usuário de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique em **Novo** e selecione **Adicionar vApp do Catálogo**.
- 3 Selecione um modelo para importar e clique em **Avançar**.
- 4 Insira um nome e, opcionalmente, uma descrição para o novo vApp.
- 5 Insira uma concessão de tempo de execução e uma locação de armazenamento para o vApp e clique em **Avançar**.
- 6 No menu suspenso **Política de Armazenamento**, selecione uma política de armazenamento para cada uma das máquinas virtuais no vApp e clique em **Avançar**.
- 7 Se as políticas de posicionamento e as políticas de dimensionamento das máquinas virtuais no vApp forem configuráveis, selecione uma política para cada máquina virtual no menu suspenso.
- 8 Se as propriedades de processamento para as máquinas virtuais no vApp forem configuráveis, personalize-as e clique em **Avançar**.

Opção	Descrição
<b>CPUs Virtuais</b>	Insira o número de CPUs virtuais para cada máquina virtual no vApp. O número máximo de CPUs virtuais que você pode atribuir a uma máquina virtual depende do número de CPUs lógicas no host e do tipo de sistema operacional convidado que está instalado na máquina virtual.
<b>Núcleos por soquete</b>	Insira o número de núcleos por soquete para cada máquina virtual no vApp. Você pode configurar como as CPUs virtuais são atribuídas em termos de núcleos e núcleos por soquete. Determine quantos núcleos de CPU você deseja na máquina virtual e, em seguida, selecione o número de núcleos desejado em cada soquete, dependendo se você deseja uma única CPU de núcleo, CPU de dois núcleos, CPU de três núcleos e assim por diante.
<b>Número de núcleos</b>	Exiba o número de núcleos para cada máquina virtual no vApp. O número muda quando você atualiza o número de CPUs virtuais.
<b>Memória</b>	Insira a memória em MB para cada máquina virtual no vApp. Essa configuração determina o quanto da memória do host ESXi é alocada para a máquina virtual. O tamanho da memória de hardware virtual determina a quantidade de memória disponível para os aplicativos executados na máquina virtual. Uma máquina virtual não pode se beneficiar de mais recursos de memória do que o tamanho da memória do hardware virtual configurado.

- 9 Se as propriedades de hardware das máquinas virtuais no vApp forem configuráveis, personalize o tamanho dos discos rígidos da máquina virtual e clique em **Avançar**.
- 10 Se as propriedades de rede das máquinas virtuais do vApp forem configuráveis, personalize-as e clique em **Avançar**.
  - a Na página **Configurar a Rede**, selecione as redes às quais você deseja que cada máquina virtual se conecte.
  - b (Opcional) Marque a caixa de seleção para alternar para o fluxo de trabalho de rede avançado e definir as configurações de rede adicionais para as máquinas virtuais no vApp.

- 11 Analise as configurações do vApp e clique em **Concluir**.

## Criar um vApp de um modelo de vApp

Você pode criar um novo vApp com base em um modelo de vApp armazenado em um catálogo ao qual você tem acesso.

Se o modelo de vApp for baseado em um arquivo OVF que inclui Propriedades OVF para personalizar suas máquinas virtuais, essas propriedades serão transmitidas ao vApp. Se qualquer uma dessas propriedades for configurável pelo usuário, você poderá especificar os valores.

### Pré-requisitos

- Somente administradores da organização e autores de vApp podem acessar modelos de vApp em catálogos públicos.
- Os usuários do vApp e funções superiores podem acessar os modelos de vApp em catálogos da organização compartilhados com eles.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.  
A lista de modelos aparece em uma exibição de grade.
- 2 Clique no botão de opção próximo ao modelo de vApp que você deseja usar e clique em **Criar vApp**.
- 3 Insira um nome e, opcionalmente, uma descrição do vApp.
- 4 Especifique por quanto tempo esse vApp pode ser executado antes de ser interrompido automaticamente, em horas ou dias.
- 5 Especifique por quanto tempo o vApp interrompido permanece disponível antes de ser limpo automaticamente, em horas ou dias.
- 6 Clique em **Avançar**.
- 7 Selecione o data center virtual no qual você deseja criar o vApp.
- 8 Selecione uma política de armazenamento.
- 9 Clique em **Avançar**.
- 10 Para o VMware Cloud Director 10.2.2 e versões posteriores, configure as políticas de posicionamento e dimensionamento de VM.  
Na versão 10.2.2, as políticas de posicionamento são globais, e você pode publicá-las em vários VDCs do provedor. Além disso, modelos de vApp incluem informações de políticas de posicionamento e dimensionamento.
- 11 Selecione as redes às quais você deseja que cada máquina virtual se conecte.
  - Selecione uma rede para cada máquina virtual no menu suspenso **Rede**.

- Você pode selecionar a opção **Alternar para o fluxo de trabalho de rede avançado** e inserir as configurações de rede, como a NIC primária, o tipo de adaptador de rede, a rede, a atribuição de IP e o endereço IP para cada máquina virtual no vApp manualmente.

É possível configurar propriedades adicionais para máquinas virtuais depois de concluir o assistente.

12 Clique em **Avançar**.

13 Personalize o hardware das máquinas virtuais no vApp e clique em **Avançar**.

Opção	Descrição
<b>Número de CPUs virtuais</b>	Insira o número de CPUs virtuais para cada máquina virtual no vApp. O número máximo de CPUs virtuais que você pode atribuir a uma máquina virtual depende do número de CPUs lógicas no host e do tipo de sistema operacional convidado que está instalado na máquina virtual.
<b>Núcleos por soquete</b>	Insira o número de núcleos por soquete para cada máquina virtual no vApp. Você pode configurar como as CPUs virtuais são atribuídas em termos de núcleos e núcleos por soquete. Determine quantos núcleos de CPU você deseja na máquina virtual e, em seguida, selecione o número de núcleos desejado em cada soquete, dependendo se você deseja uma única CPU de núcleo, CPU de dois núcleos, CPU de três núcleos e assim por diante.
<b>Número de núcleos</b>	Exiba o número de núcleos para cada máquina virtual no vApp. O número muda quando você atualiza o número de CPUs virtuais.
<b>Memória total (MB)</b>	Insira a memória em MB para cada máquina virtual no vApp. Essa configuração determina o quanto da memória do host ESXi é alocada para a máquina virtual. O tamanho da memória de hardware virtual determina a quantidade de memória disponível para os aplicativos executados na máquina virtual. Uma máquina virtual não pode se beneficiar de mais recursos de memória do que o tamanho da memória do hardware virtual configurado.
<b>Propriedades do disco rígido</b>	Insira o tamanho do disco rígido da máquina virtual em MB.

14 Na página Pronto para ser Concluído, reveja suas configurações e clique em **Concluir**.

## Resultados

O novo vApp aparece na exibição de cartão.

## Importar uma máquina virtual do vCenter Server como vApp

Se você tiver direitos de **administrador do sistema**, poderá importar as VMs do vCenter Server como vApps para o VMware Cloud Director.

Importar uma máquina virtual não mantém as configurações de compartilhamentos, limite e reserva da máquina virtual definidas no vCenter Server. As máquinas virtuais importadas recebem as configurações de alocação de recursos delas do centro de dados virtual da organização em que residem.



### Pré-requisitos

Para ver e importar máquinas virtuais do vCenter Server, verifique se você tem direitos de **administrador do sistema**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique em **Novo** e selecione **Importar do vCenter**.
- 3 No menu suspenso, selecione uma instância do vCenter Server da qual uma máquina virtual é importada.
- 4 Selecione uma máquina virtual para importar.
- 5 Insira um nome e, opcionalmente, uma descrição para o novo vApp.
- 6 No menu suspenso, selecione um centro de dados virtual no qual armazenar e executar o vApp.
- 7 (Opcional) No menu suspenso, selecione uma política de armazenamento para o vApp.
- 8 (Opcional) Para excluir a máquina virtual de origem, ative a opção **Mover Máquina Virtual**.
- 9 Clique em **Importar**.

## Operações para ligar ou desligar em vApps

Você pode realizar operações de energia em vApps, como ligar ou desligar um vApp, suspender ou redefinir um vApp.


### Ligar um vApp

Ligar um vApp liga todas as máquinas virtuais nesse vApp que ainda não estão ligadas.

### Pré-requisitos

Você deve ser pelo menos um autor de vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja ligar, selecione **Ligar**.

### Resultados

O vApp é ligado.


## Desligar um vApp

Desligar um vApp desliga todas as máquinas virtuais nesse vApp. Para realizar determinadas ações, como adicionar um vApp a um catálogo, copiá-lo ou movê-lo para outro VDC, primeiro você deve desligar o vApp.

### Pré-requisitos

O vApp deve ser iniciado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja parar, selecione **Desligar**.
- 4 Clique em **OK**.

### Resultados

Todas as máquinas virtuais no vApp e o vApp propriamente dito são desligados.


## Redefinir um vApp

Redefinir um vApp limpa o estado (memória, cache e assim por diante), mas o vApp continua a ser executado.

### Pré-requisitos

Seu vApp é iniciado, e as máquinas virtuais nela são ligadas.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja redefinir, selecione **Redefinir**.

### Resultados

O estado é limpo, e o vApp continua a ser executado.


## Suspender um vApp

A suspensão de um vApp preserva seu estado atual gravando a memória no disco.

### Pré-requisitos

O vApp está em execução.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja suspender, selecione **Suspender**.

### Resultados

O vApp é suspenso e seu estado é preservado.


## Descartar o estado suspenso de um vApp

Se um vApp estiver em um estado suspenso e você não precisar mais retomar o uso do vApp, poderá descartar o estado suspenso. Descartar o estado suspenso remove a memória salva e retorna o vApp para um estado desligado.

### Pré-requisitos

O vApp deve estar em um estado suspenso.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp suspenso, selecione **Descartar Estado Suspenso**.

### Resultados

O estado é descartado, e o vApp é desligado.

## Ligar vários vApps

Você pode ligar vários vApps ao mesmo tempo. Esta ação liga todas as VMs nesse vApp que ainda não está ligado.

### Pré-requisitos

Verifique se você é pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja ligar.
- 4 No menu **Ações**, selecione **Ligar**.
- 5 Clique em **OK** para confirmar.

## Desligar vários vApps

É possível desligar vários vApps ao mesmo tempo. Essa ação desliga todas as máquinas virtuais nos vApps. Para realizar determinadas ações, como adicionar um vApp a um catálogo, copiá-lo ou movê-lo para outro centro de dados virtual, primeiro você deve desligar o vApp.

### Pré-requisitos

- Verifique se os vApps foram iniciados.
- Verifique se você é pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja desligar.
- 4 No menu **Ações**, selecione **Desligar**.
- 5 Clique em **OK** para confirmar.

## Descartar o estado suspenso de vários vApps

Se vários vApps estiverem em um estado suspenso e você não precisar mais retomar o uso, poderá descartar o estado suspenso dos vApps ao mesmo tempo. Descartar o estado suspenso remove a memória salva e retorna os vApps para um estado desligado.

### Pré-requisitos

- Verifique se os vApps estão em estado suspenso.
- Verifique se você é pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps suspensos que você deseja desligar.
- 4 No menu **Ações**, selecione **Descartar Estado Suspenso**.

## Resultados

Os vApps estão desligados.

## Redefinir vários vApps

A redefinição de vários vApps limpa simultaneamente seu estado, que inclui memória, cache e assim por diante, mas os vApps continuam em execução.

### Pré-requisitos

- Verifique se os vApps foram iniciados e se as máquinas virtuais neles estão ligadas.
- Verifique se você é pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja redefinir.
- 4 No menu **Ações**, selecione **Redefinir** e clique em **OK** para confirmar.

## Resultados

O estado de cada vApp é limpo e os vApps continuam em execução.

## Suspender vários vApps

Suspender vários vApps simultaneamente preserva seu estado atual, gravando a memória no disco.

### Pré-requisitos

Verifique se os vApps estão em execução.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja suspender.
- 4 No menu **Ações** do vApp que você deseja suspender, selecione **Suspender** e clique em **OK** para confirmar.


## Resultados

Os vApps são suspensos e seu estado é preservado.

## Abrir um vApp

Você pode abrir um vApp para exibir as máquinas virtuais e as redes que ele contém. Você também pode visualizar um diagrama mostrando como as máquinas virtuais e as redes estão conectadas.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.  
Na exibição de cartão, você pode ver informações gerais para cada vApp, como nome, estado de energia, informações de concessão, data de criação, proprietário, o número de máquinas virtuais associadas ao vApp, número total de CPUs, armazenamento e memória totais e redes associadas.
- 3 Para exibir as configurações detalhadas de um vApp selecionado, clique em **Detalhes** no cartão do vApp.

## Editar Propriedades do vApp

Você pode editar as propriedades de um vApp existente, incluindo o nome e a descrição do vApp, as configurações de lease, a ordem em que as máquinas virtuais são iniciadas no vApp, as configurações de compartilhamento e as configurações de rede.


### Editar as propriedades gerais do vApp

Você pode revisar e alterar o nome, a descrição e outras propriedades gerais de um vApp.

#### Pré-requisitos

Verifique se o vApp está desligado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes** para exibir e editar as propriedades do vApp.

#### 4 Revise e altere as propriedades conforme necessário e clique em **Salvar**.

Opção	Ação
Nome	Insira um novo nome para o vApp.
Descrição	Digite uma descrição opcional do vApp.
Data center virtual	O nome do data center ao qual o vApp pertence.
Instantâneo	Se houver um snapshot, seus detalhes serão exibidos.
Leases	<p>Selecione <b>Renovar</b> para renovar o lease.</p> <p>a Agende o lease de tempo de execução em número de horas ou dias.</p> <p>Define por quanto tempo o vApp pode ser executado antes de ser interrompido automaticamente.</p> <p>b Agende o lease de armazenamento em número de horas ou dias.</p> <p>Define quanto tempo o vApp permanecerá disponível antes de ser excluído automaticamente.</p>

#### Resultados

As configurações gerais são salvas.

## Editar a ordem de início e interrupção de máquinas virtuais em um vApp


Você pode configurar a ordem de início e parada de máquinas virtuais no vApp. Configure a ordem inicial e final caso você tenha aplicativos instalados nas máquinas virtuais que devem iniciar e parar em uma ordem específica.

Essas configurações serão úteis se você precisar iniciar e parar as máquinas virtuais em uma ordem específica. Por exemplo, uma máquina virtual aloja um servidor de banco de dados, outra aloja um servidor de aplicativos e a última aloja um servidor Web. Para que as funções relacionadas funcionem corretamente, o servidor de banco de dados deve ser iniciado primeiro, seguido pelo servidor de aplicativos e depois pelo servidor Web.

#### Pré-requisitos

Verifique se o vApp está desligado.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Clique na guia **Ordem de Início e Interrupção** e clique em **Editar**.

- 5 Edite as propriedades de ordem de início e parada para cada máquina virtual e clique em **OK**.

Opção	Ação
<b>Ordem para Iniciar</b>	Insira a ordem na qual deseja que a máquina virtual seja iniciada. Você deve inserir um valor para cada máquina na sequência.
<b>Iniciar Ação</b>	Selecione uma ação inicial. A ação inicial determina o que acontece com uma máquina virtual quando você inicia o vApp que a contém. Por padrão, essa opção está definida como <b>Ligar</b> .
<b>Iniciar Espera</b>	Insira o tempo de espera de início. O tempo de espera de início é o tempo (em segundos) que você deseja aguardar antes de o VMware Cloud Director iniciar a próxima máquina na sequência.
<b>Parar Ação</b>	Selecione a ação de interrupção. A ação de interrupção é a ação que a máquina virtual executa quando você interrompe o vApp que a contém. Se você selecionar <b>Desligar</b> , a VM será desligada sem realizar ações de desligamento que garantem a estabilidade (que é o equivalente de extrair uma tomada da parede). Selecione essa ação se você não tiver instalado o VMware Tools. Caso contrário, selecione <b>Encerrar</b> , o que garante estabilidade no desligamento.
<b>Parar Espera</b>	Insira o tempo de espera de interrupção. O tempo de espera de interrupção é o tempo (em segundos) que você deseja aguardar antes de o VMware Cloud Director encerrar a próxima máquina virtual na sequência.

## Editar as propriedades de guest de um vApp


Se um vApp incluir propriedades OVF configuráveis pelo usuário, você poderá revisar e modificar essas propriedades.

Se uma máquina virtual no vApp incluir um valor para uma propriedade configurável pelo usuário com o mesmo nome, o valor da máquina virtual terá precedência.

### Pré-requisitos

Verifique se o vApp está parado e suas propriedades de guest são configuráveis pelo usuário.

### Procedimentos


- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **Máquinas Virtuais**.
- 2 Clique em  para exibir a lista em uma exibição de cartão e, opcionalmente, filtre a lista de máquinas virtuais no menu suspenso **Classificar por**.
- 3 No cartão da máquina virtual que você deseja editar, clique em **Detalhes**.
- 4 Clique em **Propriedades de Guest** e clique em **Editar**.
- 5 Modifique as propriedades de guest do vApp e clique em **OK**.



## Compartilhar um vApp

Você pode compartilhar seus vApps com outros grupos ou usuários dentro da sua organização. Os controles de acesso que você define determinam as operações que podem ser concluídas nos vApps compartilhado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes** e role para baixo até as propriedades de compartilhamento do vApp.
- 4 Selecione os usuários com os quais você deseja compartilhar o vApp e clique em **Salvar**.

Opção	Ação
Compartilhar com todos na organização	<p>Selecione essa opção para compartilhar com todos os usuários na organização e escolha o nível de acesso.</p> <ul style="list-style-type: none"> <li>■ Para conceder controle total, selecione <b>Controle Total</b>. Todos os usuários da organização podem abrir, iniciar, salvar um vApp como um modelo de vApp, adicionar o modelo a um catálogo, alterar o proprietário do vApp, copiar para um catálogo e modificar as propriedades.</li> <li>■ Para conceder acesso somente leitura, selecione <b>Somente Leitura</b>.</li> </ul>
Compartilhe com usuários e grupos específicos	<p>Selecione essa opção para compartilhar somente com os usuários que você especificar.</p> <ol style="list-style-type: none"> <li>a Selecione os nomes do painel <b>Usuários e grupos sem acesso</b> para movê-los até o painel <b>Usuários e grupos com acesso</b>.</li> <li>b Selecione um nível de acesso para os usuários e grupos especificados. <ul style="list-style-type: none"> <li>■ Para conceder controle total, selecione <b>Controle Total</b>. Os usuários com controle total podem abrir, iniciar, salvar um vApp como um modelo de vApp, adicionar o modelo a um catálogo, alterar o proprietário do vApp, copiar para um catálogo e modificar as propriedades.</li> <li>■ Para conceder acesso somente leitura, selecione <b>Somente Leitura</b>.</li> </ul> </li> </ol>

### Resultados

Seu vApp é compartilhado com os usuários ou grupos especificados.


## Exibir um diagrama de rede do vApp

Um diagrama de rede de vApp fornece uma visão gráfica das máquinas virtuais e das redes em um vApp.

## Pré-requisitos

Para visualizar o diagrama de rede do vApp, ele deve conter menos de 40 máquinas virtuais. Se o vApp contiver mais de 40 máquinas virtuais, o diagrama não estará disponível.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Clique na guia **Diagrama de Redes**.  
É exibido o diagrama que mostra como as máquinas virtuais e as redes no vApp estão conectadas. Um sinal de estrela representa uma NIC primária. Se uma NIC estiver conectada, sua cor será verde, se uma NIC não estiver conectada, sua cor será branca.
- 5 (Opcional) Para realçar as redes e as máquinas virtuais conectadas, clique em uma rede ou em uma máquina virtual.

Os objetos conectados e as conexões entre eles são realçados.

## Próximo passo

Você pode adicionar máquinas virtuais ou redes dessa página.

# Trabalhando com redes em um vApp

As máquinas virtuais em um vApp podem se conectar a redes vApp (isoladas ou roteadas) e redes de centro de dados virtuais da organização (direta ou isoladas). Você pode adicionar redes de diferentes tipos a um vApp para abordar vários cenários de rede.

As máquinas virtuais no vApp podem se conectar às redes que estão disponíveis em um vApp. Se você deseja conectar uma máquina virtual a uma rede diferente, deve primeiro adicioná-lo ao vApp.

Um vApp pode incluir redes vApp e redes virtuais de centro de dados da organização. Uma rede vApp pode ser isolada ou roteada. Uma rede vApp isolada está contida no vApp. Você também pode rotear uma rede vApp para uma rede de datacenter virtual da organização para fornecer conectividade a máquinas virtuais fora do vApp. Para redes vApp roteadas, você pode configurar serviços de rede, como um firewall e roteamento estático.

---

**Observação** VDCs de organização com o suporte do NSX Data Center for vSphere são compatíveis com redes de vApps roteadas, isoladas e diretas.

VDCs de organização com o suporte do NSX-T Data Center são compatíveis com redes de vApps isoladas e diretas.

---

Você pode conectar um vApp diretamente a uma rede de datacenter virtual da organização. Se você tiver vários vApps que contenham máquinas virtuais idênticas conectadas à mesma rede de datacenter virtual da organização e quiser iniciar os vApps ao mesmo tempo, poderá isolar o vApp. O isolamento do vApp permite que você ligue as máquinas virtuais sem conflito, isolando seus endereços MAC e IP.



As redes que você adiciona ao vApp usam o pool de redes que está associado ao centro de dados virtual da organização no qual você criou o vApp.

## Exibir redes do vApp

Você pode acessar e visualizar as redes em um vApp.

### Pré-requisitos

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Clique na guia **Redes**.  
A lista de redes, se houver alguma, aparece. Você pode visualizar informações sobre cada rede, como nome, gateway, máscara de rede e conexão, bem como reter recursos IP e NAT.
- 5 (Opcional) Para editar as colunas a serem visualizadas, clique no ícone do **Editor de Grade** () e marque ou desmarque as caixas de seleção das colunas que deseja visualizar ou ocultar, respectivamente.

## Isolar uma rede de vApp

Ligar máquinas virtuais idênticas que estão incluídas em diferentes vApps pode resultar em um conflito. Para permitir a ativação de máquinas virtuais idênticas em diferentes vApps sem conflitos, você deve isolar o vApp.


O isolamento de um vApp isola os endereços MAC e IP das máquinas virtuais e altera o tipo de conexão das redes de VDC de organização de Direta para Isolada. Em redes isoladas, o firewall é automaticamente habilitado e configurado para que apenas o tráfego de saída seja permitido. Ao isolar um vApp, você também pode configurar regras de NAT e firewall nas redes com isolamento.

### Pré-requisitos

- É possível isolar apenas redes de vApps diretas. Se o vApp usar mais de uma rede e as outras redes forem, por exemplo, roteadas, apenas a rede direta será isolada.

- As máquinas virtuais no vApp que usarem a rede direta deverão ser interrompidas para que a rede de vApp direta não esteja em uso no momento.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Clique na guia **Redes**.
- 5 Se o vApp não estiver em isolamento, clique no botão **Editar**.
- 6 Alterne a opção **Conter o vApp** e clique em **OK**.

### Resultados

Os endereços IP e MAC das máquinas virtuais se tornam isolados. Você pode ligar máquinas virtuais idênticas em vApps diferentes sem conflito.

## Adicionar uma rede a um vApp

Você pode adicionar uma rede a um vApp para tornar a rede disponível para as máquinas virtuais no vApp. Você pode adicionar uma rede vApp ou uma rede de data center virtual da organização a um vApp.


As conexões podem ser diretas ou isoladas. O isolamento permite que máquinas virtuais idênticas em diferentes vApps sejam ligadas sem conflito, isolando os endereços MAC e IP das máquinas virtuais.

Quando o isolamento está ativado e o vApp está ligado, uma rede isolada é criada com base no pool de redes de data center virtual da organização. Um edge gateway é criado e conectado à rede isolada e à rede de data center virtual da organização. O tráfego que vai para e das máquinas virtuais passa pelo edge gateway, que converte o endereço IP usando NAT e proxy-AR. Isso permite que um roteador passe o tráfego entre duas redes usando o mesmo espaço de IP.

### Pré-requisitos

Para adicionar uma rede de data center virtual da organização, seu administrador deve ter criado essa rede.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Ações** e selecione **Adicionar rede**.

#### 4 Selecione o tipo de rede a ser adicionada.

Opção	Ação
Rede do VDC de Organização	Selecione uma rede de data center virtual da organização na lista de redes disponíveis.
Rede do vApp	<p>a Insira um nome e, opcionalmente, uma descrição para a rede.</p> <p>b Insira o CIDR do gateway de rede.</p> <p>c (Opcional) Insira o DNS primário e o secundário e o sufixo DNS.</p> <p>d (Opcional) Selecione se deseja permitir a VLAN convidada.</p> <p>e (Opcional) Insira as configurações do pool de IPs estáticos, como intervalos de IP.</p> <p>f (Opcional) Para poder se conectar a uma rede de data center virtual da organização, ative a opção <b>Conectar-se a uma rede de VDC da organização</b> e selecione uma rede na lista.</p>

#### 5 Clique em **Adicionar**.

##### Resultados

A rede é adicionada ao vApp.

##### Próximo passo

Conecte uma máquina virtual no vApp à rede.

## Configurar serviços de rede para uma rede vApp

Você pode configurar serviços de rede, como DHCP, firewalls, conversão de endereços de rede (NAT) e roteamento estático para determinadas redes do vApp.

Os serviços de rede disponíveis dependem do tipo de rede do vApp.

**Tabela 3-1. Serviços de Rede Disponíveis por Tipo de Rede**

Tipo de rede do vApp	DHCP	Firewall	NAT	Roteamento Estático
Direto				
Roteado	X	X	X	X
Isolado	X			


**Observação** VDCs de organização com o suporte do NSX Data Center for vSphere são compatíveis com redes de vApps roteadas, isoladas e diretas.

VDCs de organização com o suporte do NSX-T Data Center são compatíveis com redes de vApps isoladas e diretas.

## Visualizar e editar detalhes gerais da rede

Você pode visualizar e editar os detalhes gerais da rede do vApp, por exemplo, o nome e a descrição dela.


### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Na guia **Geral**, analise as informações da rede.
- 6 Clique em **Editar**.
- 7 Edite o nome e a descrição da rede do vApp.
- 8 Clique em **Salvar**.

## Editar as configurações do pool de IPs estáticos de uma rede vApp

Você pode configurar uma rede de vApp para fornecer endereços IP estáticos para as máquinas virtuais no vApp, extraíndo-os de um pool estático de endereços IP.


### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Na guia **Gerenciamento de IPs**, clique em **Pools Estáticos**.
- 6 Clique em **Editar**.
- 7 Insira um intervalo de IPs e clique em **Adicionar**.
- 8 Clique em **Salvar**.

## Editar as configurações de DNS de uma rede vApp

Depois de criar a rede de vApp, você pode visualizar e editar as configurações de DNS a qualquer momento.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Na guia **Gerenciamento de IPs**, clique em **DNS**.  
São exibidas as configurações de DNS.
- 6 Clique em **Editar**.
- 7 Edite o DNS primário, o DNS secundário e o sufixo DNS.
- 8 Clique em **Salvar**.

## Configurar o DHCP para uma rede vApp


Você pode configurar determinadas redes vApp para fornecer serviços DHCP a máquinas virtuais no vApp.

Quando você habilitar o DHCP para uma rede vApp, conecte um NIC na máquina virtual no vApp a essa rede e selecione DHCP como o modo de IP para esse NIC. O VMware Cloud Director atribui um endereço IP do DHCP à máquina virtual quando você a liga.

## Pré-requisitos

- Verifique se a rede do vApp está roteada ou isolada.
- Verifique se o vApp está em um centro de dados virtual da organização com o suporte de NSX Data Center for vSphere.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Na guia **Gerenciamento de IP**, clique em **DHCP**.  
O status do DHCP é exibido.
- 6 Clique em **Editar**.
- 7 Clique em **Habilitado**.

- 8 Na caixa de texto **Pool de IPs**, insira um intervalo de endereços IP.

O VMware Cloud Director usa esses endereços para atender às solicitações do DHCP. O intervalo de endereços IP do DHCP não pode se sobrepor ao pool de IP estático para a rede vApp.

- 9 Defina o tempo de lease máximo e padrão em segundos.


- 10 Clique em **Salvar**.

## Exibir as alocações de IP da rede vApp

Você pode revisar as alocações de IP das redes no seu vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique no  para mostrar os vApps em uma exibição de cartão.

- 3 No cartão do vApp selecionado, clique em **Detalhes**.

- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.

- 5 Na guia **Gerenciamento de IP**, clique em **Alocações de IP**.

Os endereços IP alocados são exibidos.

## Configurar o roteamento estático para uma rede vApp

Você pode configurar determinadas redes vApp para fornecer serviços de roteamento estático para permitir que máquinas virtuais em diferentes redes vApp se comuniquem.

Qualquer rota estática que você criar será ativada automaticamente.

### Pré-requisitos

Uma rede vApp roteada.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique no  para mostrar os vApps em uma exibição de cartão.

- 3 No cartão do vApp selecionado, clique em **Detalhes**.

- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.

- 5 Na guia **Roteamento**, clique em **Editar**.

Você pode ativar ou desativar o roteamento estático para a rede.



## Adicionar o roteamento estático para uma rede vApp

Você pode adicionar rotas estáticas entre duas redes vApp que são roteadas para a mesma rede de datacenter virtual da organização. Rotas estáticas permitem o tráfego entre as redes.


Não é possível adicionar rotas estáticas a um vApp isolado ou entre redes sobrepostas. Depois de adicionar uma rota estática a uma rede vApp, configure as regras de firewall de rede para permitir o tráfego na rota estática. Para vApps com rotas estáticas, selecione Sempre usar endereços IP atribuídos até que esta rede vApp ou redes associadas sejam excluídas.

As rotas estáticas só funcionam quando os vApps contendo as rotas estão em execução. Se você alterar a rede principal de um vApp, excluir um vApp ou excluir uma rede vApp, e o vApp incluir rotas estáticas, essas rotas não funcionarão, e você deverá removê-las manualmente.

### Pré-requisitos

- Duas redes vApp estão roteadas para a mesma rede de datacenter virtual da organização.
- As redes vApp estão nos vApps que foram iniciados pelo menos uma vez.
- O roteamento estático está habilitado em ambas as redes vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Na guia **Roteamento**, em Roteamento estático, clique em **Adicionar**.  
Os endereços IP alocados são exibidos.
- 6 Insira o nome da rota estática.
- 7 Insira o endereço de rede no formato CIDR.  
O endereço de rede é para a rede vApp à qual uma rota estática será adicionada.
- 8 Insira o endereço IP do próximo salto.  
O endereço IP do próximo salto é o endereço IP externo do roteador da rede vApp.
- 9 Clique em **Salvar**.
- 10 Repita o mesmo procedimento para a segunda rede vApp.

### Exemplo: Exemplo de roteamento estático

A Rede vApp 1 e a Rede vApp 2 são roteadas para a Rede Organizacional Compartilhada. Você pode criar uma rota estática em cada rede vApp para permitir o tráfego entre as redes. Você pode usar as informações sobre as redes vApp para criar as rotas estáticas.

Tabela 3-2. Informações da rede

Nome da Rede	Especificação da rede	Endereço IP externo do roteador
Rede vApp 1	192.168.1.0/24	192.168.0.100
Rede vApp 2	192.168.2.0/24	192.168.0.101
Rede Organizacional Compartilhada	192.168.0.0/24	NA

Na rede vApp 1, crie uma rota estática para a rede vApp 2. Na rede vApp 2, crie uma rota estática para a rede vApp 1.

Tabela 3-3. Configurações de roteamento estático

Rede do vApp	Nome da rota	Rede	Endereço IP do próximo salto
Rede vApp 1	tovapp2	192.168.2.0/24	192.168.0.101
Rede vApp 2	tovapp1	192.168.1.0/24	192.168.0.100

## Adicionar uma regra de direcionamento de porta a uma rede do vApp

Adicione uma regra de mapeamento NAT para poder configurar determinadas redes do vApp e fornecer direcionamento de porta.

O direcionamento de porta fornece acesso externo aos serviços em execução em máquinas virtuais na rede do vApp.


Quando você configura o direcionamento de porta, o VMware Cloud Director mapeia uma porta externa para um serviço que é executado em uma máquina virtual dedicada ao tráfego de entrada.

Quando você adiciona uma regra de direcionamento de porta a uma rede do vApp, ela aparece na parte inferior da lista de regras de mapeamento NAT. Para obter informações sobre como definir a ordem na qual as regras de direcionamento de porta são aplicadas, consulte

### Pré-requisitos

- Verifique se a rede do vApp está roteada.
- Verifique se o firewall na rede do vApp está ativado. Ao desativar o firewall, as regras de mapeamento NAT não serão mais aplicadas à rede do vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.

- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Clique em **Serviços** e em **Editar**.
- 6 Para ativar a NAT, ative a opção NAT.
- 7 No menu suspenso **Tipo de NAT**, selecione **Direcionamento de porta** e clique em **Adicionar**.
- 8 (Opcional) Para ativar o mascaramento de IP, marque a caixa de seleção.
- 9 Configure a regra de direcionamento de porta.
  - a Selecione uma porta externa.
  - b Selecione uma porta para a qual direcionar.
  - c Selecione uma interface de máquina virtual.
  - d Selecione um protocolo para o tipo de tráfego a ser direcionado.
- 10 Clique em **Salvar**.

#### Próximo passo

Se necessário, reorganize as regras de direcionamento de porta usando os botões **Mover para cima** ou **Mover para baixo**.

## Adicionar uma regra de conversão de IP a uma rede do vApp


Você pode configurar determinadas redes do vApp para fornecer uma conversão de IP adicionando uma regra de mapeamento NAT.

Quando você cria uma regra de conversão de IP para uma rede, o vCloud Director adiciona uma regra de DNAT e SNAT ao edge gateway associado ao grupo de portas da rede. A regra de DNAT converte um endereço IP externo em um endereço IP interno para o tráfego de entrada. A regra de SNAT converte um endereço IP interno em um endereço IP externo para o tráfego de saída.

#### Pré-requisitos

- Verifique se a rede do vApp está roteada.
- Verifique se o firewall na rede do vApp está ativado. Ao desativar o firewall, as regras de mapeamento NAT não serão mais aplicadas à rede do vApp.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, clique em uma rede para exibir os detalhes da rede.
- 5 Clique em **Serviços** e em **Editar**.

- 6 Para ativar a NAT, ative a opção NAT.
- 7 No menu suspenso **Tipo de NAT**, selecione **Conversão de IP** e clique em **Adicionar**.
- 8 Selecione uma interface de máquina virtual e clique em **Manter**.
- 9 Selecione um modo de mapeamento.
- 10 Se tiver selecionado o modo de mapeamento **Manual**, insira um endereço IP externo.
- 11 Clique em **Salvar**.

#### Próximo passo

Se necessário, reorganize as regras de conversão de IP usando os botões **Mover para cima** ou **Mover para baixo**.


## Excluir uma rede vApp

Se você não precisar mais de uma rede no vApp, poderá excluí-la.

#### Pré-requisitos

O vApp é interrompido e nenhuma máquina virtual no vApp é conectada à rede.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No cartão do vApp selecionado, clique em **Detalhes**.
- 4 Na guia **Redes**, selecione a rede que você deseja excluir, clique em **Excluir** e confirme a exclusão.

## Como trabalhar com instantâneos

A criação de um instantâneo preserva o estado e os dados das máquinas virtuais em um vApp de um determinado point-in-time. Um instantâneo não deve ser usado por longos períodos nem no lugar do backup do vApp.

Você pode querer usar um instantâneo ao fazer upgrade das máquinas virtuais em um vApp. Por exemplo, antes de fazer upgrade das máquinas virtuais, crie um instantâneo para preservar o point-in-time antes do upgrade. Para fazer isso, salve um instantâneo antes do upgrade e, em seguida, faça o upgrade. Se não houver problemas durante o upgrade, você poderá optar por remover o instantâneo, e isso confirmará as alterações feitas durante o upgrade. No entanto, se você tiver tido um problema, poderá reverter o instantâneo, que voltará para o estado do vApp salvo antes do upgrade.

## Tirar um snapshot de um vApp

Ao tirar um snapshot de um vApp, você tira snapshots de todas as máquinas virtuais nesse vApp. Depois de tirar o snapshot, é possível reverter todas as máquinas virtuais no vApp para esse snapshot. Caso não precise mais do snapshot, basta removê-lo.

Snapshots de vApps têm algumas limitações.

- Snapshots de vApps não capturam configurações de NIC.
- Se qualquer máquina virtual no vApp estiver conectada a um disco nomeado, você não poderá tirar um snapshot desse vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique no  para mostrar os vApps em uma exibição de cartão.

- 3 No menu **Ações** do vApp do qual você deseja tirar um snapshot, selecione **Criar Snapshot**.

Tirar um snapshot de um vApp substitui o snapshot existente, se houver algum.

- 4 (Opcional) Selecione se deseja tirar o snapshot da memória do vApp.

Quando você captura o estado de memória do vApp, o snapshot mantém o estado ativo desse vApp e das máquinas virtuais nele. Snapshots de memória criam um snapshot em um momento preciso, por exemplo, para atualizar o software que ainda está funcionando. Se você tirar um snapshot de memória, e a atualização não for concluída conforme o esperado ou se o software não atender às suas expectativas, você poderá reverter a máquina virtual ao seu estado anterior.

Quando você captura o estado da memória, os arquivos do vApp não precisam de desativação. Se você não capturar o estado da memória, o snapshot não salvará o estado ativo do vApp, e os discos terão uma falha consistente, a menos que você os desative.

- 5 (Opcional) Selecione se deseja desativar o sistema de arquivos convidado.

Essa operação requer que o VMware Tools esteja instalado nas máquinas virtuais do vApp. Quando você desativa uma máquina virtual, o VMware Tools desativa o sistema de arquivos dessa máquina virtual. Uma operação de desativação garante que um disco de snapshot represente um estado consistente dos sistemas de arquivos do convidado. Snapshots desativados são apropriados para backups automáticos ou periódicos. Por exemplo, se você não tem conhecimento das atividades da máquina virtual, mas deseja reverter vários backups recentes, é possível desativar os arquivos.

Não é possível desativar vApps com discos de grande capacidade.

- 6 Clique em **OK**.

## Resultados

É criado um snapshot do vApp.

## Próximo passo

Você pode reverter todas as máquinas virtuais no vApp para o snapshot mais recente.


## Converter um vApp para um snapshot

Você pode reverter todas as máquinas virtuais em um vApp para o estado em que estavam quando você criou o snapshot do vApp.

### Pré-requisitos

Verifique se o vApp tem um snapshot existente.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja reverter, selecione **Reverter para Snapshot**.
- 4 Clique em **OK**.

## Resultados

Todas as máquinas virtuais no vApp são revertidas para o estado do snapshot.

## Excluir um snapshot de um vApp


Você pode remover um snapshot de um vApp.

Ao remover um snapshot do vApp, você exclui o estado das máquinas virtuais no snapshot do vApp e não pode retornar a esse estado novamente. A remoção de um snapshot não afeta o estado atual do vApp.

### Pré-requisitos

Você fez um snapshot do vApp.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp para o qual você deseja remover um snapshot, selecione **Remover Snapshot**.

#### 4 Clique em **OK**.

#### Resultados

O snapshot é removido.

## Tirar snapshots de vários vApps

Ao tirar snapshots de vários vApps, você tira snapshots de todas as máquinas virtuais nos vApps. Depois de tirar os snapshots, você pode reverter todas as máquinas virtuais nos vApps para os snapshots ou removê-los, se não precisar deles.

Snapshots de vApps têm algumas limitações.

- Snapshots de vApps não capturam configurações de NIC.
- Se qualquer máquina virtual em um vApp estiver conectada a um disco nomeado, você não poderá tirar um snapshot desse vApp.
- Tirar snapshots de vários vApps não cria snapshots da memória dos vApps e não interrompe o sistema de arquivos convidados dos vApps. Se você quiser criar um snapshot da memória dos seus vApps ou desativar o sistema de arquivos convidado, deverá criar snapshots individuais para cada vApp. Consulte [Tirar um snapshot de um vApp](#).

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps para os quais você deseja criar snapshots.
- 4 No menu **Ações**, selecione **Criar Snapshot** e clique em **OK** para confirmar.

#### Próximo passo

- Você pode reverter todas as máquinas virtuais nos vApps para os snapshots mais recentes. Consulte [Reverter vários vApps para snapshots](#).
- Você pode remover os snapshots dos vApps. Consulte [Remover snapshots de vários vApps](#).

## Remover snapshots de vários vApps

Se você não precisar dos snapshots de vários vApps, poderá removê-los simultaneamente.

Ao remover um snapshot do vApp, você exclui o estado das máquinas virtuais no snapshot do vApp e não pode retornar a esse estado novamente. A remoção de um snapshot não afeta o estado atual do vApp.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os snapshots dos vApps que você deseja remover.
- 4 No menu **Ações**, selecione **Remover Snapshot**.

## Reverter vários vApps para snapshots

Você pode reverter todas as máquinas virtuais em vários vApps para o estado em que estavam quando você criou os snapshots do vApp.

### Pré-requisitos

Verifique se os vApps que você deseja reverter têm snapshots existentes.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja reverter para seus snapshots mais recentes.
- 4 No menu **Ações**, selecione **Reverter para Snapshot**.
- 5 Clique em **OK** para confirmar.


## Alterar o proprietário de um vApp

Você pode alterar o proprietário do vApp, por exemplo, quando um proprietário do vApp deixa a empresa ou muda de função dentro da empresa.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp para o qual você deseja alterar o proprietário, selecione **Alterar proprietário**.
- 4 Selecione um usuário na lista.
- 5 Clique em **OK**.



## Resultados

O proprietário do vApp foi alterado.


## Mover um vApp para outro data center virtual

Quando você move um vApp para outro data center virtual, esse vApp é removido do data center virtual de origem.

### Pré-requisitos

- Você deve ser pelo menos um **autor de vApp**.
- Seu vApp está desligado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja mover, selecione **Mover para**.
- 4 Selecione o data center virtual para o qual deseja mover o vApp e clique em **OK**.
- 5 (Opcional) Selecione a política de armazenamento.
- 6 Clique em **OK**.

## Resultados

O vApp é removido do data center de origem e movido para o data center de destino.


## Copiar um vApp interrompido para outro data center virtual

Quando você copia um vApp para outro data center virtual, o vApp original permanece no data center virtual de origem.

### Pré-requisitos

- Você deve ser pelo menos um **autor de vApp**.
- O vApp está desligado.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja copiar, selecione **Copiar para**.

- 4 Digite um nome e uma descrição.
- 5 Selecione o data center virtual no qual você deseja criar a cópia do vApp.
- 6 (Opcional) Selecione uma política de armazenamento.
- 7 Clique em **OK**.

#### Resultados

O vApp é copiado com o nome e a descrição que você forneceu para o data center virtual especificado.

## Copiar um vApp ligado


Para criar um vApp com base em um vApp existente, você pode copiar um vApp e alterar essa cópia para que ela atenda às suas necessidades. Não é preciso desligar máquinas virtuais no vApp antes de copiar o vApp. O estado de memória das máquinas virtuais em execução é preservado no vApp copiado.

#### Pré-requisitos

Garanta que as seguintes condições sejam atendidas.

- Você deve ser pelo menos um **usuário de vApp**.
- O backup do data center virtual de organização é feito por meio do vCenter Server 5.5 ou versão posterior.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja copiar, selecione **Copiar para**.
- 4 Digite um nome e uma descrição.
- 5 Selecione o data center virtual no qual você deseja criar a cópia do vApp.
- 6 (Opcional) Selecione uma política de armazenamento.
- 7 Clique em **OK**.

#### Resultados

Uma cópia do vApp é criada e colocada em estado suspenso. O vApp copiado está habilitado para isolamento de rede.

#### Próximo passo

Modifique as propriedades de rede do novo vApp ou ligue o vApp.

# Adicionar uma máquina virtual a um vApp

Você pode adicionar uma máquina virtual a um vApp.

## Pré-requisitos

Você deve ser um **administrador de organização** ou **autor do vApp** para acessar máquinas virtuais em catálogos públicos.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique no  para mostrar os vApps em uma exibição de cartão.

- 3 No menu **Ações** do vApp ao qual você deseja adicionar uma máquina virtual, selecione **Adicionar VM**.

A lista de máquinas virtuais que estão associadas ao vApp é exibida na janela **Adicionar VMs**.

- 4 Para criar uma nova máquina virtual e associá-la ao vApp automaticamente, clique em **Adicionar Máquina Virtual**.

- 5 Insira o nome e o nome do computador da máquina virtual.

---

**Importante** O nome do computador pode conter apenas caracteres alfanuméricos e hífens. Um nome de computador não pode consistir somente em dígitos nem conter espaços.

---

- 6 (Opcional) Insira uma descrição significativa.
- 7 Selecione se deseja que a máquina virtual seja ligada imediatamente após sua criação.

## 8 Selecione como você deseja implantar a máquina virtual.

Opção	Ação
<b>Novo</b>	<p>Implante uma nova máquina virtual com configurações personalizáveis.</p> <ul style="list-style-type: none"> <li>a Selecione uma família de sistemas operacionais e um sistema operacional.</li> <li>b (Opcional) Selecione uma imagem de inicialização.</li> <li>c Selecione a política de Processamento.</li> <li>d Selecione o tamanho da máquina virtual ou clique em <b>Opções de Dimensionamento Personalizadas</b> para inserir manualmente as configurações de processamento, memória e armazenamento.</li> </ul> <p>As opções de dimensionamento predefinidas são pequeno, médio ou grande.</p> <ul style="list-style-type: none"> <li>e Especifique as configurações de armazenamento da máquina virtual, como a política de armazenamento e o tamanho em GB.</li> <li>f Especifique as configurações de rede para a máquina virtual, como rede, modo de IP, endereço IP e NIC primário.</li> </ul>
<b>Modelo de origem</b>	<p>Implante uma máquina virtual de um modelo que você seleciona no catálogo de modelos.</p> <ul style="list-style-type: none"> <li>a Selecione o modelo da máquina virtual no catálogo.</li> <li>b (Opcional) Selecione para usar uma política de armazenamento personalizada e selecione a política em <b>Política de armazenamento personalizada a ser usada</b>.</li> <li>c Se houver um contrato de licença de usuário final disponível, você deverá revisá-lo e aceitá-lo.</li> </ul>

## 9 Clique em **OK** para criar a máquina virtual.

## 10 Clique em **Adicionar** para adicionar a máquina virtual ao vApp.

# Salvar um vApp como um modelo do vApp em um catálogo

Ao adicionar um vApp a um catálogo, você converte o vApp específico em um modelo do vApp.


No VMware Cloud Director 10.2.2, quando você adiciona um vApp a um catálogo, o modelo de vApp inclui as políticas de posicionamento e dimensionamento do vApp de origem como tags não modificáveis.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Autor de vApp** ou um conjunto equivalente de direitos.
- Sua organização deve ter um catálogo e um data center virtual com espaço disponível.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.

- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja adicionar a um catálogo, selecione **Adicionar ao Catálogo**.

**Observação** Você pode adicionar vApps a um catálogo mesmo se as máquinas virtuais que pertencem ao vApp estiverem em execução. No entanto, se você selecionar um vApp em execução, ele será adicionado ao catálogo como um modelo do vApp, e todas as máquinas virtuais estarão em estado suspenso.

- 4 Selecione o catálogo de destino no menu suspenso **Catálogo**.
- 5 Insira um nome e, opcionalmente, uma descrição para o modelo do vApp.
- 6 (Opcional) Selecione **Substituir item de catálogo** se quiser que o novo item de catálogo substitua qualquer modelo do vApp existente e selecione o item de catálogo a ser substituído.

Por exemplo, ao carregar uma nova versão de um vApp no catálogo, talvez você queira substituir a versão antiga.

- 7 Especifique como o modelo deve ser usado.

A configuração se aplica quando você está criando um vApp com base no modelo do vApp. Ela é ignorada quando você cria um vApp usando máquinas virtuais individuais baseadas nesse modelo.

Opção	Descrição
Fazer cópia idêntica	Selecione para fazer uma cópia idêntica do vApp quando você criar um vApp baseado no modelo do vApp.
Personalizar configurações da VM	Selecione para habilitar a personalização das configurações da máquina virtual quando você criar um vApp baseado no modelo do vApp.

- 8 Para concluir a criação do modelo de vApp, clique em **OK**

#### Resultados

O modelo de vApp aparece na catálogo especificado.


## Baixar um vApp como um pacote OVF

Você pode baixar um vApp como um pacote OVF ou como um OVA, que é uma única distribuição de arquivo do mesmo pacote de arquivos OVF.

#### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Autor de vApp** ou um conjunto equivalente de direitos.
- Verifique se a vApp está desligado e desimplantado.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Clique no  para mostrar os vApps em uma exibição de cartão.
- 3 No menu **Ações** do vApp que você deseja baixar, selecione **Baixar**.
- 4 Selecione o formato no qual você deseja baixar o vApp.
- 5 (Opcional) Selecione **Preservar informações de identidade** para incluir os UUIDs e endereços MAC das máquinas virtuais que residem no vApp no pacote OVF baixado.  
Isso limita a portabilidade do pacote e deve ser usado somente quando necessário.
- 6 Clique em **OK** para confirmar a seleção e iniciar o download.

## Resultados

Por padrão, o pacote é baixado na pasta `Downloads` do seu navegador.

# Renovar um lease de vApp

Se a concessão de um vApp tiver expirado ou estiver prestes a expirar, você poderá renová-la.

## Pré-requisitos

Verifique se você recebeu a função predefinida **Usuário vApp** ou um conjunto equivalente de direitos.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Selecione o vApp que deseja renovar.
- 3 No menu **Ações**, selecione **Renovar Lease**.
- 4 Renove a concessão de tempo de execução do vApp.
  - a Marque a caixa de seleção **Concessão de tempo de execução**.
  - b No menu suspenso, selecione um valor para a concessão de tempo de execução.  
Você pode selecionar um valor em horas, dias ou definir a concessão para **Nunca Expira**. **Administradores de sistema** podem limitar o comprimento máximo que você pode escolher.

5 Renove a locação de armazenamento do vApp.

- a Marque a caixa de seleção **Locação de armazenamento**.
- b No menu suspenso, selecione um valor para a locação de armazenamento.

Você pode selecionar um valor em horas, dias ou definir a concessão para **Nunca Expira**. **Administradores de sistema** podem limitar o comprimento máximo que você pode escolher.

## Exclua um vApp

Você pode excluir um vApp, o que o remove da sua organização.

### Pré-requisitos

Seu vApp deve ser interrompido.

Você deve ser pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Selecione o vApp que você deseja excluir.
- 3 No menu **Ações**, selecione **Excluir**.
- 4 Clique em **OK**.

### Resultados

O vApp é excluído.

## Excluir vários vApps

Para remover vários vApps da sua organização, você pode excluí-los simultaneamente.

### Pré-requisitos

- Verifique se os vApps estão interrompidos.
- Verifique se você é pelo menos um **autor de vApp**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, no painel esquerdo, selecione **vApps**.
- 2 Ative a opção **Seleção Múltipla**.
- 3 Selecione os vApps que você deseja excluir.
- 4 No menu **Ações**, selecione **Excluir**.

- 5 Para confirmar, clique em **Excluir**.



# Trabalhando com clusters Kubernetes

## 4

Você pode criar clusters Kubernetes de diferentes tamanhos de nó com base nas políticas existentes do VDC da organização.

Kubernetes Container Clusters são o plug-in do Container Service Extension para o VMware Cloud Director. Você pode usar o plug-in Kubernetes Container Clusters no VMware Cloud Director Tenant Portal para implantar clusters com clusters nativos e VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). Você pode criar clusters Tanzu Kubernetes sem o plug-in Kubernetes Container Clusters.

Quando habilitado em um cluster vSphere, o VMware vSphere® with VMware Tanzu™ fornece a capacidade de criar clusters Kubernetes de upstream em pools de recursos dedicados. Para obter mais informações, consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere.

Quando um provedor de serviços cria uma política do Kubernetes do VDC de provedor e publica essa política em um VDC de organização, ele cria uma política do Kubernetes do VDC de organização. Você pode usar o plug-in Kubernetes Container Clusters para criar clusters do Tanzu Kubernetes, aplicando uma das políticas do Kubernetes do VDC de organização.

## Opções de tempo de execução do Kubernetes

- Clusters do Tanzu Kubernetes - É possível usar a opção de tempo de execução do vSphere Kubernetes para criar clusters do vSphere with VMware Tanzu gerenciados do Tanzu Kubernetes. Essa opção oferece mais recursos, mas pode ser mais cara. Para obter mais informações, consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere.
- Clusters nativos - O plug-in Kubernetes Container Clusters gerencia os clusters com o tempo de execução do Kubernetes nativo. Esses clusters têm uma função de Alta Disponibilidade reduzida com um único nó da camada de controle. Eles oferecem menos opções de volume persistentes e nenhuma automação de rede. No entanto, podem ter um custo mais baixo.
- Clusters TKGI - O VMware Tanzu Kubernetes Grid Integrated Edition é uma solução de contêiner desenvolvida especificamente para operacionalizar o Kubernetes para empresas e provedores de serviços de várias nuvens. Alguns dos seus recursos são alta disponibilidade,

dimensionamento automático, verificações de integridade, bem como atualizações contínuas e de recuperação automática para clusters do Kubernetes. Para obter mais informações sobre clusters TKGI, consulte a documentação do *VMware Tanzu Kubernetes Grid Integrated Edition*.

Este capítulo inclui os seguintes tópicos:

- [Adicionar uma política do Kubernetes do VDC de Organização](#)
- [Editar uma política do Kubernetes do VDC de organização](#)
- [Criar um cluster do Tanzu Kubernetes](#)
- [Criar um cluster do Kubernetes nativo](#)
- [Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition](#)
- [Configurar o acesso externo a um serviço em um cluster Tanzu Kubernetes](#)

## Adicionar uma política do Kubernetes do VDC de Organização

Se você tiver direitos de **administrador de sistema**, poderá adicionar uma política do Kubernetes do VDC de organização usando uma política do Kubernetes do VDC de provedor. É possível usar a política do Kubernetes do VDC de organização para criar clusters do Tanzu Kubernetes.

Ao adicionar ou publicar uma políticas do Kubernetes do VDC de provedor a um VDC de organização, você torna essa política disponível para os tenants, criando uma política de VDC de organização. Os tenants podem usar as políticas do Kubernetes do VDC de organização disponíveis para aproveitar a capacidade do Kubernetes ao criar clusters do Tanzu Kubernetes. Uma política do Kubernetes engloba classes de posicionamento, qualidade de infraestrutura e armazenamento de volume persistente. As políticas do Kubernetes podem ter diferentes limites de processamento.

É possível adicionar várias políticas do Kubernetes do VDC de organização a um único VDC de organização. Você pode usar uma única política do Kubernetes do VDC de provedor para criar várias políticas do Kubernetes do VDC de organização. As políticas do Kubernetes do VDC de organização podem ser usadas como um indicador da qualidade do serviço. Por exemplo, você pode publicar uma política do Kubernetes Gold que permite uma seleção das classes de máquinas garantidas e uma classe de armazenamento rápido ou uma política do Kubernetes Silver que permite uma seleção das classes de máquina de melhor esforço e uma classe de armazenamento lenta.

### Pré-requisitos

- Verifique se você tem uma função de **administrador de sistema** ou uma função que inclua um conjunto equivalente de direitos. Todas as outras funções apenas podem visualizar as políticas do Kubernetes do VDC de organização.
- Verifique se o seu ambiente tem pelo menos um VDC de provedor com o suporte de um Cluster de Supervisor. Os VDCs de provedor com o suporte de um Cluster de Supervisor

são marcados com um ícone do Kubernetes na guia **VDCs de Provedor** do Service Provider Admin Portal. Para obter mais informações sobre o vSphere with VMware Tanzu no VMware Cloud Director, consulte [Usando o vSphere with Kubernetes no VMware Cloud Director](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

- Verifique se você está conectado a um VDC de organização flexível.
- Familiarize-se com os tipos de classe de máquina virtual para clusters do Tanzu Kubernetes. Consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Centro de Dados** e clique em **Centro de Dados Virtual**.
- 2 Selecione um centro de dados virtual de organização.
- 3 No painel esquerdo, em **Configurações**, selecione **Políticas do Kubernetes** e clique em **Adicionar**.

O assistente para **Publicar no VDC de Organização** é exibido.

- 4 Insira um nome e uma descrição visíveis ao tenant para a política do Kubernetes do VDC de organização e clique em **Avançar**.
- 5 Selecione a política do Kubernetes do VDC de provedor que você deseja usar e clique em **Avançar**.
- 6 Selecione limites de CPU e Memória para os clusters do Tanzu Kubernetes criados de acordo com essa política.

Os limites máximos dependem das alocações de Memória e CPU do VDC de organização. Quando você adicionar a política, os limites selecionados atuarão como máximos para os tenants.

- 7 Escolha se deseja reservar a CPU e a memória para os nós de cluster do Tanzu Kubernetes criados nessa política e clique em **Avançar**.

Há duas edições para cada tipo de classe: garantida e melhor esforço. Uma edição de classe garantida reserva totalmente seus recursos configurados, enquanto uma edição de melhor esforço permite que os recursos sejam comprometidos em excesso. Dependendo da sua seleção, na próxima página do assistente, você poderá selecionar entre os tipos de classe de VM da edição garantida ou de melhor esforço.

- Selecione **Sim** para tipos de classe de VM da edição garantida para reservas completas de CPU e Memória.
- Selecione **Não** para tipos de classe de VM da edição de melhor esforço sem reservas de CPU e memória.

- 8 Na página **Classes de máquinas** do assistente, selecione um ou mais tipos de classe de VM disponíveis para essa política.

As classes de máquina selecionadas são os únicos tipos de classe disponíveis para os tenants quando você adiciona a política ao VDC de organização.

- 9 Selecione uma ou mais políticas de armazenamento.
- 10 Revise suas escolhas e clique em **Publicar**.

### Resultados

As informações sobre a política publicada aparecem na lista de políticas do Kubernetes. A política publicada cria um Namespace de Supervisor no Cluster de Supervisor com os limites de recursos especificados da política.

Os tenants podem começar a usar a política do Kubernetes para criar clusters do Tanzu Kubernetes. O VMware Cloud Director coloca cada cluster do Tanzu Kubernetes criado de acordo com essa política do Kubernetes no mesmo Namespace de Supervisor. Os limites de recursos da política se tornam limites de recursos para o Namespace de Supervisor. Todos os clusters do Tanzu Kubernetes criados pelo tenant no Namespace de Supervisor competem pelos recursos dentro desses limites.

### Próximo passo

- Exclua uma política do Kubernetes do VDC de organização.
- Usando o Service Provider Admin Portal, você pode gerenciar cotas de recursos da organização. Consulte [Gerenciar cotas sobre o consumo de recursos de uma organização](#), no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.
- [Gerenciar as cotas de recursos de um grupo](#) ou [Gerenciar as cotas de recursos de um usuário](#)

## Editar uma política do Kubernetes do VDC de organização

Se você tiver direitos de **administrador do sistema**, poderá modificar uma política do Kubernetes do VDC de organização para alterar sua descrição e os limites de CPU e memória.

### Pré-requisitos

Verifique se você tem uma função de **administrador de sistema** ou uma função que inclua um conjunto equivalente de direitos. Todas as outras funções apenas podem visualizar as políticas do Kubernetes do VDC de organização.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Centro de Dados** e clique em **Centro de Dados Virtual**.
- 2 Selecione um centro de dados virtual de organização.
- 3 No painel esquerdo, em **Configurações**, selecione **Políticas do Kubernetes**.

- 4 Selecione a política do Kubernetes do VDC de organização que você deseja editar e clique em **Editar**.

O assistente para **Editar Política do Kubernetes do VDC** é exibido.

- 5 Edite a descrição da política do Kubernetes do VDC de organização e clique em **Avançar**.

O nome da política é vinculado ao Namespace de Supervisor, criado durante a publicação da política, e você não pode alterá-lo.

- 6 Edite o limite de CPU e Memória para a política do Kubernetes do VDC de organização e clique em **Avançar**.

Não é possível editar a reserva de CPU e Memória.

- 7 Revise os detalhes da nova política e clique em **Salvar**.

#### Próximo passo

- Exclua uma política do Kubernetes do VDC de organização.
- Ao usar o Service Provider Admin Portal, você pode alterar cotas de recursos da organização. Consulte [Gerenciar cotas sobre o consumo de recursos de uma organização](#), no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.
- Altere cotas de grupos e usuários. Consulte [Gerenciar as cotas de recursos de um grupo](#) ou [Gerenciar as cotas de recursos de um usuário](#).

## Criar um cluster do Tanzu Kubernetes

Você pode criar clusters do Tanzu Kubernetes usando o plug-in Kubernetes Container Clusters.

Para obter mais informações sobre as diferentes opções de tempo de execução do Kubernetes para a criação do cluster, consulte [Capítulo 4 Trabalhando com clusters Kubernetes](#).

Você também pode gerenciar clusters do Kubernetes usando a CLI do Container Service Extension. Consulte a documentação do [Container Service Extension](#).

O VMware Cloud Director provisiona clusters do Tanzu Kubernetes com PodSecurityPolicy Admission Controller ativado. Você deve criar uma política de segurança de pod para implantar cargas de trabalho. Para obter informações sobre como implementar o uso de políticas de segurança de pod no Kubernetes, consulte o tópico *Usando políticas de segurança de pod com os clusters do Tanzu Kubernetes* na guia *Configuração e Gerenciamento do vSphere with Kubernetes*.

#### Pré-requisitos

- Verifique se seu provedor de serviços publicou o plug-in Kubernetes Container Clusters para sua organização. Você pode encontrar o plug-in na barra de navegação superior em **Mais > Kubernetes Container Clusters**.

- Verifique se você tem pelo menos uma política do Kubernetes do VDC de organização no VDC da sua organização. Para adicionar uma política do Kubernetes do VDC de organização, consulte [Adicionar uma política do Kubernetes do VDC de Organização](#).
- Verifique se o seu provedor de serviços publicou o pacote de direitos **vmware:tkgcluster Entitlement** para a sua organização e lhe concedeu o direito **Edit: Tanzu Kubernetes Guest Cluster** para criar e modificar os clusters do Tanzu Kubernetes. Para a capacidade de excluir clusters, você deve ter o direito **Full Control: Tanzu Kubernetes Guest Cluster**.
- Verifique se o seu provedor de serviços criou uma entrada da Lista de Controle de Acesso (ACL) para você com informações sobre o seu nível de acesso.

## Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Kubernetes Container Clusters**.
- 2 (Opcional) Se o VDC de organização estiver ativado para a criação de cluster do TKGI, na página **Kubernetes Container Clusters**, selecione a guia **vSphere with Tanzu e Nativo**.
- 3 Clique em **Novo**.
- 4 Selecione a opção de tempo de execução do **vSphere with Tanzu** e clique em **Avançar**.
- 5 Insira um nome para o novo cluster do Kubernetes e clique em **Avançar**.
- 6 Selecione o VDC de organização para o qual você deseja implantar um cluster do Tanzu Kubernetes e clique em **Avançar**.
- 7 Selecione uma política do Kubernetes do VDC de organização e uma versão do Kubernetes e clique em **Avançar**.

VMware Cloud Director exibe um conjunto padrão de versões do Kubernetes que não estão ligadas a nenhum VDC de organização ou política do Kubernetes. Essas versões são uma configuração global. Para alterar a lista de versões disponíveis, use a ferramenta de gerenciamento de células para executar o comando `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` com números de versão separados por vírgula.

- 8 Selecione o número da camada de controle e os nós de trabalhador no novo cluster.
- 9 Selecione as classes de máquina para a camada de controle e os nós de trabalhador e clique em **Avançar**.
- 10 Selecione uma classe de armazenamento de política Kubernetes para a camada de controle e os nós de trabalhador e clique em **Próximo**.
- 11 (Opcional) Para o VMware Cloud Director 10.2.2 e versões posteriores, especifique um intervalo de endereços IP para serviços Kubernetes e um intervalo para pods Kubernetes e clique em **Avançar**.

O roteamento entre domínios sem classe (CIDR) é um método para alocação de endereços IP e roteamento de IP.

Opção	Descrição
<code>Pods CIDR</code>	Especifica um intervalo de endereços IP a ser usado para pods Kubernetes. O valor padrão é 192.168.0.0/16. O tamanho da sub-rede de pods deve ser igual ou superior a /24. Esse valor não deve se sobrepor às configurações do cluster supervisor. Você pode inserir um único intervalo de IDs.
<code>Services CIDR</code>	Especifica um intervalo de endereços IP a ser usado para serviços Kubernetes. O valor padrão é 10.96.0.0/12. Esse valor não deve se sobrepor às configurações do cluster supervisor. Você pode inserir um único intervalo de IDs.

12 Analise as configurações do cluster e clique em **Concluir**.

#### Próximo passo

- Redimensione o cluster do Kubernetes se quiser alterar o número de nós de trabalho.
- Baixe o arquivo kubeconfig. A ferramenta de linha de comando kubectl usa arquivos kubeconfig para obter informações sobre clusters, usuários, namespaces e mecanismos de autenticação.
- Exclua um cluster do Kubernetes.

## Criar um cluster do Kubernetes nativo

Você pode criar clusters do Kubernetes gerenciados pelo Container Service Extension 3.0 usando o plug-in Kubernetes Container Clusters.

Para obter mais informações sobre as diferentes opções de tempo de execução do Kubernetes para a criação do cluster, consulte [Capítulo 4 Trabalhando com clusters Kubernetes](#).

Você também pode gerenciar clusters do Kubernetes usando a CLI do Container Service Extension. Consulte a documentação do [Container Service Extension](#).

#### Pré-requisitos

- Verifique se seu provedor de serviços publicou o plug-in Kubernetes Container Clusters para sua organização. Kubernetes Container Clusters são o plug-in do Container Service Extension para o VMware Cloud Director. Você pode encontrar o plug-in na barra de navegação superior em **Mais > Kubernetes Container Clusters**.
- Verifique se o seu provedor de serviços concluiu a configuração do servidor Container Service Extension 3.0 e publicou uma política de colocação nativa do Container Service Extension no VDC de organização.
- Verifique se o seu provedor de serviços publicou o pacote de direitos **cse:nativeCluster Entitlement** para a sua organização e lhe concedeu o direito **Edit CSE:NATIVECLUSTER** para criar e modificar clusters do Kubernetes nativos. Para a capacidade de excluir clusters, você deve ter o direito **Full Control CSE:NATIVECLUSTER**.

- Verifique se o seu provedor de serviços criou uma entrada da Lista de Controle de Acesso (ACL) para você com informações sobre o seu nível de acesso.

#### Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Kubernetes Container Clusters**.
- 2 (Opcional) Se o VDC de organização estiver ativado para a criação de cluster do TKGI, na página **Kubernetes Container Clusters**, selecione a guia **vSphere with Tanzu e Nativo**.
- 3 Clique em **Novo**.
- 4 Selecione a opção de tempo de execução do Kubernetes **Nativo**.
- 5 Insira um nome e selecione um Modelo de Kubernetes na lista.
- 6 (Opcional) Insira uma descrição para o novo cluster do Kubernetes e uma chave pública SSH.
- 7 Clique em **Avançar**.
- 8 Selecione o VDC de organização para o qual você deseja implantar um cluster nativo e clique em **Avançar**.
- 9 Selecione o número da camada de controle e os nós de trabalhador e, opcionalmente, as políticas de dimensionamento para os nós.
- 10 Clique em **Avançar**.
- 11 Se você quiser implantar uma VM adicional com o software NFS, ative a opção **Ativar NFS**.
- 12 (Opcional) Selecione as políticas de armazenamento para a camada de controle e os nós de trabalhador.
- 13 Clique em **Avançar**.
- 14 Selecione uma rede para o cluster do Kubernetes e clique em **Avançar**.
- 15 Analise as configurações do cluster e clique em **Concluir**.

#### Próximo passo

- Redimensione o cluster do Kubernetes se quiser alterar o número de nós de trabalho.
- Baixe o arquivo kubeconfig. A ferramenta de linha de comando kubectl usa arquivos kubeconfig para obter informações sobre clusters, usuários, namespaces e mecanismos de autenticação.
- Exclua um cluster do Kubernetes.

## Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition

Você pode criar clusters do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) usando o Container Service Extension.



Para obter mais informações sobre as diferentes opções de tempo de execução do Kubernetes para a criação do cluster, consulte [Capítulo 4 Trabalhando com clusters Kubernetes](#).

Você também pode gerenciar clusters do Kubernetes usando a CLI do Container Service Extension. Consulte a documentação do [Container Service Extension](#).

### Pré-requisitos

- Verifique se seu provedor de serviços publicou o plug-in Kubernetes Container Clusters para sua organização. Kubernetes Container Clusters são o plug-in do Container Service Extension para o VMware Cloud Director. Você pode encontrar o plug-in na barra de navegação superior em **Mais > Kubernetes Container Clusters**.
- Verifique se o seu provedor de serviços concluiu a configuração do servidor Container Service Extension 3.0 e publicou metadados de ativação de TKGI do Container Service Extension no VDC de organização.
- Verifique se você tem o direito **{cse}:PKS DEPLOY RIGHT**.

### Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Kubernetes Container Clusters**.
- 2 Na página **Kubernetes Container Clusters**, selecione a guia **TKGI** e clique em **Novo**.  
O assistente para **Criar Novo Cluster do TKGI** é aberto.
- 3 Selecione o VDC de organização para o qual você deseja implantar um cluster do TKGI e clique em **Avançar**.  
A lista pode demorar mais para ser carregada porque o VMware Cloud Director solicita as informações do servidor CSE.
- 4 Insira um nome para o novo cluster do TKGI e selecione o número de nós de trabalhador.  
Os clusters do TKGI devem ter pelo menos um nó de trabalhador.
- 5 Clique em **Avançar**.
- 6 Analise as configurações do cluster e clique em **Concluir**.
- 7 (Opcional) Clique no botão **Atualizar** no lado direito da página para que o novo cluster do TKGI apareça na lista de clusters.

### Próximo passo

- Redimensione o cluster do Kubernetes se quiser alterar o número de nós de trabalho.
- Baixe o arquivo kubeconfig. A ferramenta de linha de comando kubectl usa arquivos kubeconfig para obter informações sobre clusters, usuários, namespaces e mecanismos de autenticação.
- Exclua um cluster do Kubernetes.

## Configurar o acesso externo a um serviço em um cluster Tanzu Kubernetes

A partir do VMware Cloud Director 10.2.2, os clusters Tanzu Kubernetes são, por padrão, acessíveis apenas em sub-redes de IP que fazem parte de redes no mesmo centro de dados virtual da organização no qual esses clusters são criados. Se necessário, você pode configurar manualmente o acesso externo a serviços específicos em um cluster Tanzu Kubernetes.

Quando uma política Kubernetes de VDC é publicada em um VDC da organização, uma política de firewall é provisionada automaticamente no edge gateway do cluster para permitir o acesso a esse cluster por fontes autorizadas no VDC. Além disso, uma regra de SNAT do sistema é automaticamente adicionada aos edge gateways do NSX-T Data Center dentro do VDC da organização para garantir que o edge gateway do cluster seja acessível pelas cargas de trabalho no VDC da organização.

---

**Observação** Se o centro de dados virtual da organização fizer parte de um grupo do NSX-T Data Center, o edge gateway do cluster não poderá ser acessado pelos outros VDCs no grupo de centros de dados.

---

A política de firewall provisionada no edge gateway do cluster e a regra de SNAT no edge gateway do NSX-T Data Center só poderão ser removidas se um **administrador do sistema** excluir a política Kubernetes do VDC.

Se necessário, você pode configurar manualmente o acesso de uma rede externa a um serviço específico em um cluster Tanzu Kubernetes. Para fazer isso, é necessário criar uma regra de DNAT no edge gateway do NSX-T Data Center que garanta que o tráfego proveniente de localizações externas seja encaminhado ao edge gateway do cluster.

### Pré-requisitos

- Verifique se a sua infraestrutura em nuvem tem o suporte do vSphere 7.0 Update 1C, 7.0 Update 2 ou posterior. Entre em contato com o **administrador do sistema**.
- Verifique se você é um **administrador da organização**.
- Verifique se o **administrador do sistema** criou um edge gateway do NSX-T Data Center dentro do centro de dados virtual da organização no qual o cluster Tanzu Kubernetes está localizado.
- Verifique se o endereço IP público que você deseja usar para o serviço foi alocado à interface do edge gateway na qual você deseja adicionar uma regra de DNAT.
- Use o comando `get services my-service` da ferramenta de linha de comando `kubectl` para recuperar o IP externo do serviço que você deseja expor.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway e, em **Serviços**, clique em **NAT**.

- 3 Para adicionar uma regra, clique em **Novo**.
- 4 Configure uma regra de DNAT para o serviço que você deseja conectar a uma rede externa.

Opção	Descrição
Nome	Insira um nome significativo para a regra.
Descrição	(Opcional) Insira uma descrição para a regra.
Estado	Para ativar a regra após a criação, ligue o botão de alternância <b>Estado</b> .
Tipo de interface	No menu suspenso, selecione DNAT.
IP Externo	Insira o endereço IP público do serviço. O endereço IP inserido deve pertencer ao intervalo de IPs subalocado do edge gateway do NSX-T Data Center.
Aplicativo	Deixe a caixa vazia.
IP Interno	Insira o endereço IP do serviço que foi alocado do pool de entrada Kubernetes.
Porta interna	(Opcional) Insira um número de porta ao qual o tráfego de entrada é direcionado.
Log	(Opcional) Para que a conversão de endereço realizada por essa regra seja registrada, ative a opção <b>Log</b> .

- 5 Clique em **Salvar**.

#### Próximo passo

Se quiser fornecer acesso a outros aplicativos publicados como serviços Kubernetes de redes externas, deverá configurar regras de DNAT adicionais para cada uma deles.

# Como trabalhar com redes

# 5

Para fornecer uma infraestrutura de rede altamente flexível e segura em um ambiente de nuvem com várias finalidades, o VMware Cloud Director usa uma arquitetura de rede em camadas com quatro categorias de redes. As categorias de rede são redes externas, redes de centros de dados virtuais (VDCs) de organização, redes de grupos de centros de dados e redes de vApps. A maioria dos tipos de redes do VMware Cloud Director requer objetos de infraestrutura adicionais, como edge gateways e pools de redes.

## Redes Externas

Uma rede externa fornece uma interface de uplink que conecta redes e máquinas virtuais no ambiente do VMware Cloud Director a redes externas, como uma VPN, uma intranet corporativa ou a Internet pública.

Uma rede externa é apoiada por uma única rede do vSphere, por várias redes do vSphere ou por um roteador lógico de camada 0 do NSX-T Data Center.

Apenas um **administrador do sistema** pode criar uma rede externa. Para obter informações sobre redes externas, consulte *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

## Pools de Redes

Um pool de redes é uma coleção de segmentos de rede isolados de camada 2 que você pode usar para criar redes do vApp e certos tipos de redes de VDCs de organização sob demanda.

Os pools de redes devem ser criados antes das redes de VDCs de organização e das redes de vApps. Se eles não existirem, a única opção de rede disponível para uma organização será a conexão direta com uma rede externa.

Apenas um **administrador do sistema** pode criar um pool de redes.

Para obter informações sobre pools de redes, consulte *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

## Redes VDC da organização

Redes de centros de dados virtuais (VDCs) de organização permitem que vApps se comuniquem entre si ou com redes externas fora da organização.

Dependendo da conexão da rede de VDC de organização com uma rede externa, existem vários tipos diferentes de redes de VDC de organização.

Redes de VDCs de organização fornecem conexões diretas ou roteadas para redes externas ou podem ser isoladas de redes externas e outras redes de VDCs de organização. Conexões roteadas exigem um edge gateway e um pool de redes no VDC de organização.

Um **administrador do sistema** ou um **administrador da organização** cria redes de VDC de organização e as atribui à sua organização.

Um VDC de organização criado recentemente não tem redes disponíveis. Depois que um **administrador do sistema** cria a infraestrutura de rede necessária, um **administrador da organização** pode criar e gerenciar a maioria dos tipos de redes de VDC de organização.

## Redes de grupo de centros de dados com suporte do NSX Data Center for vSphere

Uma rede com suporte do NSX Data Center for vSphere que abrange um grupo de centros de dados. Um grupo de centros de dados pode abranger de um a 16 VDCs da organização em uma implantação do VMware Cloud Director única ou multissite.

## Redes de grupo de centros de dados com suporte do NSX-T Data Center

Redes de grupos de centros de dados são um tipo de redes de VDC de organização que são compartilhadas entre um ou mais VDCs e com as quais os vApps podem se conectar.

Um **administrador do sistema** ou um **administrador da organização** cria redes de grupos de centros de dados e define seu escopo a um único grupo de VDCs.

O VMware Cloud Director é compatível com redes isoladas, importadas, diretas e roteadas de grupos de centros de dados com o suporte do NSX-T Data Center.

## Redes do vApp

Redes de vApps permitem que as máquinas virtuais se comuniquem entre si ou, por meio da conexão com uma rede de VDCs de organização, a máquinas virtuais em outros vApps.

Uma rede do vApp isolada está contida em um vApp. Uma rede de vApps pode ser isolada de outras redes ou conectada a uma rede de VDCs de organização.

Cada vApp contém uma rede de vApp. A rede é criada quando o vApp é implantado e apagado quando o vApp é desimplantado.

Um **administrador da organização** configura e controla redes de vApps.

## Tipos de redes em um vApp

As máquinas virtuais em um vApp podem se conectar a redes do vApp, que podem ser isoladas, diretas ou roteadas, e para as redes de VDCs de organização.

---

**Observação** VDCs de organização com o suporte do NSX Data Center for vSphere são compatíveis com redes de vApps roteadas, isoladas e diretas.

VDCs de organização com o suporte do NSX-T Data Center são compatíveis com redes de vApps isoladas e diretas.

---

Você pode adicionar redes de diferentes tipos a um vApp para abordar vários cenários de rede.

As máquinas virtuais no vApp podem se conectar às redes que estão disponíveis em um vApp. Se você deseja conectar uma máquina virtual a uma rede diferente, deve primeiro adicionar essa rede ao vApp.

Um vApp pode incluir redes do vApp e redes de VDCs de organização. Uma rede vApp isolada está contida no vApp.

Você também pode rotear uma rede de vApps para uma rede de VDCs de organização para fornecer conectividade a máquinas virtuais fora do vApp. Para redes vApp roteadas, você pode configurar serviços de rede, como um firewall e roteamento estático.

Você pode conectar um vApp diretamente a uma rede de VDCs de organização.

Se você tiver vários vApps que contenham máquinas virtuais idênticas conectadas à mesma rede de VDCs de organização e quiser iniciar os vApps ao mesmo tempo, poderá isolar o vApp. O isolamento do vApp permite que você ligue as máquinas virtuais sem conflito, isolando seus endereços MAC e IP.

Para obter informações, consulte [Trabalhando com redes em um vApp](#).

## Edge Gateways

Um edge gateway oferece uma rede de VDCs de organização roteada que possui conectividade com redes externas e pode fornecer serviços, como balanceamento de carga, conversão de endereços de rede (NAT) e firewall. O VMware Cloud Director oferece suporte aos edge gateways IPv4 e IPv6.

Os edge gateways exigem NSX Data Center for vSphere ou NSX-T Data Center.

Este capítulo inclui os seguintes tópicos:

- [Gerenciando redes de centros de dados virtuais de organização](#)
- [Gerenciamento de rede de grupo de centros de dados com o NSX-T Data Center](#)
- [Gerenciamento de rede de grupo de centros de dados com o NSX Data Center for vSphere](#)

- [Gerenciando serviços de edge gateway do NSX Data Center for vSphere](#)
- [Gerenciando Edge Gateways do NSX-T Data Center](#)

## Gerenciando redes de centros de dados virtuais de organização

Um **administrador do sistema** ou um **administrador da organização** cria redes de VDC de organização e as atribui ao seu VDC de organização ou a um grupo de VDCs de organização.

Um **administrador da organização** pode visualizar informações sobre redes, configurar serviços de rede e muito mais.

Você pode usar redes de VDC diretas, roteadas, isoladas ou de organizações de grupos de centros de dados com suporte do NSX Data Center for vSphere.

Você pode usar redes de VDC de organização roteadas, isoladas, importadas e diretas com o suporte do NSX-T Data Center. Você também pode usar redes de grupos de centros de dados virtuais roteadas, isoladas e importadas com suporte do NSX-T Data Center.

Tabela 5-1. Tipos de redes de VDC de organização

Rede do tipo de centros de dados	Descrição
Direto	<p>Uma rede de VDC de organização com uma conexão direta com uma das redes externas que são provisionadas pelo <b>administrador do sistema</b> e com suporte dos recursos do vSphere.</p> <p>Redes diretas têm suporte para VDCs da organização com o suporte do NSX Data Center for vSphere e, no VMware Cloud Director 10.2.2, para VDCs da organização com o suporte do NSX-T Data Center.</p> <p>As redes diretas podem ser acessadas por vários VDCs de organização.</p> <p>As máquinas virtuais que pertencem a diferentes VDCs de organização podem se conectar e ver o tráfego nesta rede.</p> <p>Uma rede direta fornece conectividade direta na camada 2 às máquinas virtuais fora do VDC de organização. As máquinas virtuais fora desse VDC da organização podem se conectar às máquinas virtuais no VDC da organização diretamente.</p> <hr/> <p><b>Observação</b> Somente um <b>administrador do sistema</b> pode adicionar uma rede do VDC de organização direta.</p> <hr/> <p>Pode ser IPv4 ou IPv6.</p>
Isolada (interna)	<p>As redes isoladas são acessíveis apenas pelo mesmo VDC de organização. Apenas as máquinas virtuais dessa organização podem se conectar ao VDC e ver o tráfego na rede do VDC de organização interna.</p> <p>Redes isoladas são compatíveis com VDCs de organização com suporte do NSX-T Data Center e para o VDC de organização do NSX Data Center for vSphere.</p> <p>A rede do VDC de organização isolada fornece um VDC da organização com uma rede privada isolada que várias máquinas virtuais e vApps podem conectar. Essa rede não fornece conectividade com máquinas virtuais fora do VDC da organização. Máquinas fora do VDC da organização não têm conectividade com máquinas no VDC da organização.</p>

Tabela 5-1. Tipos de redes de VDC de organização (continuação)

Rede do tipo de centros de dados	Descrição
Roteado	<p>As redes roteadas são acessíveis apenas pelo mesmo VDC de organização. Apenas as máquinas virtuais nesse VDC da organização podem se conectar a essa rede.</p> <p>Essa rede também fornece acesso controlado a uma rede externa. Como um <b>administrador do sistema</b> ou um <b>administrador da organização</b>, você pode configurar a conversão de endereços de rede (NAT) e as configurações de firewall e VPN para máquinas virtuais específicas acessíveis pela rede externa.</p> <p>Pode ser IPv4 ou IPv6.</p>
Comutador lógico importado do NSX-T Data Center	<p>Redes importadas do NSX-T Data Center são segmentos lógicos criados no NSX-T Data Center e usam um comutador lógico do NSX-T Data Center existente. Elas são importadas em uma organização específica como rede de VDC de organização.</p> <p><b>Observação</b> Apenas um <b>administrador do sistema</b> pode importar uma rede do NSX-T Data Center.</p>
Redes de grupo de centros de dados com suporte do NSX Data Center for vSphere	<p>Esta rede é parte de uma rede de grupo de centros de dados que abrange um grupo de centros de dados. Um grupo de centros de dados pode abranger de um a 16 VDCs da organização em uma implantação do VMware Cloud Director única ou multissite.</p> <p>As máquinas virtuais conectadas a essa rede estão conectadas à rede estendida subjacente.</p>
Redes de grupo de centros de dados com suporte do NSX-T Data Center	<p>As redes de grupo de centros de dados são um tipo de redes de VDC de organização com suporte do NSX-T Data Center que são compartilhadas entre um ou mais VDCs e com as quais os vApps podem se conectar.</p> <p>As redes de grupos de centros de dados podem ser isoladas, importadas ou roteadas e exigir o NSX-T Data Center.</p>

Todas as etapas para gerenciar as redes de VDC da sua organização são documentadas, supondo que você tenha mais de um VDC no seu ambiente.

## Visualizar as redes VDC da organização disponíveis

Você pode visualizar as redes de centros de dados virtuais da organização que estão disponíveis.

### Pré-requisitos

Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.

### Procedimentos

- ◆ Na barra de navegação superior, clique em **Rede**.

### Resultados

Na guia **Redes**, você vê uma lista das redes disponíveis que você pode filtrar por vários critérios.

### Próximo passo

Você pode adicionar uma rede de VDC da organização. Você também pode editar, aumentar o escopo, excluir ou redefinir uma rede de VDC da organização que já existe.



## Adicionar uma rede isolada de data center virtual da organização

Você pode adicionar uma rede isolada de VDC da organização, que é acessível somente por essa organização. Essa rede não fornece conectividade com máquinas fora dessa organização. As máquinas virtuais fora dessa organização não têm conectividade com as máquinas virtuais da organização.

Você pode adicionar uma combinação de redes de VDC isoladas e roteadas da organização para atender às necessidades da sua organização. Por exemplo, pode isolar uma rede que contenha informações confidenciais e ter uma rede separada que esteja associada a um edge gateway e conectada à Internet.

Você pode criar uma rede de VDC isolada com suporte de um pool de rede. Seu provedor de serviços também pode criar uma rede de VDC isolada com suporte de um switch lógico do NSX-T.

Você pode criar apenas uma rede do VDC de organização isolada IPv4.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Centro de Dados Virtual da Organização**, selecione o VDC no deseja qual criar a rede e clique em **Avançar**.
- 4 Na página **Selecionar o Tipo de Rede**, selecione **Isolada** e clique em **Avançar**.
- 5 Insira um nome relevante para a rede.
- 6 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 7 Insira uma descrição da rede de VDC da organização.
- 8 (Opcional) Se o VDC no qual você criar a rede tiver o suporte do NSX Data Center for vSphere, alterne a opção **Compartilhado** para tornar a rede de VDC de organização disponível para outros VDCs de organização na mesma organização.

Essa opção pode ser usada, por exemplo, quando um aplicativo em um VDC de organização tem uma reserva ou um pool de alocações definido como o modelo de alocação. Nesse caso, talvez não haja espaço suficiente para executar mais máquinas virtuais. Como solução, você pode criar um VDC da organização secundário com pagamento por consumo e executar temporariamente mais máquinas virtuais nessa rede.

---

**Observação** Os VDCs da organização devem ter suporte do mesmo VDC do provedor.

---

9 Clique em **Avançar**.

10 (Opcional) Para reservar um ou mais endereços IP para atribuição a máquinas virtuais que exigem endereços IP estáticos, configure os **Pools de IPs Estáticos** para a rede.

a Insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.

Para adicionar vários endereços IP ou intervalos estáticos, repita essa etapa.

b (Opcional) Para modificar ou remover endereços IP e intervalos, clique em **Modificar** ou **Remover**.

11 Clique em **Avançar**.

12 (Opcional) Defina as configurações de DNS.

Opção	Ação
DNS Primário	Insira o endereço IP do servidor DNS primário.
DNS Secundário	Insira o endereço IP do seu servidor DNS secundário.
Sufixo DNS	Insira seu sufixo DNS. O sufixo DNS é o nome DNS sem incluir o nome do host.

13 Clique em **Avançar**.

14 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Adicionar uma rede roteada de VDC da organização

Para controlar o acesso a uma rede externa, você pode adicionar uma rede roteada de VDC da organização. Os **administradores de sistema** e os **administradores de organização** podem configurar a conversão de endereços de rede (NAT) e as configurações de firewall e VPN para máquinas virtuais específicas acessíveis pela rede externa.

Você pode adicionar uma combinação de redes roteadas e isoladas de VDC da organização para atender às necessidades da sua organização. Por exemplo, pode adicionar uma rede associada a um edge gateway e conectada à Internet e ter uma rede isolada com informações confidenciais.

É possível adicionar uma rede roteada IPv4 ou IPv6 de VDC da organização .

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

1 Na barra de navegação superior, clique em **Rede**.

2 Na guia **Redes**, clique em **Novo**.

3 Na página **Escopo**, selecione **Centro de Dados Virtual da Organização**, selecione o VDC no deseja qual criar a rede e clique em **Avançar**.

- 4 Na página **Selecionar o Tipo de Rede**, selecione **Roteada** e clique em **Avançar**.
- 5 Insira um nome relevante para a rede.
- 6 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 7 Insira uma descrição da rede de VDC da organização.
- 8 (Opcional) Se o VDC no qual você criar a rede tiver o suporte do NSX Data Center for vSphere, alterne a opção **Compartilhado** para tornar a rede de VDC de organização disponível para outros VDCs de organização na mesma organização.

Essa opção pode ser usada, por exemplo, quando um aplicativo em um VDC da organização tem uma reserva ou um pool de alocações definido como o modelo de alocação. Nesse caso, talvez não haja espaço suficiente para executar mais máquinas virtuais. Como solução, você pode criar um VDC da organização secundário com pagamento por consumo e executar temporariamente mais máquinas virtuais nessa rede.

---

**Observação** Os VDCs da Organização devem compartilhar o mesmo pool de redes.

---

- 9 Clique em **Avançar**.
- 10 Na página **Conexão do Edge**, selecione um edge gateway ao qual associar a rede de VDC da organização.  
  
Se o VDC da organização incluir mais de um edge gateway, você deverá selecionar um edge gateway para esta rede para a conexão. Para poder suportar outra rede roteada, o Edge Gateway deve mostrar um valor de pelo menos 1 na coluna N° de Redes Disponíveis.
- 11 No menu suspenso **Tipo de Interface**, selecione o tipo de interface.

Opção	Descrição
<b>Interno</b>	Conecta-se a uma das interfaces internas do edge gateway. O número máximo de redes permitidas é 9.
<b>Distribuído</b>	Cria a rede em um roteador lógico distribuído conectado a esse edge gateway. O número máximo de redes permitidas é 400.
<b>Subinterface</b>	Estende uma rede de VDC da organização. O VMware Cloud Director identifica a rede a ser usada para se estender pela VPN L2. O VMware Cloud Director, com a ajuda do NSX Network Virtualization, cria um tipo de interface de tronco para essa rede. O número máximo de redes permitidas é 200.

- 12 (Opcional) Para ativar a marcação de VLANs convidadas nesta rede, ative a opção **VLAN Convidada Permitida**.
- 13 Clique em **Avançar**.

- 14 (Opcional) Para reservar um ou mais endereços IP para atribuição a máquinas virtuais que exigem endereços IP estáticos, configure os **Pools de IPs Estáticos** para a rede.
  - a Insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.  
Para adicionar vários endereços IP ou intervalos estáticos, repita essa etapa.
  - b (Opcional) Para modificar ou remover endereços IP e intervalos, clique em **Modificar** ou **Remover**.
- 15 Clique em **Avançar**.
- 16 (Opcional) Defina as configurações de DNS.

Opção	Ação
DNS Primário	Insira o endereço IP do servidor DNS primário.
DNS Secundário	Insira o endereço IP do seu servidor DNS secundário.
Sufixo DNS	Insira seu sufixo DNS. O sufixo DNS é o nome DNS sem incluir o nome do host.

- 17 Clique em **Avançar**.
- 18 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Adicionar uma rede direta de data center virtual da organização

Para se conectar a uma rede externa por uma rota direta, os **Administradores do Sistema** podem configurar uma conexão direta.

No VMware Cloud Director 10.2.2, a criação de redes diretas é compatível em VDCs da organização com suporte do NSX-T Data Center e do NSX Data Center for vSphere.

Se você fizer login no portal de tenant do VMware Cloud Director como um **administrador de organização** e tentar criar uma rede direta de data center virtual da organização, receberá uma mensagem de aviso informando que não possui direitos suficientes.

### Pré-requisitos

Verifique se você tem direitos de **administrador do sistema**.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Centro de Dados Virtual da Organização**, selecione o VDC no deseja qual criar a rede e clique em **Avançar**.
- 4 Na página **Tipo de Rede**, selecione **Direta** e clique em **Avançar**.
- 5 Insira um nome relevante para a rede.
- 6 Insira uma descrição da rede de VDC da organização.

- 7 (Opcional) Para tornar a rede de VDC da organização disponível para outros VDCs na mesma organização, ative a opção **Compartilhada**.
- 8 Na página **Conexão de Rede Externa**, selecione a rede externa à qual deseja que sua nova rede do data center virtual da organização se conecte diretamente e clique em **Avançar**.
- 9 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Adicionar uma rede de VDC de organização com um comutador lógico do NSX-T Data Center importado

Os **administradores do sistema** podem criar uma rede de VDC de organização importando um comutador lógico de uma instância associada do NSX-T Manager.

### Pré-requisitos

- Verifique se você tem direitos de **administrador do sistema**.
- Verifique se o centro de dados virtual do provedor que oferece suporte ao centro de dados virtual da organização de destino está associado a uma instância do NSX-T Manager.
- Você deve criar pelo menos um comutador lógico do NSX-T que não esteja sendo usado por outras redes de centros de dados virtuais da organização.

Para obter informações sobre como criar e configurar os comutadores lógicos do NSX-T, consulte *Guia de administração do NSX-T Data Center*.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Centro de Dados Virtual da Organização**, selecione o VDC no deseja qual criar a rede e clique em **Avançar**.
- 4 Na página **Tipo de Rede**, selecione **Importada**, escolha **Comutador Lógico NSX-T** e clique em **Avançar**.
- 5 Na lista de comutadores lógicos de NSX-T disponíveis, selecione o comutador de destino e clique em **Avançar**.
- 6 Insira um nome relevante para a rede.
- 7 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.  
Se o comutador estiver configurado com uma sub-rede, essas informações serão preenchidas automaticamente.
- 8 Insira uma descrição da rede de VDC da organização.
- 9 Clique em **Avançar**.

**10** (Opcional) Defina as configurações de DNS e o pool de IP estático.

Você pode adicionar vários endereços IP e intervalos de IP.

**11** Clique em **Avançar**.

**12** Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Editar as configurações gerais de uma rede de data center virtual da organização

Você pode modificar as propriedades de redes de VDC da organização.

### Pré-requisitos

Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.

### Procedimentos

**1** Na barra de navegação superior, clique em **Rede**.

**2** Na guia **Redes**, clique no nome da rede de VDC de organização que você deseja editar.

**3** Na guia **Geral**, clique em **Editar**.

a Edite o nome e a descrição da rede.

b Se o VDC no qual você criou a rede tiver o suporte do NSX Data Center for vSphere, ative ou desative a opção **Compartilhado** para tornar a rede de VDC de organização disponível para outros VDCs de organização na mesma organização.

**4** Clique em **Salvar**.

## Conectar uma rede de centro de dados virtual da organização a um edge gateway

Depois de criar uma rede de VDC de organização, você pode conectar a rede a um edge gateway.

A partir da versão 10.1, o VMware Cloud Director oferece suporte à conexão a um edge gateway para redes de VDC de organização que são apoiadas por NSX Data Center for vSphere ou NSX-T Data Center.

### Pré-requisitos

Essa operação requer uma das funções predefinidas de **administrador da organização** ou **administrador do sistema** ou uma função que inclua os direitos **Rede de VDC de Organização: Editar Propriedades** e **Grupo de VDCs: Exibir** publicados na organização.

### Procedimentos

**1** Na barra de navegação superior, clique em **Rede**.

**2** Clique no nome da rede de VDC de organização que você deseja conectar a um gateway de borda.

- 3 Na guia **Geral**, clique em **Editar**.
- 4 Clique em **Conexão**.
- 5 Conecte a rede a um edge gateway.
  - a Ative a opção **Conectar-se a um edge gateway**.
  - b Selecione o edge gateway ao qual se conectar na lista de edge gateways disponíveis.
  - c Selecione o tipo de interface.
  - d Para permitir uma VLAN convidada, alterne a opção **VLAN convidada permitida**.
- 6 Clique em **Salvar**.

#### Resultados

A rede de VDC de organização se conecta a um gateway de borda e é convertida de isolada em roteada.

## Desconectar uma rede de VDC de organização de um edge gateway

Ao desconectar uma rede de VDC de organização de um edge gateway, você pode convertê-la de roteada para isolada.

A partir da versão 10.1, a conexão e a desconexão de um edge gateway é compatível com as redes de VDC de organização que são apoiadas por NSX Data Center for vSphere ou NSX-T Data Center.

#### Pré-requisitos

Esta operação requer uma das funções predefinidas **administrador da organização** ou **administrador do sistema** ou uma função que inclua a **Rede de VDC de Organização: Editar Propriedades** certa.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede de VDC de organização que você deseja desconectar.
- 3 Na guia **Geral**, clique em **Editar**.
- 4 Clique em **Conexão**.
- 5 Para desconectar a rede do edge gateway, desative a opção **Conectar-se a um edge gateway**.
- 6 Clique em **Salvar**.

#### Resultados

Você desconectou a rede de VDC de organização de um edge gateway. A rede de VDC de organização é convertida de roteada para isolada.

## Converter a interface de uma rede do VDC de organização roteada

Você pode alterar a interface de uma rede de roteamento interno para subinterface ou distribuído, por exemplo, editando as propriedades de rede.

**Observação** As redes entre VDCs não podem ser convertidas.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede do VDC de organização que você deseja editar.
- 3 Na guia **Geral**, clique em **Editar**.
- 4 Clique em **Conexão**.
- 5 No menu suspenso **Tipo de Interface**, selecione o tipo de interface.

Opção	Descrição
<b>Interno</b>	Conecta-se a uma das interfaces internas do edge gateway. O número máximo de redes permitidas é 9.
<b>Distribuído</b>	Cria a rede em um roteador lógico distribuído conectado a esse edge gateway. O número máximo de redes permitidas é 400.
<b>Subinterface</b>	Estende uma rede de VDC da organização. O VMware Cloud Director identifica a rede a ser usada para se estender pela VPN L2. O VMware Cloud Director, com a ajuda do NSX Network Virtualization, cria um tipo de interface de tronco para essa rede. O número máximo de redes permitidas é 200.

- 6 Clique em **Salvar**.

## Visualizar os endereços IP usados para uma rede de centros de dados virtuais da organização

Você pode visualizar uma lista dos endereços IP de um pool de IPs de rede de centros de dados virtuais da organização que estão sendo usados no momento.

### Pré-requisitos

- Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se sua rede de data center virtual da organização é isolada ou roteada.



## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede cujos endereços IP usados você deseja ver.
- 3 Na seção **Gerenciamento de IP**, clique em **Uso de IP** para ver quais endereços IP estão em uso no momento.

## Adicionar endereços IP a um pool de IPs de rede de data center virtual da organização

Se uma rede de data center virtual da organização estiver ficando sem endereços IP, você poderá adicionar mais endereços ao pool de IPs.

Não é possível adicionar endereços IP a redes externas de data center virtual da organização que tenham uma conexão direta.

### Pré-requisitos

- Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se sua rede de data center virtual da organização é isolada ou roteada.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Na seção **Gerenciamento de IP**, clique na guia **Pools de IPs Estáticos**.
- 4 Clique no botão **Editar** à direita.

Na janela **Editar rede**, você vê o CIDR do gateway e os intervalos de endereços IP, se houver.

- 5 Na caixa de texto **Pools de IPs estáticos**, insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.

---

**Observação** No caso de redes entre VDCs, os endereços IP não devem se sobrepor aos endereços IP atribuídos às outras redes de VDC da organização da mesma rede estendida.

---

- 6 Clique em **Salvar**.

## Resultados

O endereço IP ou o intervalo de endereços IP é adicionado ao pool de IPs de rede.

## Editar ou remover intervalos de IP usados em uma rede de data center virtual da organização

Se uma rede de data center virtual da organização contiver endereços IP de que você não precisa mais, poderá editar esses endereços ou excluí-los do pool de IP.

### Pré-requisitos

- Verifique se você é um **administrador da organização, administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se sua rede de data center virtual da organização é isolada ou roteada.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Na seção **Gerenciamento de IP**, clique em **Pools de IPs Estáticos**.
- 4 Clique no botão **Editar** à direita.
  - Para modificar um intervalo de IPs, selecione esse intervalo, faça as edições necessárias e clique em **Modificar**.
  - Para remover um intervalo de IPs, selecione-o e clique em **Remover**.
- 5 Clique em **Salvar**.

## Editar as configurações de DNS de uma rede de data center virtual da organização

Você pode editar as configurações de DNS de uma rede de data center virtual da organização.

### Pré-requisitos

- Verifique se você é um **administrador da organização, administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se sua rede de data center virtual da organização é isolada ou roteada.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Na seção **Gerenciamento de IP**, clique **DNS**.
- 4 Clique no botão **Editar** à direita.
- 5 Edite o DNS primário, o DNS secundário e as informações de sufixo DNS, conforme necessário.
- 6 Clique em **Salvar**.

## Definir as configurações de DHCP para uma rede de data center virtual de organização isolada

Você pode editar as configurações de DHCP de uma rede isolada de VDC da organização com o suporte do NSX Data Center for vSphere. O serviço DHCP de uma rede de VDC de organização

fornece endereços IP do seu pool de endereços a NICs de VM configuradas para solicitar um endereço do DHCP. O serviço fornece o endereço quando a máquina virtual é ligada.

A partir da versão 10.2, o VMware Cloud Director oferece suporte a configurações de DHCP para IPv4 e IPv6. É possível definir configurações de IPv6 usando a API do VMware Cloud Director.

#### Pré-requisitos

- Verifique se você é um **administrador da organização, administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se a sua rede é uma rede de data center virtual de organização isolada.
- Verifique se a sua rede tem suporte do NSX Data Center for vSphere.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Na seção **Gerenciamento de IP**, clique em **DHCP**.
- 4 Para habilitar o DHCP, clique em **Editar** à direita de **Serviço de Pools DHCP**.
- 5 Ative o serviço de **Serviço de Pools DHCP** e clique em **Salvar**.

Os endereços solicitados pelos clientes DHCP são extraídos de um pool DHCP.

- 6 Crie um pool de DHCP para a rede.
  - a Clique em **Novo**.
  - b Insira um intervalo de endereços IP para o pool.  
O intervalo de endereços IP que você especificar não pode se sobrepor ao pool de endereços IP estáticos do data center virtual da organização.
  - c Especifique o tempo de lease padrão para os endereços DHCP em segundos.  
O valor padrão é 3.600 segundos.
  - d Especifique o tempo máximo de lease para os endereços DHCP em segundos.  
Esse é o período de tempo máximo que os endereços IP atribuídos por DHCP são concedidos às máquinas virtuais. O valor padrão é 7.200 segundos.
- 7 Clique em **Salvar**.

## Adicionar um pool DHCP a uma rede roteada de centro de dados virtual da organização com o suporte do NSX-T Data Center

Você pode adicionar pools DHCP a uma rede roteada de VDC da organização com o suporte do NSX-T Data Center.

---

**Observação** A exclusão ou atualização de pools DHCP não é compatível em redes de VDC da organização com o suporte do NSX-T Data Center.

---

### Pré-requisitos

- Essas operações requerem as funções predefinidas de **administrador de organização** ou de **administrador de sistema** ou uma função que inclua um conjunto equivalente de direitos.
- Verifique se a sua rede é uma rede roteada de centro de dados virtual da organização.
- Verifique se a sua rede tem suporte do NSX-T Data Center.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Na seção **Gerenciamento de IP**, clique em DHCP.
- 4 Para adicionar um pool DHCP, clique em **Novo**.
- 5 Insira um intervalo de endereços IPv4 para o pool.
- 6 Clique em **Salvar**.

## Editar ou excluir um pool DHCP existente para uma rede isolada de centro de dados virtual da organização com o suporte do NSX Data Center for vSphere

Se você não precisa mais de um pool DHCP na sua rede isolada de centro de dados virtual da organização, pode editá-lo ou excluir ou editar o pool com o suporte do NSX Data Center for vSphere.

### Pré-requisitos

- Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se a sua rede é uma rede de data center virtual de organização isolada.
- Verifique se a rede de centro de dados virtual da organização tem o suporte do NSX Data Center for vSphere.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no nome da rede que você deseja editar.
- 3 Clique na seção **Gerenciamento de IP**, depois clique em **DHCP**.

#### 4 Edite ou exclua um pool DHCP existente.

Opção	Ação
Edite um pool DHCP.	<ol style="list-style-type: none"> <li>1 Selecione o pool DHCP que você deseja editar.</li> <li>2 Clique no botão <b>Editar</b>.</li> <li>3 Atualize o intervalo de endereços IP do pool.</li> <li>4 Edite o tempo de lease padrão para os endereços DHCP, em segundos.</li> <li>5 Edite o tempo máximo de lease para os endereços DHCP, em segundos.</li> <li>6 Clique em <b>Salvar</b>.</li> </ol>
Exclua um pool DHCP.	<ol style="list-style-type: none"> <li>1 Selecione o pool DHCP que você deseja excluir.</li> <li>2 Clique no botão <b>Excluir</b>.</li> </ol>

## Redefinir uma rede de data center virtual de organização

Se os serviços de rede, como configurações de DHCP ou configurações de firewall associadas a uma rede de data center virtual de organização, não estiverem funcionando conforme o esperado, você poderá redefinir a rede.

Ao redefinir a rede de data center virtual de organização, você força a reimplantação do gateway de serviço DHCP de rede. Essa operação resulta em uma interrupção temporária dos serviços DHCP, e nenhum serviço de rede está disponível enquanto a rede está sendo redefinida.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- A rede não está conectada a nenhuma máquina virtual, vApps ou outras redes.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Selecione uma rede de VDC de organização.
- 3 Clique em **Redefinir** e confirme a operação de redefinição.

## Excluir uma rede de data center virtual de organização

Se você não precisar mais de uma rede de data center virtual de organização, pode excluir essa rede.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- A rede não está conectada a máquinas virtuais, vApps ou outras redes.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.

- 2 Clique no botão de seleção ao lado do nome da rede de destino e clique em **Excluir**.
- 3 Para confirmar, clique em **OK**.

## Gerenciamento de rede de grupo de centros de dados com o NSX-T Data Center

A partir da versão 10.2, o VMware Cloud Director é compatível com a rede de grupo de centros de dados com suporte do NSX-T Data Center.

Para criar uma rede entre VDCs de organização, primeiro agrupe esses VDCs e, em seguida, crie uma rede de grupo compartilhada com eles.

As redes de grupo de centros de dados com suporte do NSX-T Data Center fornecem compartilhamento de rede de nível 2, configuração de ponto de saída ativo único e regras de firewall distribuído (DFW) que são aplicadas em um grupo de centros de dados.

### Grupo de data centers

Um grupo de centros de dados atua como um roteador entre VDCs que fornece administração de rede centralizada, configuração de ponto de saída e tráfego leste-oeste entre todas as redes dentro do grupo. Um grupo de centros de dados pode conter entre um e 16 VDCs configurados para compartilhar um ponto de saída ativo.

### Zona de disponibilidade

Uma zona de disponibilidade representa os clusters de processamento, ou os domínios de falha de processamento, que estão disponíveis para a rede. Por padrão, a zona de disponibilidade é o VDC de provedor.

---

**Importante** O **administrador do sistema** deve configurar as zonas de disponibilidade para rede de grupo com o NSX-T Data Center definindo um **Escopo do Provedor de Processamento** para a instância do vCenter Server e, opcionalmente, para os VDCs do provedor apoiados pela instância do vCenter Server. Por padrão, o escopo do provedor de processamento de um VDC de provedor é copiado da instância do vCenter Server que está apoiando esse VDC. Um **administrador do sistema** pode diferenciar o escopo do provedor de processamento para os VDCs de provedor diferentes que têm o apoio de uma única instância do vCenter Server. Por exemplo, você pode ter uma instância do vCenter Server com **Alemanha** como escopo e um VDC de provedor com **Munique** como escopo.

---

Seu **administrador do sistema** também pode reconfigurar a zona de disponibilidade para ser o escopo do provedor de rede, que normalmente representa a instância subjacente do vCenter Server com o NSX-T Manager associado.

### Ponto de ingresso

Um edge gateway existente do NSX-T Data Center que você configura para conectar um grupo de centros de dados a uma rede externa.

### Rede de grupo de centros de dados

Uma rede de camada 2 que é compartilhada em todos os VDCs em um grupo de centros de dados.

## Gerenciamento de grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Depois de criar um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center, você poderá adicionar centros de dados a esse grupo, removê-los e editar as configurações do grupo.

Um grupo de centros de dados pode incluir até 16 centros de dados virtuais.

Os VDCs removidos do grupo de centros de dados não devem ter cargas de trabalho anexadas a qualquer uma das redes que participam do grupo de centros de dados.

### Criar um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Você pode agrupar entre um e 16 VDCs em um grupo de centros de dados com o tipo de provedor de rede do NSX-T Data Center.

#### Pré-requisitos

Verifique se você é um **administrador da organização**, **administrador do sistema** ou se você recebeu uma função que inclui um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.
- 2 Clique em **Novo**.
- 3 Na página **Iniciando o VDC**, selecione um VDC com suporte pelo NSX-T Data Center para iniciar o grupo.
- 4 Insira um nome e, opcionalmente, uma descrição para o novo grupo de data centers.
- 5 Na página **Participando de VDCs**, selecione centros de dados adicionais para o novo grupo de centros de dados e clique em **Avançar**.
- 6 Revise os detalhes do grupo de centros de dados e clique em **Concluir**.

#### Resultados

O grupo recém-criado aparece na lista de grupos de centros de dados.

### Próximo passo

Crie uma rede que abranja o grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.

## Exibir e editar as configurações gerais de um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Você pode exibir e editar os grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center na sua organização.

### Pré-requisitos

Verifique se você é um **administrador da organização** ou se tem uma função com um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.  
A lista de grupos de centros de dados é exibida.
- 2 Clique no grupo de centros de dados desejado.
- 3 No painel **Configurações Gerais**, clique em **Editar**.
- 4 Edite o nome e, opcionalmente, a descrição do grupo de centros de dados e clique em **Salvar** para confirmar.

## Gerenciar VDCs participantes em um grupo de centros de dados

Você pode selecionar quais VDCs devem fazer parte de um grupo de VDCs e se comunicar entre si.

### Pré-requisitos

Verifique se você é um **administrador da organização** ou se tem uma função com um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.  
A lista de grupos de centros de dados é exibida.
- 2 Clique no grupo de centros de dados desejado.
- 3 Clique em **VDCs Participantes** e depois em **Gerenciar**.
- 4 Selecione os VDCs que você deseja incluir no grupo e clique em **Salvar** para confirmar.



## Sincronizar um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Para verificar se todos os VDCs que participam de um grupo de centros de dados ainda existem e estão configurados corretamente, você pode sincronizar esse grupo.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Clique em **Sincronizar** e confirme.

## Usando o firewall distribuído em um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

A partir da versão 10.2, o VMware Cloud Director oferece suporte ao serviço de firewall distribuído para grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center.

Ao ativar um firewall distribuído para um grupo de centros de dados com o tipo de provedor de rede do NSX-T Data Center, você cria uma única política de segurança padrão que é aplicada a esse grupo.

Como **administrador da organização**, você pode criar e modificar regras de firewall distribuído adicionais que estão associadas à política de segurança padrão do grupo de centros de dados.

O serviço de firewall distribuído não está ativado por padrão. Depois de ativar o firewall distribuído, você poderá criar conjuntos de IPs e grupos de segurança para facilitar a criação de regras de firewall distribuído.

---

**Observação** As regras de firewall distribuído que você criar serão aplicadas somente às cargas de trabalho que estiverem conectadas às redes de grupos de centros de dados.

---

## Ativar o firewall distribuído para um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Ao usar o firewall distribuído, você pode aplicar um conjunto de regras de firewall de nível 3 a um único grupo de centros de dados.

O firewall distribuído não está ativado por padrão. Ao ativá-lo, você cria uma política de segurança padrão única.

### Pré-requisitos

Verifique se você é um **administrador do sistema**.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.  
A lista de grupos de centros de dados é exibida.
- 2 Clique no grupo de centros de dados desejado.
- 3 Na seção **Firewall Distribuído**, clique em **Ativar** e confirme que você deseja ativar o firewall distribuído.

## Próximo passo

Crie regras de firewall distribuído.

## Adicionar um conjunto de IPs a um grupo de centros de dados

Para criar regras de firewall distribuído e adicioná-las a um grupo de centros de dados, você deve primeiro criar conjuntos de IPs. Conjuntos de IPs são grupos de endereços IP e redes aos quais as regras de firewall distribuído se aplicam. Combinar vários objetos em conjuntos de IPs ajuda a reduzir o número total de regras de firewall distribuído a serem criadas.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.  
A lista de grupos de centros de dados é exibida.
- 2 Clique no grupo de centros de dados desejado.
- 3 Em Segurança, clique em **Conjuntos de IPs**.
- 4 Clique em **Novo**.
- 5 Insira um nome significativo e, opcionalmente, uma descrição para o novo conjunto de IPs.
- 6 Insira um endereço IPv4, um endereço IPv6 ou um intervalo de endereços em um formato CIDR e clique em **Adicionar**.
- 7 Para modificar um endereço IP ou um intervalo existente, clique em **Modificar** e edite o valor.
- 8 Para confirmar, clique em **Salvar**.

## Criar um grupo de segurança em um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Antes de criar regras de firewall distribuído para um grupo de centros de dados, você pode agrupar redes de grupos de centros de dados em grupos de segurança aos quais essas regras se aplicam.

Grupos de segurança são grupos de redes de grupos de centros de dados aos quais se aplicam regras de firewall distribuído. O agrupamento de redes ajuda a reduzir o número total de regras de firewall distribuído a serem criadas.

## Pré-requisitos

Verifique se você tem pelo menos uma rede de grupos de centros de dados com o suporte do NSX-T Data Center.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Em **Segurança**, clique em **Grupos de Segurança** e clique em **Novo**.
- 4 Insira um nome e, opcionalmente, uma descrição para o grupo de segurança e clique em **Salvar**.

O novo grupo de segurança é exibido na lista.

- 5 Selecione o grupo de segurança recém-criado e clique em **Gerenciar Membros**.
- 6 Selecione redes de grupos de centros de dados que você deseja adicionar ao grupo de segurança.
- 7 Clique em **Salvar**.

## Próximo passo

[Adicionar uma regra de firewall distribuído a um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center](#)

## Adicionar um perfil de portas de aplicativo a um grupo de centros de dados

Para criar regras de firewall distribuído, você pode usar perfis de portas de aplicativo pré-configurados e perfis de portas de aplicativo personalizados.

Perfis de portas de aplicativo incluem uma combinação de um protocolo e uma porta, ou um grupo de portas, que é usada para serviços de firewall. Além dos perfis de portas padrão pré-configurados, você pode criar perfis de portas de aplicativo personalizados.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Em **Segurança**, clique em **Perfis de Portas de Aplicativo**.
- 4 No painel **Aplicativos Personalizados**, clique em **Novo**.
- 5 Insira um nome e, opcionalmente, uma descrição para o perfil de porta de aplicativo.

- 6 No menu suspenso **Protocolo**, selecione o protocolo.
- 7 Insira uma porta ou um intervalo de portas, separados por vírgula, e clique em **Salvar**.
- 8 Para configurar perfis de porta adicionais, repita as etapas.

#### Próximo passo

Use os perfis de portas de aplicativo para criar regras de firewall distribuído.

## Adicionar uma regra de firewall distribuído a um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center

As regras de firewall distribuído que você criar serão aplicadas somente a cargas de trabalho que estiverem anexadas às redes de grupos de centros de dados.

#### Pré-requisitos

Verifique se o serviço de firewall distribuído para o grupo de centros de dados está ativado.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Clique na guia **Firewall Distribuído** à esquerda.
- 4 Clique em **Editar Regras**.
- 5 Para adicionar uma regra de firewall, clique em **Novo no Topo**.
- 6 Configure a regra.

Opção	Descrição
Nome	Digite um nome para a regra.
Estado	Para ativar a regra na criação, alterne para a opção <b>Estado</b> .
Aplicativos	(Opcional) Para selecionar um perfil de porta específico ao qual a regra se aplica, ative a opção <b>Aplicativos</b> e clique em <b>Salvar</b> .
Contexto	(Opcional) Selecione um perfil de contexto do NSX-T Data Center para a regra.
Origem	<p>Selecione o tráfego de origem e clique em <b>Manter</b>.</p> <ul style="list-style-type: none"> <li>■ Para permitir ou recusar o tráfego de qualquer endereço de origem, ative a opção <b>Qualquer Origem</b>.</li> <li>■ Para permitir ou negar o tráfego de conjuntos de IP ou grupos de segurança específicos, selecione os conjuntos de IPs e grupos de segurança na lista.</li> </ul>

Opção	Descrição
<b>Destino</b>	<p>Selecione o tráfego de destino e clique em <b>Manter</b>.</p> <ul style="list-style-type: none"> <li>■ Para permitir ou negar o tráfego para qualquer endereço de destino, ative a opção <b>Qualquer Destino</b>.</li> <li>■ Para permitir ou negar o tráfego para conjuntos de IP ou grupos de segurança específicos, selecione os conjuntos de IPs e grupos de segurança na lista.</li> </ul>
<b>Ação</b>	<p>No menu suspenso <b>Ação</b>, selecione se deseja permitir ou negar o tráfego de ou para origens específicas.</p> <ul style="list-style-type: none"> <li>■ Para permitir o tráfego de ou para as origens, os destinos e os serviços especificados, selecione <b>Aceitar</b>.</li> <li>■ Para bloquear o tráfego de ou para as origens, os destinos e os serviços especificados, selecione <b>Negar</b>.</li> </ul>
<b>Protocolo IP</b>	Selecione se deseja aplicar a regra ao tráfego IPv4 ou IPv6.
<b>Ativar log.</b>	Para que a conversão de endereços realizada por essa regra seja registrada, ative a opção <b>Ativar o log</b> .

7 Clique em **Salvar**.

8 Para configurar regras adicionais, repita as etapas.

#### Resultados

Depois que você criar as regras de firewall, elas aparecerão na lista Regras de Firewall Distribuído. É possível mover as regras para cima ou para baixo, editá-las ou excluí-las conforme necessário.

### Desativar a política de firewall distribuído padrão

Se você quiser desativar o serviço de firewall distribuído, deverá primeiro desativar a política de firewall distribuído padrão.

Ao desativar a política padrão, você pode editar as regras de firewall distribuído, mas elas deixarão de ser aplicadas.

#### Procedimentos

1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

2 Clique no grupo de centros de dados desejado.

3 Clique na guia **Firewall Distribuído** à esquerda.

4 No cartão **Política Padrão** acima da lista de regras de firewall distribuído, clique em **Desativar** e confirme a ação.

#### Resultados

A política padrão está desativada. O restante das regras de firewall distribuído podem ser editadas, mas elas não são aplicadas.

## Desativar o serviço de firewall distribuído

Se você não quiser usar o serviço de firewall distribuído, poderá desativá-lo.

Quando você desativa o serviço de firewall distribuído para um grupo de centros de dados, a configuração de regras de segurança para esse grupo é excluída permanentemente e não pode ser recuperada.

### Pré-requisitos

[Desativar a política de firewall distribuído padrão](#)

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.  
A lista de grupos de centros de dados é exibida.
- 2 Clique no grupo de centros de dados desejado.
- 3 Clique em **Geral**.
- 4 No painel **Firewall Distribuído** à direita, clique em **Desativar** e confirme a ação.

### Resultados

O serviço de firewall distribuído é desativado, e a configuração de regras de segurança é excluída.

## Gerenciamento de redes de grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Depois de criar e configurar um grupo de centros de dados, você pode criar e gerenciar redes de grupos de centros de dados abrangendo os VDCs participantes.

Você pode usar redes de grupos de centros de dados virtuais da organização roteadas, isoladas e importadas com suporte do NSX-T Data Center.

Uma rede de grupo de centros de dados só pode ser abrangida em um único grupo de centros de dados.

Você pode aumentar o escopo de uma rede existente de um VDC de organização para um grupo de centros de dados.

Você pode adicionar todos os tipos de redes a um grupo de centros de dados.

---

**Importante** Os endereços IP nas redes que participam de um grupo de centros de dados não devem se sobrepor, mesmo se as redes estiverem isoladas.

---

Tabela 5-2. Tipos de redes de grupos de centros de dados

Tipo de rede de grupo de centros de dados	Descrição
Isolada	Uma rede de grupo de centro de dados isolada é acessível apenas pelos VDCs no mesmo grupo de centros de dados. Apenas as máquinas virtuais no grupo de centros de dados podem se conectar e ver o tráfego na rede de grupo de centros de dados.
Roteado	Uma rede de grupo de centros de dados roteada fornece acesso controlado a uma rede externa por meio de um edge gateway do NSX-T Data Center que faz parte do grupo de centros de dados.
Importada	Uma rede de grupo de centros de dados importada usa um comutador lógico do NSX-T Data Center existente. Apenas um <b>administrador do sistema</b> pode importar uma rede.

## Criar uma rede de grupos de centros de dados isolada com o suporte de um NSX-T Data Center

É possível adicionar uma rede de grupos de centros de dados isolada, que é acessível apenas para VMs nesse grupo. As VMs fora dessa rede não têm conectividade com ela, independentemente de estarem conectadas a outras redes no mesmo grupo de centros de dados.

### Pré-requisitos

- Verifique se você é um **administrador da organização**.
- Verifique se você criou um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Grupo de Centros de Dados** e escolha um grupo com um provedor de rede NSX-T Data Center no qual deseja criar a rede.
- 4 Na página **Tipo de Rede**, selecione **Isolada** e clique em **Avançar**.
- 5 Insira um nome relevante para a rede.
- 6 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 7 Insira uma descrição da rede de VDC da organização.
- 8 Clique em **Avançar**.

- 9 (Opcional) Para reservar um ou mais endereços IP para atribuição a máquinas virtuais que exigem endereços IP estáticos, configure os **Pools de IPs Estáticos** para a rede.
  - a Insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.  
Para adicionar vários endereços IP ou intervalos estáticos, repita essa etapa.
  - b (Opcional) Para modificar ou remover endereços IP e intervalos, clique em **Modificar** ou **Remover**.
- 10 (Opcional) Defina as configurações de DNS.

Opção	Ação
DNS Primário	Insira o endereço IP do servidor DNS primário.
DNS Secundário	Insira o endereço IP do seu servidor DNS secundário.
Sufixo DNS	Insira seu sufixo DNS. O sufixo DNS é o nome DNS sem incluir o nome do host.

- 11 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Criar uma rede de grupos de centros de dados roteada com o suporte do NSX-T Data Center

Para controlar o acesso a uma rede externa, você pode adicionar uma rede de grupos de centros de dados roteada.

### Pré-requisitos

- Verifique se você é um **administrador da organização** ou se tem uma função com um conjunto equivalente de direitos.
- Verifique se você criou um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.
- Verifique se você definiu o escopo de um edge gateway do NSX-T Data Center existente para o grupo de centros de dados no qual deseja criar uma rede roteada.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Grupo de Centros de Dados** e escolha um grupo com um provedor de rede NSX-T Data Center no qual deseja criar a rede.
- 4 Na página **Tipo de Rede**, selecione **Roteada** e clique em **Avançar**.

Se houver apenas um edge gateway disponível com escopo definido para o grupo de centros de dados, ele será automaticamente atribuído à rede.

- 5 Se houver mais de um NSX-T Data Center disponível para o grupo de centros de dados, selecione um edge gateway na lista e clique em **Avançar**.



- 6 Insira um nome relevante para a rede.
- 7 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 8 Insira uma descrição da rede de VDC da organização.
- 9 Clique em **Avançar**.
- 10 (Opcional) Para reservar um ou mais endereços IP para atribuição a máquinas virtuais que exigem endereços IP estáticos, configure os **Pools de IPs Estáticos** para a rede.
  - a Insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.  
Para adicionar vários endereços IP ou intervalos estáticos, repita essa etapa.
  - b (Opcional) Para modificar ou remover endereços IP e intervalos, clique em **Modificar** ou **Remover**.
- 11 (Opcional) Defina as configurações de DNS.

Opção	Ação
DNS Primário	Insira o endereço IP do servidor DNS primário.
DNS Secundário	Insira o endereço IP do seu servidor DNS secundário.
Sufixo DNS	Insira seu sufixo DNS. O sufixo DNS é o nome DNS sem incluir o nome do host.

- 12 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Criar uma rede de grupos de centros de dados com um comutador lógico NSX-T importado

**Administradores de sistema** podem criar uma rede de VDCs de organização importando um segmento de uma instância associada do NSX-T Manager.

### Pré-requisitos

- Verifique se você é um **administrador do sistema**.
- Verifique se você criou um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.
- Verifique se o centro de dados virtual do provedor que oferece suporte ao grupo de centros de dados virtuais de destino está associado a uma instância do NSX-T Manager.
- Verifique se você criou pelo menos um comutador lógico NSX-T que não esteja em uso por outras redes. Para obter informações sobre como criar e configurar os comutadores lógicos do NSX-T, consulte *Guia de administração do NSX-T Data Center*.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.

- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Grupo de Centros de Dados** e escolha um grupo com um provedor de rede NSX-T Data Center no qual deseja criar a rede.
- 4 Na página **Tipo de Rede**, selecione **Importada** e clique em **Avançar**.
- 5 Na lista de comutadores lógicos NSX-T disponíveis, selecione o comutador de destino e clique em **Avançar**.
- 6 Insira um nome relevante para a rede.
- 7 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 8 Insira uma descrição da rede de VDC da organização.
- 9 Clique em **Avançar**.
- 10 (Opcional) Para reservar um ou mais endereços IP para atribuição a máquinas virtuais que exigem endereços IP estáticos, configure os **Pools de IPs Estáticos** para a rede.
  - a Insira o endereço IP ou o intervalo de endereços IP e clique em **Adicionar**.  
Para adicionar vários endereços IP ou intervalos estáticos, repita essa etapa.
  - b (Opcional) Para modificar ou remover endereços IP e intervalos, clique em **Modificar** ou **Remover**.
- 11 (Opcional) Defina as configurações de DNS.

Opção	Ação
DNS Primário	Insira o endereço IP do servidor DNS primário.
DNS Secundário	Insira o endereço IP do seu servidor DNS secundário.
Sufixo DNS	Insira seu sufixo DNS. O sufixo DNS é o nome DNS sem incluir o nome do host.

- 12 Na página **Pronto para ser Concluído**, reveja suas configurações e clique em **Concluir**.

## Aumentar o escopo de uma rede de VDCs de organização com o suporte do NSX-T Data Center

Depois de aumentar o escopo de uma rede de VDC de organização para uma rede de grupos de centros de dados, você pode conectar cargas de trabalho de todos os centros de dados que participam desse grupo.

### Pré-requisitos

- Verifique se você é um **administrador da organização** ou se tem uma função com um conjunto equivalente de direitos.

- Verifique se você criou um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.
- Verifique se você criou uma rede de VDCs de organização com o suporte do NSX-T Data Center.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no botão de opção ao lado da rede de VDCs de organização cujo escopo você deseja aumentar e clique em **Aumentar Escopo**.
- 3 Selecione um grupo de centros de dados na lista de grupos de centros de dados e clique em **OK** para confirmar.

#### Resultados

O escopo da rede é aumentado para uma rede de grupos de centros de dados. Na lista de redes, ela está listada como com escopo para o grupo de centros de dados que você selecionou.

### Diminuir o escopo de uma rede de grupos de centros de dados com o suporte do NSX-T Data Center

É possível diminuir o escopo de uma rede de grupos de centros de dados com o suporte do NSX-T Data Center para uma rede de VDCs de organização.

Se você diminuir o escopo de uma rede de grupos de centros de dados para uma única rede de VDCs de organização, fornecerá conectividade de rede para cargas de trabalho que pertencem apenas ao VDC de organização.

#### Pré-requisitos

- Verifique se você é um **administrador da organização** ou se tem uma função com um conjunto equivalente de direitos.
- Verifique se você criou uma rede de VDCs e definiu seu escopo para um grupo de centros de dados com um tipo de provedor de rede do NSX-T Data Center.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique no botão de opção ao lado da rede de grupos de centros de dados cujo escopo você deseja diminuir e clique em **Diminuir Escopo**.
- 3 Na lista de VDCs que são membros da rede de grupos, selecione o VDC para o qual você deseja definir o escopo da rede e clique em **OK**.

#### Resultados

O escopo da rede é reduzido para uma única rede de VDCs de organização.

## Gerenciamento de pontos de saída para grupos de centros de dados com um tipo de provedor de rede do NSX-T Data Center

Para rotear o tráfego para dentro e para fora de uma rede de grupos de centros de dados para uma rede externa, você pode configurar um edge gateway do NSX-T Data Center para ser o ponto de saída para um grupo de centros de dados.

Ao configurar um edge gateway para ser o ponto de saída de um grupo de centros de dados, você aumenta o seu escopo para esse grupo de centros de dados. O edge gateway torna-se compartilhado em todos os centros de dados que participam do grupo. Todas as redes roteadas que estão conectadas ao edge gateway são anexadas ao grupo de centros de dados e abrangidas por ele.

Todos os serviços do edge gateway permanecem como parte das funções do edge gateway. Para obter mais informações, consulte [Gerenciando Edge Gateways do NSX-T Data Center](#).

Se um VDC for membro do grupo de centros de dados e se nenhuma carga de trabalho estiver conectada a qualquer uma das redes roteadas que não façam parte do escopo de destino, você poderá remover um edge gateway de um grupo de centros de dados e definir o escopo dele para um único VDC.

É possível adicionar um edge gateway a uma rede de grupos de centros de dados isolada e convertê-la em uma rede de centros de dados roteada. Você também pode remover a conexão com um edge gateway de uma rede de grupos de centros de dados, convertendo a rede roteada em uma rede de grupos de centro de dados isolada.

### Adicionar um Edge Gateway do NSX-T Data Center a um grupo de centros de dados

Para configurar um edge gateway do NSX-T Data Center para ser o ponto de saída de um grupo de centros de dados, aumente o escopo do edge gateway. O edge gateway se tornará compartilhado em todos os centros de dados que participam desse grupo.

Quando você delimita um edge gateway em um grupo de centros de dados, todas as redes roteadas que estão conectadas ao edge gateway são anexadas ao grupo de centros de dados e abrangidas por ele.

Todas as novas redes roteadas que você anexar ao edge gateway pertencem ao grupo de centros de dados.

Uma rede roteada conectada a um edge gateway que tem o escopo para um VDC poderá participar de um grupo de centros de dados somente se o escopo do edge for aumentado para esse grupo de centros de dados.

#### Pré-requisitos

Verifique se você associou um edge gateway existente do NSX-T Data Center a um dos VDCs que participam do grupo de centros de dados.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Clique em **Edge Gateway** e, em seguida, clique em **Adicionar Edge**.
- 4 Selecione um dos edge gateways disponíveis e clique em **Salvar**.

## Resultados

O escopo do edge gateway é aumentado para o grupo de centros de dados. A alteração do escopo não afeta quaisquer redes ou serviços subjacentes existentes.

## Diminuir o escopo de um Edge Gateway do NSX-T Data Center para um VDC

Você pode diminuir o escopo de um edge gateway do NSX-T Data Center para um VDC específico removendo o edge gateway do grupo de centros de dados ao qual ele tem o escopo.

Quando você diminui o escopo de um edge gateway para um VDC específico, todos os objetos do grupo de segurança que estão em uso pelo edge gateway permanecem com ele. Os grupos de segurança que são usados exclusivamente pelo firewall distribuído permanecem como parte do grupo de VDCs.

## Pré-requisitos

- Verifique se o VDC para o qual você deseja diminuir o escopo do edge gateway é um membro do grupo de centros de dados.
- Verifique se não há cargas de trabalho conectadas a nenhuma rede roteada que não faça parte do escopo do edge gateway de destino.
- Verifique se não há grupos de segurança ou conjuntos de IPs no grupo do centro de dados em uso pelo edge gateway e pelo firewall distribuído.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.
- 3 Clique em **Edge Gateway** e em **Remover Edge**.
- 4 Selecione um VDC para o qual diminuir o escopo do edge gateway e clique em **Salvar**.

## Gerenciamento de rede de grupo de centros de dados com o NSX Data Center for vSphere

Para criar uma rede entre centros de dados virtuais de organização, primeiro agrupe os centros de dados virtuais e, em seguida, crie uma rede VDC abrangida no grupo de centros de dados.

O VMware Cloud Director oferece suporte à rede de grupo de centros de dados para centros de dados virtuais da organização com suporte do NSX Data Center for vSphere com um ponto de saída ativo e outro em espera para um único domínio de falha de rede.

Um grupo de centros de dados com suporte do NSX Data Center for vSphere pode ter uma configuração comum de ponto de saída, uma configuração de ponto de saída para cada domínio de falha de rede ou uma configuração de grupo local.

### Grupo de data centers

Um grupo de centros de dados atua como um roteador de grupo de centros de dados virtuais que fornece administração de rede centralizada, configuração para vários pontos de saída em vários centros de dados virtuais e tráfego leste-oeste entre todas as redes do grupo. Um grupo de centros de dados pode conter entre um e 16 centros de dados virtuais configurados para compartilhar vários pontos de saída. Um grupo de data centers pode ter uma das seguintes configurações de pontos de saída:

**Tabela 5-3. Tipo de configuração de pontos de saída para grupos de centros de dados com suporte do NSX Data Center for vSphere**

Tipo de configuração de pontos de saída	Descrição
Configuração de pontos de saída comuns	<p>Você pode configurar o grupo de centros de dados com um ponto de saída ativo e um ponto de saída de espera. Os dois pontos de saída são comuns a todos os data centers que participam em todos os domínios de falha de rede no grupo de data centers.</p> <p>Um grupo de centros de dados com essa configuração pode incluir centros de dados de até quatro domínios de falha de rede.</p>
Configuração de pontos de saída por domínio de falha	<p>Você pode configurar o grupo de centros de dados com um ponto de saída ativo e um ponto de saída de espera para cada domínio de falha de rede no grupo de centros de dados.</p> <p>Um grupo de centros de dados com essa configuração pode incluir centros de dados de até quatro domínios de falha de rede.</p>
Configuração do grupo local	<p>Os centros de dados virtuais da organização em um grupo de centros de dados local têm o suporte de uma única instância do vCenter Server. Você pode configurar o grupo de centros de dados locais com um ponto de saída ativo e um ponto de saída de espera para um único domínio de falha de rede.</p>

Uma organização pode ter vários grupos de data centers. Um data center virtual da organização pode participar de vários grupos de data centers.

Os centros de dados virtuais da organização participante podem pertencer a diferentes sites do VMware Cloud Director. Consulte [Configurar e gerenciar implantações multissite](#).

### Domínio de Falha de Rede

O escopo do provedor de rede, normalmente representando a instância do vCenter Server subjacente com o NSX Manager associado.

### Ponto de ingresso

Um edge gateway que conecta um domínio de falha de rede ou um grupo de data centers à Internet. O edge gateway deve pertencer a um data center virtual do grupo de data centers. As rotas de BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do domínio de falha de rede ou do grupo de data centers virtuais. As rotas existentes no edge gateway não são afetadas.

### Rede estendida

Uma rede de camada 2 que é estendida em todos os data centers virtuais em um grupo de data centers. Pode ser somente IPv4.

## Gerenciando grupos de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Depois de criar um grupo de centros de dados com suporte do NSX Data Center for vSphere, você poderá editar a topologia de rede de um grupo de centros de dados. É possível adicionar e remover data centers virtuais do grupo. É possível trocar, substituir e remover pontos de saída. É possível corrigir falhas de configuração realizando diferentes tarefas de sincronização.

Não é possível converter uma configuração de saída comum em uma configuração de saída de domínio de falha, ou vice-versa.

### Criar e configurar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída comum

Você pode criar e configurar um grupo de centros de dados virtuais com suporte do NSX Data Center for vSphere com uma configuração de saída comum na qual você define um par de edge gateways que atuam como ponto de saída ativo e em espera para todos os centros de dados virtuais participantes.

#### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.

- O **administrador do sistema** deve ativar os centros de dados virtuais de destino para a rede entre centros de dados virtuais.

## Procedimentos

- 1 [Criar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída comum](#)

Você pode agrupar entre um e 16 centros de dados virtuais em um grupo de centros de dados com uma configuração de saída comum.

- 2 [Adicionar um ponto de saída ativo a um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere](#)

Para conectar seu grupo de data centers à Internet, você deve adicionar um ponto de saída ativo à sua topologia de rede.

- 3 [Adicionar um ponto de saída de espera a um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere](#)

Em grupos de data centers virtuais com configurações comuns de saída, você pode adicionar um ponto de saída secundário, que atua como um ponto de saída de espera para cenários de tolerância a falhas.

## Criar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída comum

Você pode agrupar entre um e 16 centros de dados virtuais em um grupo de centros de dados com uma configuração de saída comum.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique em **Novo**.

- 3 Na página **Iniciando VDC**, selecione um VDC virtual para iniciar o grupo de VDCs.

- 4 Insira um nome e, opcionalmente, uma descrição para o novo grupo de data centers.

- 5 Selecione **Pontos de Saída Comuns** e clique em **Avançar**.

- 6 Na página **Participando de VDCs**, selecione centros de dados adicionais para o novo grupo de centros de dados e clique em **Avançar**.

A página **Centros de Dados** contém uma lista dos VDCs que o **administrador do sistema** ativou para a rede de centros de dados virtuais cruzados.

- 7 Revise os detalhes do grupo de centros de dados e clique em **Concluir**.



## Resultados

O grupo de centros de dados virtuais recém-criado é listado na exibição **Grupos de Centros de Dados**.

### Adicionar um ponto de saída ativo a um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Para conectar seu grupo de data centers à Internet, você deve adicionar um ponto de saída ativo à sua topologia de rede.

## Pré-requisitos

O **administrador de sistema** criou pelo menos um edge gateway em um dos data centers virtuais que estão participando no grupo de data centers.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Adicionar ponto de saída**.

A página **Adicionar Ponto de Saída Ativo**, que é aberta, fornece uma lista dos edge gateways que pertencem aos data centers virtuais participantes.

- 4 Selecione o edge gateway que deseja que atue como um ponto de saída ativo para este grupo de data centers e clique em **Adicionar**.

## Resultados

As rotas BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do grupo de data centers virtuais. As rotas existentes no edge gateway não são afetadas.

O diagrama da topologia de rede é atualizado com o ponto de saída adicionado recentemente. O tráfego dos data centers virtuais participantes para a Internet é representado por uma linha azul sólida.

### Adicionar um ponto de saída de espera a um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Em grupos de data centers virtuais com configurações comuns de saída, você pode adicionar um ponto de saída secundário, que atua como um ponto de saída de espera para cenários de tolerância a falhas.

## Pré-requisitos

Além do edge gateway que atua como um ponto de saída ativo, você deve ter pelo menos mais um edge gateway em qualquer um dos data centers virtuais que estejam participando do grupo.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Adicionar ponto de saída de espera**.

A página **Adicionar ponto de saída de espera** fornece uma lista dos edge gateways não utilizados que pertencem aos data centers virtuais participantes. O edge gateway que está em uso pelo ponto de saída ativo neste grupo de centros de dados virtuais não é exibido.

- 4 Selecione o edge gateway que você deseja que atue como um ponto de saída de espera para este grupo de data centers e clique em **Adicionar**.

## Resultados

As rotas BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do domínio de falha de rede. A configuração não afeta as rotas existentes no gateway de borda.

O diagrama da topologia de rede é atualizado com o ponto de saída adicionado recentemente. O tráfego dos data centers virtuais participantes para a Internet em cenários de tolerância a falhas é representado com uma linha azul tracejada.

## Criar e configurar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha

Você pode criar e configurar um grupo de centros de dados virtuais com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha na qual você configura um edge gateway que atua como ponto de saída ativo para cada domínio de falha de rede no grupo. Não é possível criar saídas em espera em um grupo de centros de dados com uma configuração de saída de domínio de falha.

## Pré-requisitos

Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.

## Procedimentos

- 1 [Criar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha](#)

Você pode agrupar de 1 a 16 centros de dados virtuais em um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha.

- 2 [Adicionar um ponto de saída a um domínio de falha](#)

Para conectar os centros de dados virtuais de um domínio de falha de rede em um grupo de centros de dados com suporte do NSX Data Center for vSphere à internet, você deve adicionar um ponto de saída a este domínio de falha de rede. Você pode adicionar um ponto de saída a cada domínio de falha de rede no grupo de data centers. Os pontos de saída de espera não são suportados em um grupo de data centers com uma configuração de saída de domínio de falha.

### Criar um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha

Você pode agrupar de 1 a 16 centros de dados virtuais em um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha.

## Pré-requisitos

O **administrador de sistema** ativou os data centers virtuais de destino para a rede entre data centers virtuais.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo grupo de data centers.
- 4 Selecione **Pontos de Saída por Domínio de Falha** e clique em **Próximo**.
- 5 Na página **Participando de VDCs**, selecione centros de dados adicionais para o novo grupo de centros de dados e clique em **Avançar**.

A página **Centros de Dados** contém uma lista dos VDCs que o **administrador do sistema** ativou para a rede de centros de dados virtuais cruzados.

- 6 Revise os detalhes do grupo de centros de dados e clique em **Concluir**.

## Resultados

O grupo de centros de dados virtuais recém-criado é listado na exibição **Grupos de Centros de Dados**.

### Adicionar um ponto de saída a um domínio de falha

Para conectar os centros de dados virtuais de um domínio de falha de rede em um grupo de centros de dados com suporte do NSX Data Center for vSphere à internet, você deve adicionar um ponto de saída a este domínio de falha de rede. Você pode adicionar um ponto de saída a cada domínio de falha de rede no grupo de data centers. Os pontos de saída de espera não são suportados em um grupo de data centers com uma configuração de saída de domínio de falha.

### Pré-requisitos

Além dos edge gateways que estão em uso como pontos de saída neste grupo de data centers, você deve ter pelo menos um edge gateway não utilizado em um dos data centers virtuais participantes.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 No diagrama da topologia de rede, clique no domínio de falha da rede de destino.

Os domínios de falha de rede são representados com linhas sólidas e seus nomes na parte inferior do diagrama.

O domínio de falha selecionado está marcado em azul.

- 4 Clique em **Adicionar ponto de saída**.

A página **Adicionar Ponto de Saída Ativo** é aberta e fornece uma lista dos edge gateways que pertencem aos data centers virtuais participantes.

- 5 Selecione o edge gateway que você deseja que atue como um ponto de saída para este domínio de falha e clique em **Adicionar**.

## Resultados

As rotas BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do domínio de falha de rede. As rotas existentes no edge gateway não são afetadas.

O diagrama da topologia de rede é atualizado com o ponto de saída adicionado recentemente. O tráfego dos data centers virtuais no domínio de falha de rede para a Internet é representado por uma linha azul contínua.

## Criar e configurar um grupo de centros de dados virtuais locais com o tipo de provedor de rede NSX Data Center for vSphere

Da versão 10.1 em diante, o VMware Cloud Director oferece suporte a grupos de centros de dados com suporte do NSX Data Center for vSphere com um ponto de saída ativo e outro de espera para um único domínio de falha de rede.

Os centros de dados virtuais da organização em um grupo local têm o suporte de uma única instância do vCenter Server.

Em um grupo de centros de dados locais, você pode definir um par de edge gateways — um ponto de saída ativo e um ponto de saída de espera, para oferecer suporte a cenários de alta disponibilidade e recuperação de desastres no mesmo domínio de falha de rede.

### Pré-requisitos

Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.

### Procedimentos

#### 1 Criar um grupo de centros de dados locais com o tipo de provedor de rede NSX Data Center for vSphere

Você pode agrupar de 1 a 16 centros de dados virtuais (VDCs) em um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha.

#### 2 Adicionar um ponto de saída ativo a um grupo de centros de dados locais com tipo de provedor de rede do NSX Data Center for vSphere

Para conectar os centros de dados do grupo de centros de dados locais com suporte do NSX Data Center for vSphere à Internet, você deve adicionar um ponto de saída ativo ao domínio de falha de rede.

#### 3 Adicionar um ponto de saída de espera a um grupo de centros de dados local com o tipo de provedor de rede NSX Data Center for vSphere

Em configurações de grupos de centros de dados locais, você pode adicionar um ponto de saída secundário, que atua como um ponto de saída de espera para cenários de tolerância a falhas.

### Criar um grupo de centros de dados locais com o tipo de provedor de rede NSX Data Center for vSphere

Você pode agrupar de 1 a 16 centros de dados virtuais (VDCs) em um grupo de centros de dados com suporte do NSX Data Center for vSphere com uma configuração de saída de domínio de falha.

## Pré-requisitos

O **administrador de sistema** ativou os data centers virtuais de destino para a rede entre data centers virtuais.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique em **Novo**.

- 3 Na página **Iniciando VDC**, selecione um VDC virtual para iniciar o grupo de VDCs.

- 4 Insira um nome e, opcionalmente, uma descrição para o novo grupo de data centers.

- 5 Para criar um grupo que contenha apenas centros de dados virtuais a partir de um único domínio de falha de rede, ative a opção **Criar Grupo Local**.

- 6 Clique em **Avançar**.

- 7 Na página **Participando de VDCs**, selecione centros de dados adicionais para o novo grupo de centros de dados e clique em **Avançar**.

A página **Centros de Dados** contém uma lista dos VDCs que o **administrador do sistema** ativou para a rede de centros de dados virtuais cruzados.

- 8 Revise os detalhes do grupo de centros de dados e clique em **Concluir**.

## Resultados

O grupo de centros de dados virtuais recém-criado aparece na exibição **Grupos de Centros de Dados**.

### Adicionar um ponto de saída ativo a um grupo de centros de dados locais com tipo de provedor de rede do NSX Data Center for vSphere

Para conectar os centros de dados do grupo de centros de dados locais com suporte do NSX Data Center for vSphere à Internet, você deve adicionar um ponto de saída ativo ao domínio de falha de rede.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

### 3 Clique em **Adicionar Ponto de Saída**.

- 4 Na lista de gateways de borda que pertencem aos centros de dados virtuais participantes, selecione um gateway de borda para atuar como um ponto de saída ativo para o grupo de centros de dados e clique em **Adicionar**.

#### Resultados

As rotas BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do domínio de falha de rede. A configuração não afeta as rotas existentes no gateway de borda.

O ponto de saída ativo recém-adicionado aparece no diagrama da topologia de rede. Uma linha azul contínua representa o tráfego dos centros de dados virtuais no domínio de falha de rede para a Internet.

#### Próximo passo

Para permitir a tolerância a falhas do ponto de saída, adicione um ponto de saída de espera para o grupo de centros de dados locais.

#### Adicionar um ponto de saída de espera a um grupo de centros de dados local com o tipo de provedor de rede NSX Data Center for vSphere

Em configurações de grupos de centros de dados locais, você pode adicionar um ponto de saída secundário, que atua como um ponto de saída de espera para cenários de tolerância a falhas.

#### Pré-requisitos

Além do edge gateway que atua como ponto de saída ativo, você deve ter pelo menos um edge gateway extra em qualquer um dos centros de dados virtuais que integram o grupo de centros de dados locais.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Adicionar ponto de saída de espera**.

A página **Adicionar ponto de saída de espera** fornece uma lista dos edge gateways não utilizados que pertencem aos data centers virtuais participantes. O edge gateway que está em uso pelo ponto de saída ativo neste grupo de centros de dados virtuais parece esmaecido.

- 4 Selecione o edge gateway que você deseja que atue como um ponto de saída de espera para este grupo de data centers e clique em **Adicionar**.

## Resultados

As rotas BGP são configuradas no edge gateway que representa o ponto de saída e o roteador universal do domínio de falha de rede. A configuração não afeta as rotas existentes no gateway de borda.

O ponto de saída recém-adicionado aparece no diagrama de topologia de rede. Uma linha azul tracejada representa o tráfego dos centros de dados virtuais participantes para a Internet em cenários de tolerância a falhas.

## Visualizar um grupo de centros de dados com tipo de provedor de rede do NSX Data Center for vSphere

Você pode visualizar os grupos de centros de dados da sua organização e os detalhes sobre a configuração atual deles.

### Pré-requisitos

Essa operação requer a função de **Administrador de Sistema** ou uma função com o direito de **Grupo de VDCs: Exibir Grupo de VDCs** publicado na organização.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

## Adicionar um centro de dados virtual a um grupo de centro de dados com o tipo de provedor de rede NSX Data Center for vSphere

Você pode adicionar um datacenter virtual a um grupo de datacenters, como resultado da extensão das redes existentes para o novo datacenter virtual.

### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.
- O grupo de datacenters contém menos de quatro datacenters virtuais.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.



- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Adicionar Centro de Dados**.

- 4 Na página **Centros de Dados**, selecione o centro de dados que deseja adicionar ao grupo de centros de dados e clique em **Concluir**.

A página **Centros de Dados** contém uma lista de centros de dados virtuais que estão ativados para a rede de centros de dados virtuais cruzados pelo administrador do sistema.

---

**Observação** Um grupo de datacenters deve conter até quatro datacenters virtuais.

---

## Remover um centro de dados virtual de um grupo de centro de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Você pode remover um data center virtual de um grupo de data centers, o que remove a extensão das redes existentes desse data center virtual.

### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.
- O grupo de data centers deve conter pelo menos três data centers virtuais.
- O data center virtual que você deseja remover não deve fornecer um ponto de saída para o grupo de data centers.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 No canto superior direito do cartão do data center virtual de destino, clique nos três pontos e clique em **Remover**.
- 4 Para confirmar, clique em **Remover**.

### Resultados

O data center virtual é removido do diagrama de topologia de rede do grupo de data centers.

## Sincronizar um grupo de centro de dados com o tipo de provedor de rede NSX Data Center for vSphere

Para reaplicar as configurações de rede do grupo de centros de dados e garantir que todos os centros de dados virtuais participantes estejam ativos, sincronize esse grupo.

---

**Observação** Durante o processo de sincronização do grupo de centros de dados, este fica indisponível por alguns segundos, porque o roteador universal sincroniza no NSX.

---

### Pré-requisitos

Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Sincronizar grupo de centros de dados**.
- 4 Para confirmar, clique em **OK**.

## Alternar os pontos de saída em um grupo de centros de dados com tipo de provedor de rede NSX Data Center for vSphere com uma configuração de saída comum

Depois de configurar pontos de saída ativos e em espera num grupo de centros de dados com a configuração de saída comum, você poderá alternar as funções dos pontos de saída. O ponto de saída ativo pode se tornar um ponto de saída em espera e vice-versa.

### Pré-requisitos

Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Clique em **Alternar pontos de saída**.

- 4 Para confirmar, clique em **OK**.

#### Resultados

O diagrama da topologia de rede é atualizado com as novas rotas de tráfego. Agora o tráfego para a Internet é redirecionado para o novo ponto de saída ativo.

### Substituir o edge gateway de um ponto de saída de um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Você pode substituir o edge gateway que representa um ponto de saída ativo ou em espera em um grupo de data centers.

#### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.
- O novo edge gateway não deve estar sendo usado por outros pontos de saída no grupo de data centers.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Se você estiver substituindo um ponto de saída de uma configuração de domínio de falha de rede, no diagrama de topologia de rede, selecione o domínio de falha de rede do ponto de saída de destino.

Os domínios de falha de rede são representados com linhas sólidas e nomes de domínio na parte inferior do diagrama.

O domínio de falha de rede selecionado está marcado em azul.

- 4 No canto superior direito do cartão do ponto de saída de destino, clique nos três pontos e clique em **Substituir**.

A página **Substituir Ponto de Saída** é aberta, fornecendo uma lista dos edge gateways que pertencem aos data centers virtuais participantes.

- 5 Selecione o novo edge gateway e clique em **Substituir**.

#### Resultados

As rotas BGP são removidas do antigo edge gateway e configuradas no novo edge gateway que representa o ponto de saída e o roteador universal do grupo de data centers virtuais.

O diagrama de topologia de rede é atualizado com o nome do novo edge gateway.

### Remover um ponto de saída de um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Para desconectar um domínio de falha de rede ou grupo de data center da Internet, você pode remover seu ponto de saída.

#### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.
- Se você quiser remover um ponto de saída ativo que está emparelhado com um ponto de saída em espera, você deve trocar os pontos de saída ou remover o ponto de saída de espera.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Se você estiver removendo um ponto de saída de uma configuração de domínio de falha de rede, no diagrama de topologia de rede, selecione o domínio de falha de rede do ponto de saída de destino.

Os domínios de falha de rede são representados com linhas sólidas e nomes de domínio na parte inferior do diagrama.

O domínio de falha de rede selecionado está marcado em azul.

- 4 No canto superior direito do cartão do ponto de saída de destino, clique nos três pontos e clique em **Excluir**.
- 5 Para confirmar, clique em **OK**.

## Resultados

As rotas BGP são removidas do edge gateway que representa o ponto de saída se este não estiver em uso por outros roteadores universais.

O ponto de saída é removido do diagrama de topologia de rede.

## Sincronizar rotas e pontos de saída de um grupo de centros de dados com o tipo de provedor de rede do NSX Data Center for vSphere

Sincronizando as rotas, você pode reaplicar a configuração de roteamento dinâmico a um grupo de centros de dados ou um domínio de falha de rede e seus pontos de saída associados.

Sincronizando o ponto de saída, você pode garantir que um ponto de saída esteja conectado adequadamente ao grupo de centros de dados.

### Pré-requisitos

- Essa operação requer a função **Administrador de Sistema** ou uma função com o direito **Grupo de VDCs: Configurar Grupo de VDCs** publicado na organização.
- Você configurou um ponto de saída para o domínio de falha da rede ou grupo de centros de dados de destino.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Grupos de Centros de Dados**.

A lista de grupos de centros de dados é exibida.

- 2 Clique no grupo de centros de dados desejado.

A exibição **Topologia de Rede** desse grupo de centros de dados é aberta. O diagrama da topologia de rede atual exibe os VDCs participantes com seus domínios de falha de rede, os pontos de saída, se configurados, e as rotas de tráfego.

- 3 Se você estiver sincronizando um domínio de falha de rede em um grupo de centros de dados, no diagrama de topologia de rede, selecione o domínio de falha da rede de destino.

Os domínios de falha de rede são representados com linhas sólidas e nomes de domínio na parte inferior do diagrama.

O domínio de falha de rede selecionado está marcado em azul.

- 4 Para reaplicar a configuração de roteamento dinâmico ao grupo ou ao domínio de falha de rede e seus pontos de saída associados, clique em **Sincronizar rotas** e clique em **OK**.

- 5 Para sincronizar um ponto de saída com o grupo de centros de dados dele, no canto superior direito do cartão do ponto de saída de destino, clique nos três pontos, depois em **Sincronizar** e **OK**.

## Gerenciamento de redes do grupo de centros de dados com suporte do NSX Data Center for vSphere

Depois de criar e configurar um grupo de centros de dados, você pode criar e gerenciar redes de camada 2 do grupo de VDC, abrangendo os centros de dados virtuais participantes.

### Adicionar uma rede de grupos de VDC com suporte do NSX Data Center for vSphere

Você pode criar uma rede de grupos de VDC em todos os centros de dados virtuais que integram um grupo de centros de dados.

Você pode adicionar apenas uma rede de grupo de centros de dados IPv4 com suporte do NSX Data Center for vSphere.

#### Pré-requisitos

Essa operação requer a função predefinida **Administrador da Organização** ou uma função com o direito **Rede VDC da Organização: Editar Propriedades**.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia **Redes**, clique em **Novo**.
- 3 Na página **Escopo**, selecione **Grupo de Centros de Dados**, escolha o grupo de centro de dados com suporte do NSX Data Center for vSphere no qual deseja criar a rede e clique em **Avançar**.
- 4 Insira um nome relevante para a rede.
- 5 Insira as configurações de roteamento entre domínios sem classe (CIDR) para a rede.  
Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.
- 6 Insira uma descrição da rede de VDC da organização.
- 7 Clique em **Avançar**.
- 8 Analise as configurações e clique em **Concluir**.

#### Resultados

Você pode ver a rede de grupo de centros de dados recém-criada na lista de redes da organização.

Seu tipo de rede é listado como Entre VDCs.

Uma rede de data centers virtuais da organização com o tipo de roteamento entre VDCs é criada para cada data center virtual participante. Você pode ver as redes de grupos de VDC dos centros de dados virtuais participantes clicando no cartão de um centro de dados virtual participante e, em seguida, em **Redes**. Se uma máquina virtual ou vApp se conectar a tal rede de centros de dados virtuais da organização, essa máquina virtual ou vApp se conectará à rede de grupos de VDC.

#### Próximo passo

Você pode atribuir endereços IP estáticos e pools de IPs a cada rede de data centers virtuais de organização entre VDCs. Consulte [Adicionar endereços IP a um pool de IPs de rede de data center virtual da organização](#).

Para configurações de DNS e DHCP para máquinas virtuais conectadas a uma rede de grupos de VDC, você pode usar o OpenAPI do VMware Cloud Director. Para examinar a documentação do OpenAPI do VMware Cloud Director, acesse [https://Cloud\\_Director\\_IP\\_address\\_or\\_host\\_name/docs](https://Cloud_Director_IP_address_or_host_name/docs). Para exibir exemplos de código e testar as chamadas do OpenAPI do VMware Cloud Director, acesse [https://Cloud\\_Director\\_IP\\_address\\_or\\_host\\_name/api-explorer?scope=organization\\_name](https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name).

### Exibir ou editar uma rede de grupos de centro de dados com suporte do NSX Data Center for vSphere

Você pode ver o nome, a descrição e as configurações de CIDR de uma rede de grupos de centros de dados com suporte do NSX Data Center for vSphere. Você pode editar apenas o nome e a descrição de uma rede de grupos de centros de dados com suporte do NSX Data Center for vSphere.

Para obter informações sobre como editar a alocação do pool de IPs estáticos para uma rede de grupos de centros de dados em um nível de centro de dados virtual, consulte [Adicionar endereços IP a um pool de IPs de rede de data center virtual da organização](#).

#### Pré-requisitos

Verifique se você recebeu a função predefinida de **Administrador da Organização** ou uma função que inclua os direitos **Rede de VDC da Organização: Exibir Propriedades** e **Rede de VDC da Organização: Editar Propriedades**.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Clique na rede de destino para visualizar detalhes.
- 3 Para editar o nome e a descrição das redes, clique em **Editar**.
- 4 Edite os detalhes da rede e clique em **Salvar**.

## Sincronizar rede de grupo de centros de dados com suporte do NSX Data Center for vSphere

Para garantir que todos os centros de dados virtuais participantes possam acessar a rede de grupo de centros de dados com suporte do NSX Data Center for vSphere, você pode sincronizar a rede de grupo de centros de dados.

### Pré-requisitos

Essa operação requer a função predefinida **Administrador da Organização** ou uma função com o direito **Rede VDC da Organização: Editar Propriedades**.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede**.
- 2 Na guia de redes, clique no botão de seleção ao lado do nome da rede de destino e, depois, em **Sincronizar**.
- 3 Para confirmar, clique em **OK**.

## Gerenciando serviços de edge gateway do NSX Data Center for vSphere

O VMware Cloud Director fornece os recursos de rede avançados com o software de virtualização de rede do NSX Data Center for vSphere que oferece controles de segurança aprimorados e recursos de roteamento e dimensionamento de rede em um ambiente de nuvem.

Usando esses recursos de rede, você pode obter segurança e isolamento sem precedentes no datacenter virtual da organização. Esses recursos oferecem os seguintes benefícios:

- Roteamento dinâmico. Os recursos do NSX Data Center for vSphere no seu ambiente do VMware Cloud Director dão suporte aos protocolos de roteamento, como o Border Gateway Protocol (BGP) e o Open Shortest Path First (OSPF), para simplificar a integração de rede entre sistemas, fornecendo redundância e continuidade na implantação do aplicativo hospedado em nuvem.
- Isolamento e segurança de rede refinados. Os recursos do NSX Data Center for vSphere no seu ambiente do VMware Cloud Director oferecem suporte ao uso de definições de regras baseadas em objetos para fornecer isolamento de tráfego de rede com monitoração de estado sem exigir várias redes virtuais. Esse modelo de segurança Zero Trust impede que intrusos obtenham acesso total à rede se um aplicativo ou máquina virtual estiver comprometido. A configuração de rede é simplificada usando as mesmas políticas de segurança de rede para proteger aplicativos onde quer que estejam fisicamente localizados no ambiente do VMware Cloud Director e para estender o modelo de segurança Zero Trust para a segurança portátil, independentemente de onde um aplicativo é implantado.
- Os recursos adicionais fornecidos pelo NSX Data Center for vSphere são: suporte VPN aprimorado para conectividade ponto a site (VPN IPsec) e usuário (SSL VPN-Plus), balanceamento de carga aprimorado para HTTPS e dimensionamento de rede expandido.



Você pode configurar dois tipos de firewalls: o firewall do edge gateway e o firewall distribuído. Para obter mais informações sobre as diferenças entre esses firewalls, consulte [Configuração de firewall de tenant com NSX Data Center for vSphere](#).

Você pode acessar esses recursos de rede avançados usando o Portal do Tenant do VMware Cloud Director ou o VMware Cloud Director Service Provider Admin Portal. O edge gateway deve ser convertido primeiro em um edge gateway avançado. Consulte [Converter um edge gateway do NSX Data Center for vSphere em um edge gateway avançado](#).

---

**Importante** Os gateways de borda IPv6 fornecem suporte aos serviços limitados. Os gateways de borda IPv6 oferecem suporte aos firewalls de borda, à distribuição de firewalls e ao roteamento estático.

---

## Introdução ao recuso de Rede Avançada do VMware Cloud Director com NSX Data Center for vSphere

Use o recurso de Rede Avançada do VMware Cloud Director para executar tarefas de gerenciamento em uma organização em um sistema VMware Cloud Director. Você pode gerenciar firewalls distribuídos e outros recursos avançados de rede fornecidos pelo NSX Data Center for vSphere e disponibilizados para uma organização por um administrador de sistema do VMware Cloud Director.

Os usuários típicos da rede avançada fornecida pelo NSX Data Center for vSphere são:

- **Administradores do sistema** do VMware Cloud Director, que podem usar o portal do tenant para configurar o firewall distribuído e outros recursos avançados de rede para uma organização.
- **Administradores de organizações**, que usam o portal do tenant para gerenciar o firewall distribuído e outros recursos de rede avançados que o **administrador do sistema** disponibilizou para essa organização.

## Configuração de firewall de tenant com NSX Data Center for vSphere

Usando o portal do tenant, você pode configurar os recursos de firewall fornecidos pelo NSX Data Center for vSphere no seu centro de dados virtual de organização do VMware Cloud Director. Você pode criar regras de firewall para firewalls distribuídos para fornecer segurança entre máquinas virtuais em um data center virtual de organização e regras de firewall para aplicar a um firewall de edge gateway para proteger as máquinas virtuais em um data center virtual de organização contra o tráfego de rede externo.

---

**Observação** O portal do tenant fornece a capacidade de configurar firewalls de edge gateway e firewalls distribuídos.

---

A tecnologia lógica de firewall do NSX Data Center for vSphere consiste em dois componentes para abordar diferentes casos de uso de implantação. O firewall do edge gateway concentra-se na imposição do tráfego de norte a sul, enquanto o firewall distribuído se concentra nos controles de acesso de leste a oeste.

## Principais diferenças entre firewalls de edge gateway e firewalls distribuídos

Um firewall de edge gateway monitora o tráfego norte-sul para fornecer funcionalidade de segurança de perímetro, incluindo firewall, conversão de endereços de rede (NAT), bem como a funcionalidade de IPSec de site para site e VPN SSL.

Um firewall distribuído fornece a capacidade de isolar e proteger cada máquina virtual e aplicativo no nível de camada 2 (L2). A configuração de firewalls distribuídos coloca em quarentena de forma efetiva qualquer comprometimento de segurança de rede externa ou interna, isolando o tráfego de leste a oeste entre máquinas virtuais no mesmo segmento de rede. As políticas de segurança são gerenciadas centralmente, herdáveis e aninhadas, para que os administradores de rede e segurança possam gerenciá-las em grande escala. Além disso, depois de implantadas, as políticas de segurança definidas seguem as máquinas virtuais ou os aplicativos ao se moverem entre diferentes data centers virtuais.

## Sobre regras de firewall

Conforme descrito na documentação do produto relevante, no NSX Data Center for vSphere, as regras de firewall definidas no nível centralizado são referidas como pré regras. Você também pode adicionar regras em um nível de edge gateway individual, e essas regras são referidas como regras locais.

Cada sessão de tráfego é verificada em relação à regra superior na tabela de firewall antes de mover as regras subsequentes para baixo na tabela. A primeira regra da tabela que corresponder aos parâmetros de tráfego será imposta. As regras são exibidas na seguinte ordem:

- 1 As pré-regras definidas pelo usuário têm a prioridade mais alta e são aplicadas em ordem de cima para baixo, com precedência por nível de NIC virtual.
- 2 Regras de auto-bombeamento (regras que permitem que o tráfego de controle flua para serviços de edge gateway).
- 3 Regras locais definidas em um nível de edge gateway.
- 4 Regra de firewall distribuído padrão

Para obter mais informações sobre como o software NSX Data Center for vSphere impõe regras de firewall, consulte *Alterar a Ordem de uma Regra de Firewall* na documentação do NSX Data Center for vSphere.

## Firewall do Edge Gateway do NSX Data Center for vSphere

O firewall do edge gateway ajuda a atender aos principais requisitos de segurança do perímetro, como a criação de DMZs com base em construções de IP/VLAN, isolamento de tenant para tenant em data centers virtuais de vários tenants, NAT (conversão de endereços de rede), parceiro (extranet) VPNs e VPNs SSL baseadas em usuário.

O recurso de firewall do edge gateway no ambiente VMware Cloud Director é fornecido pelo NSX Data Center for vSphere. No NSX Data Center for vSphere, esse recurso de firewall também é chamado de firewall do edge. O firewall de edge gateway monitora o tráfego norte-sul para fornecer funcionalidade de segurança de perímetro, incluindo firewall, conversão de endereços de rede (NAT), bem como a funcionalidade de IPsec de site para site e VPN SSL.

Para obter informações mais detalhadas sobre os recursos fornecidos pelo firewall do edge gateway do NSX Data Center for vSphere, consulte a documentação do NSX Data Center for vSphere.

## Gerenciando um firewall do edge gateway do NSX Data Center for vSphere

Para proteger o tráfego de e para um edge gateway, você pode criar e gerenciar regras de firewall nesse edge gateway.

Para obter informações sobre como proteger o tráfego se deslocando entre máquinas virtuais em um centro de dados virtual da organização, consulte [Gerenciamento de regras de firewall distribuído do NSX Data Center for vSphere usando o portal do tenant](#).

As regras criadas na tela de firewall distribuído que têm um edge gateway avançado especificado na coluna Aplicado a não são exibidas na tela Firewall desse edge gateway avançado.

As regras de firewall do edge gateway para um edge gateway são exibidas na tela **Firewall** e são aplicadas na seguinte ordem:

- 1 Regras internas, também conhecidas como regras de autobombeamento. Essas regras internas permitem que o tráfego de controle flua para serviços de edge gateway.
- 2 Regras definidas pelo usuário.
- 3 Regra padrão.

As configurações de regra padrão aplicam-se ao tráfego que não corresponde a nenhuma das regras de firewall definidas pelo usuário. A regra padrão é exibida na parte inferior das regras na tela Firewall.

No portal do tenant, use o botão de alternância **Ativar** na tela Regras de Firewall do edge gateway para desativar ou ativar um firewall de edge gateway.

## Converter um edge gateway do NSX Data Center for vSphere em um edge gateway avançado

Para trabalhar com um edge gateway do NSX Data Center for vSphere no portal do tenant, você precisa convertê-lo em um edge gateway avançado. Depois de convertê-lo em um edge gateway avançado, você poderá usar o portal do tenant para configurar os recursos de roteamento estático e dinâmico fornecidos pelo NSX Data Center for vSphere para esses edge gateways avançados.

### Pré-requisitos

Você tem um edge gateway existente.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.

2 Selecione o edge gateway a ser editado.

3 Clique em **Converter em Avançado**.

#### Resultados

Seu edge gateway é convertido em um edge gateway avançado.

#### Próximo passo

Depois de converter para um edge gateway avançado, você pode definir as configurações selecionando o gateway e clicando em **Serviços**.

#### Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere

Use a guia **Firewall** do edge gateway para adicionar regras de firewall para esse edge gateway. Você pode adicionar várias interfaces do NSX Edge e vários grupos de endereços IP como a origem e o destino para essas regras de firewall.

A especificação de **Interno** para uma origem ou um destino de uma regra indica o tráfego de todas as sub-redes nos grupos de portas conectados ao gateway do NSX Edge. Se você selecionar **Interno** como a origem, a regra será automaticamente atualizada quando as interfaces internas adicionais forem configuradas no gateway do NSX.

---

**Observação** As regras de firewall de edge gateway em interfaces internas não funcionam quando o edge gateway está configurado para roteamento dinâmico.

---

#### Procedimentos

1 Abra Serviços de Edge Gateway.

a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.

b Selecione o edge gateway que você deseja editar e clique em **Serviços**.

2 Se a tela **Regras de Firewall** ainda não estiver visível, clique na guia **Firewall**.

3 Para adicionar uma regra abaixo de uma regra existente na tabela de regras de firewall, clique na linha existente e, em seguida, clique no botão **Criar**.

Uma linha para a nova regra é adicionada abaixo da regra selecionada e são atribuídos qualquer destino, qualquer serviço e a ação **Permitir** por padrão. Quando a regra de permissão padrão definida pelo sistema é a única na tabela de firewall, a nova regra é adicionada acima da regra padrão.

4 Clique na célula **Nome** e digite um nome.

- 5 Clique na célula **Origem** e use os ícones visíveis agora para selecionar uma origem a ser adicionada à regra:

Opção	Descrição
Clique no ícone IP.	Digite o valor de origem que deseja usar. Os valores válidos podem ser o endereço IP, o CIDR, o intervalo de IPs ou a palavra-chave <b>any</b> . O firewall do edge gateway suporta os formatos IPv4 e IPv6.
Clique no ícone +	<p>Use o ícone + para especificar a origem como um objeto diferente de um endereço IP específico:</p> <ul style="list-style-type: none"> <li>■ Use a janela <b>Selecionar objetos</b> para adicionar objetos que correspondem às suas seleções e clique em <b>Manter</b> para adicioná-los à regra.</li> <li>■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela <b>Selecionar objetos</b> e selecione o ícone de exclusão de alternância a fim de excluir essa origem dessa regra.</li> </ul> <p>Quando a exclusão de alternância é selecionada na origem, a regra é aplicada ao tráfego proveniente de todas as origens, exceto para a origem excluída. Quando a exclusão de alternância não é selecionada, a regra se aplica ao tráfego proveniente da origem especificada na janela <b>Selecionar objetos</b>.</p>

- 6 Clique na célula **Destino** e execute uma das seguintes ações:

Opção	Descrição
Clique no ícone IP.	Digite o valor de destino que você deseja usar. Os valores válidos podem ser o endereço IP, o CIDR, o intervalo de IPs ou a palavra-chave <b>any</b> . O firewall do edge gateway suporta os formatos IPv4 e IPv6.
Clique no ícone +	<p>Use o ícone + para especificar a origem como um objeto diferente de um endereço IP específico:</p> <ul style="list-style-type: none"> <li>■ Use a janela <b>Selecionar objetos</b> para adicionar objetos que correspondem às suas seleções e clique em <b>Manter</b> para adicioná-los à regra.</li> <li>■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela <b>Selecionar objetos</b> e, em seguida, selecione o ícone de exclusão de alternância para excluir essa origem dessa regra.</li> </ul> <p>Quando a exclusão de alternância é selecionada na origem, a regra é aplicada ao tráfego proveniente de todas as origens, exceto para a origem excluída. Quando a exclusão de alternância não é selecionada, a regra se aplica ao tráfego proveniente da origem especificada na janela <b>Selecionar objetos</b>.</p>

- 7 Clique na célula **Serviço** da nova regra e clique no ícone + para especificar o serviço como uma combinação de porta-protocolo:
- Selecione o protocolo de serviço.
  - Digite os números de porta para as portas de origem e de destino ou especifique **qualquer**.
  - Clique em **Manter**.

- 8 Na célula **Ação** da nova regra, configure a ação para a regra.

Opção	Descrição
<b>Aceitar</b>	Permite o tráfego de ou para origens, destinos e serviços especificados.
<b>Negar</b>	Bloqueia o tráfego de ou para origens, destinos e serviços especificados.

- 9 Clique em **Salvar alterações**.

A operação de salvamento pode levar um minuto para ser concluída.

### Modificar regras de firewall do edge gateway do NSX Data Center for vSphere

Você pode editar e excluir apenas as regras de firewall definidas pelo usuário que foram adicionadas a um edge gateway. Não é possível editar ou excluir uma regra gerada automaticamente ou uma regra padrão, exceto para alterar a configuração de ação da regra padrão. Você pode alterar a ordem de prioridade das regras definidas pelo usuário.

Para obter detalhes sobre as configurações disponíveis para as várias células de uma regra, consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

#### Procedimentos

- Abra Serviços de Edge Gateway.
  - Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- Clique na guia **Firewall**.
- Gerencie as regras de firewall.
  - Desative uma regra clicando na marca de seleção verde em sua célula N°. A marca de seleção verde se transforma em um ícone vermelho desativado. Se a regra estiver desativada e você quiser ativá-la, clique no ícone vermelho desativado.
  - Edite um nome de regra clicando duas vezes na célula **Nome** e digitando o novo nome.
  - Modifique as configurações de uma regra, como as configurações de origem ou de ação, selecionando a célula apropriada e usando os controles exibidos.
  - Exclua uma regra selecionando-a e clicando no botão **Excluir** localizado acima da tabela de regras.
  - Oculte as regras geradas pelo sistema usando a opção **Mostrar apenas as regras definidas pelo usuário**.
  - Mova uma regra para cima ou para baixo na tabela de regras selecionando a regra e clicando nos botões de seta para cima e para baixo localizados acima da tabela de regras.
- Clique em **Salvar alterações**.

## Firewall distribuído do NSX Data Center for vSphere

O firewall distribuído permite segmentar as entidades do centro de dados virtual da organização, como máquinas virtuais, com base em nomes e atributos de máquinas virtuais.

O VMware Cloud Director oferece suporte a serviços de firewall distribuídos em centros de dados virtuais da organização com suporte do NSX Data Center for vSphere. Conforme descrito na documentação do NSX Data Center for vSphere, esse firewall distribuído é um firewall incorporado ao kernel do hipervisor que oferece visibilidade e controle para cargas de trabalho e redes virtualizadas. Você pode criar políticas de controle de acesso com base em objetos como nomes de máquinas virtuais e em construções de rede, como endereços IP ou endereços de conjuntos de IPs. Regras de firewall são aplicadas no nível de vNIC de cada máquina virtual para fornecer controle de acesso consistente, mesmo quando a máquina virtual é movida para um novo host ESXi pelo vSphere vMotion. Esse firewall distribuído oferece suporte a um modelo de segurança de micro segmentação em que o tráfego do leste-oeste pode ser inspecionado no próximo processamento da taxa de linha.

Conforme descrito na documentação do NSX Data Center for vSphere, para pacotes da camada 2 (L2), o firewall distribuído cria um cache para aumento de desempenho. Os pacotes da camada 3 (L3) são processados na seguinte sequência:

- 1 Todos os pacotes são verificados em busca de um estado existente.
  - 2 Quando uma correspondência de estado é encontrada, os pacotes são processados.
  - 3 Quando uma correspondência de estado não é encontrada, os pacotes são processados através das regras até que uma correspondência seja encontrada.
- Para pacotes TCP, um estado é definido apenas para pacotes com um sinalizador SYN. No entanto, as regras que não especificam um protocolo (serviço), podem corresponder aos pacotes TCP com qualquer combinação de sinalizadores.
  - Para pacotes UDP, os detalhes de 5 tuplas são extraídos do pacote. Quando um estado não existe na tabela de estado, um novo estado é criado usando os detalhes de 5 tuplas extraídas. Os pacotes recebidos posteriormente são correspondidos em relação ao estado que acabou de ser criado.
  - Para pacotes ICMP, o tipo de ICMP, o código e a direção do pacote são usados para criar um estado.

O firewall distribuído também pode ajudar a criar regras baseadas em identidade. Os administradores podem impor o controle de acesso com base na associação de grupo do usuário, conforme definido no Active Directory (AD) corporativo. Alguns casos de uso para quando você pode usar as regras de firewall com base em identidade são:

- Usuários que acessam aplicativos virtuais usando um laptop ou dispositivo móvel no qual o AD é usado para autenticação de usuário
- Usuários que acessam aplicativos virtuais usando a infraestrutura VDI em que as máquinas virtuais são baseadas no Microsoft Windows

Para obter informações mais detalhadas sobre os recursos fornecidos pelo firewall distribuído, consulte a documentação do NSX Data Center for vSphere.

## Ativar o firewall distribuído em um centro de dados virtual de organização com suporte do NSX Data Center for vSphere

Para poder usar o portal do tenant para trabalhar com os recursos de firewall distribuído fornecido pelo NSX Data Center for vSphere em um centro de dados virtual de organização, o firewall distribuído deve ser ativado para esse centro de dados virtual de organização.

Um administrador de sistema do VMware Cloud Director ou um usuário com o direito **org\_vdc\_distributed\_firewall\_enable** pode ativar o firewall distribuído em um centro de dados virtual de organização.

Use a tela Firewall Distribuído no portal do tenant para habilitar o firewall distribuído para um data center virtual de organização.

### Pré-requisitos

Verifique se a organização à qual o data center virtual de organização pertence tem os seguintes direitos atribuídos:

- Firewall Distribuído do vDC de Organização: Habilitar/Desabilitar
- Firewall Distribuído do vDC de Organização: Configurar Regras
- Firewall Distribuído do vDC de Organização: Exibir Regras

O VMware Cloud Director **administrador do sistema** atribui direitos a uma organização. O direito Firewall Distribuído do vDC de Organização: Ativar/Desativar é necessário para ativar o firewall distribuído usando a interface do usuário no portal do tenant. O direito Firewall Distribuído do vDC de Organização: Exibir Regras é necessário para exibir as regras de firewall no portal do tenant, enquanto o direito Firewall Distribuído do vDC de Organização: Configurar Regras é necessário para configurar as regras de firewall usando o portal do tenant.

Verifique se você tem uma função atribuída que lhe conceda o direito chamado Firewall Distribuído do vDC de Organização: Habilitar/Desabilitar. Das funções predefinidas em um sistema VMware Cloud Director, somente a função de Administrador do Sistema tem esse direito por padrão.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione o data center virtual de organização para o qual você deseja configurar regras de firewall distribuído.
- 3 Clique em **Configurar Serviços**.
- 4 Habilite o firewall distribuído na guia **Firewall Distribuído**.



## Próximo passo

Para obter uma descrição da regra de firewall distribuído padrão, consulte [Gerenciamento de regras de firewall distribuído do NSX Data Center for vSphere usando o portal do tenant](#).

## Gerenciamento de regras de firewall distribuído do NSX Data Center for vSphere usando o portal do tenant

Conforme descrito na documentação do NSX Data Center for vSphere, as configurações de firewall padrão se referem ao tráfego que não corresponde a qualquer uma das regras de firewall definidas pelo usuário. No VMware Cloud Director Tenant Portal, a regra de firewall distribuído padrão é rotulada como Regra de Permissão Padrão.

O recurso de firewall distribuído deve ser habilitado em um centro de dados virtual de organização antes que você possa gerenciar as configurações do firewall distribuído usando o VMware Cloud Director Tenant Portal.

A regra de firewall distribuído padrão é configurada para permitir que todo o tráfego da camada 3 e da camada 2 passe pelo data center virtual da organização. Essa configuração é indicada pela definição de permissão na coluna ação da interface do usuário. A regra padrão está sempre na parte inferior da tabela de regras.

---

**Importante** Não é possível excluir ou modificar as regras padrão de firewall distribuído.

---

### Adicionar uma regra de firewall distribuído

Primeiro, adicione uma regra de firewall distribuído ao escopo do centro de dados virtual da organização. Em seguida, você pode restringir o escopo ao qual deseja aplicar a regra. O firewall distribuído permite adicionar vários objetos aos níveis de origem e de destino para cada regra, o que ajuda a reduzir o número total de regras de firewall a serem adicionadas.

Para obter informações sobre os serviços e os grupos de serviços predefinidos que você pode usar em uma regra, consulte [Exibir serviços disponíveis para regras de firewall](#) e [Exibir grupos de serviços disponíveis para regras de firewall](#).

### Pré-requisitos

- [Ativar o firewall distribuído em um centro de dados virtual de organização com suporte do NSX Data Center for vSphere](#)
- Se você quiser usar um conjunto de IPs como origem ou destino em uma regra, [Criar um conjunto de IPs para uso em regras de firewall e configuração de retransmissão DHCP](#).
- Se você quiser usar um conjunto de MACs como origem ou destino em uma regra, [Criar um conjunto de MACs para uso em regras de firewall](#).
- Se você quiser usar um grupo de segurança como origem ou destino em uma regra, [Criar um grupo de segurança](#).

## Procedimentos


- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.

- 2 Selecione a rede de VDC de serviços de segurança cujas regras de firewall você deseja modificar e clique em **Configurar Serviços**.

A tela Serviços de Segurança é exibida.

- 3 Selecione o tipo de regra que deseja criar. Você tem a opção de criar uma regra geral ou uma regra de Ethernet.

As regras da camada 3 (L3) são configuradas na guia **Geral**. As regras da camada 2 (L2) são configuradas na guia **Ethernet**.

- 4 Para adicionar uma regra abaixo de uma regra existente na tabela de firewall, clique na linha existente e, em seguida, clique no botão **Criar** ().

Uma linha para a nova regra é adicionada abaixo da regra selecionada e são atribuídos qualquer destino, qualquer serviço e a ação **Permitir** por padrão. Quando a regra de permissão padrão definida pelo sistema é a única regra na tabela de firewall, a nova regra é adicionada acima da regra padrão.

- 5 Clique na célula **Nome** e digite um nome.
- 6 Clique na célula **Origem** e use os ícones visíveis agora para selecionar uma origem a ser adicionada à regra:

Ação	Descrição
Clique no ícone IP.	<p>Aplicável a regras definidas na guia <b>Geral</b>.</p> <p>Digite o valor de origem que deseja usar. Os valores válidos podem ser o endereço IP, o CIDR, o intervalo de IPs ou a palavra-chave <b>any</b>. O firewall distribuído oferece suporte apenas ao formato IPv4.</p>
Clique no ícone +	<p>Use o ícone + para especificar a origem como um objeto diferente de um endereço IP específico:</p> <ul style="list-style-type: none"> <li>■ Use a janela <b>Selecionar objetos</b> para adicionar objetos que correspondem às suas seleções e clique em <b>Manter</b> para adicioná-los à regra.</li> <li>■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela <b>Selecionar objetos</b> e selecione o ícone de exclusão de alternância a fim de excluir essa origem dessa regra.</li> </ul> <p>Quando a exclusão de alternância é selecionada na origem, a regra é aplicada ao tráfego proveniente de todas as origens, exceto para a origem excluída. Quando a exclusão de alternância não é selecionada, a regra se aplica ao tráfego proveniente da origem especificada na janela <b>Selecionar objetos</b>.</p>

## 7 Clique na célula **Destino** e execute uma das seguintes ações:

Ação	Descrição
Clique no ícone IP.	Aplicável a regras definidas na guia <b>Geral</b> . Digite o valor de destino que você deseja usar. Os valores válidos podem ser o endereço IP, o CIDR, o intervalo de IPs ou a palavra-chave <b>any</b> . O firewall distribuído oferece suporte apenas ao formato IPv4.
Clique no ícone +	Use o ícone + para especificar a origem como um objeto diferente de um endereço IP específico: <ul style="list-style-type: none"> <li>■ Use a janela <b>Selecionar objetos</b> para adicionar objetos que correspondem às suas seleções e clique em <b>Manter</b> para adicioná-los à regra.</li> <li>■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela <b>Selecionar objetos</b> e, em seguida, selecione o ícone de exclusão de alternância para excluir essa origem dessa regra.</li> </ul> Quando a exclusão de alternância é selecionada na origem, a regra é aplicada ao tráfego proveniente de todas as origens, exceto para a origem excluída. Quando a exclusão de alternância não é selecionada, a regra se aplica ao tráfego proveniente da origem especificada na janela <b>Selecionar objetos</b> .

## 8 Clique na célula **Serviço** da nova regra e execute uma das seguintes ações:

Ação	Descrição
Clique no ícone IP.	Para especificar o serviço como uma combinação de porta e protocolo: <ol style="list-style-type: none"> <li>Selecione o protocolo de serviço.</li> <li>Digite os números para as portas de origem e de destino ou especifique <b>any</b> e clique em <b>Manter</b>.</li> </ol>
Clique no ícone +	Para selecionar um serviço ou um grupo de serviços predefinido ou definir um novo: <ol style="list-style-type: none"> <li>Selecione um ou mais objetos e adicione-os ao filtro.</li> <li>Clique em <b>Manter</b>.</li> </ol>

## 9 Na célula **Ação** da nova regra, configure a ação para a regra.

Opção	Descrição
<b>Permitir</b>	Permite o tráfego de ou para origens, destinos e serviços especificados.
<b>Negar</b>	Bloqueia o tráfego de ou para origens, destinos e serviços especificados.

## 10 Na célula **Direção** da nova regra, selecione se a regra se aplica a tráfego de entrada, tráfego de saída ou a ambos.

## 11 Se esta for uma regra na guia **Geral**, na célula **Tipo de Pacote** da nova regra, selecione um tipo de pacote: **Qualquer**, **IPV4** ou **IPV6**.

- 12 Selecione a célula **Aplicada A** e use o ícone **+** para definir o escopo do objeto ao qual essa regra é aplicável.

Quando a regra contém máquinas virtuais nas células **Origem** e **Destino**, você deve adicionar as máquinas virtuais de origem e de destino à regra **Aplicado A** para que a regra funcione corretamente.

---

**Importante** Grupos de endereços IP (conjuntos de IPs), grupos de endereços MAC (conjuntos MAC) e grupos de segurança que contêm conjuntos de IPs ou conjuntos de MACs não são parâmetros de entrada válidos.

---

- 13 Clique em **Salvar Alterações**.

### Editar uma regra de firewall distribuído

Em um ambiente VMware Cloud Director, para modificar uma regra de firewall distribuído existente de um centro de dados virtual da organização, use a tela **Firewall Distribuído**.

Para obter detalhes sobre as configurações disponíveis para as várias células de uma regra, consulte [Adicionar uma regra de firewall distribuído](#).

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.

- 2 Selecione a rede de VDC de serviços de segurança cujas regras de firewall você deseja modificar e clique em **Configurar Serviços**.

A tela Serviços de Segurança é exibida.

- 3 Realize qualquer uma das seguintes ações para gerenciar as regras de firewall distribuído:

- Desative uma regra clicando na marca de seleção verde em sua célula N° .  
A marca de seleção verde se transforma em um ícone vermelho desativado. Se a regra estiver desativada e você quiser ativá-la, clique no ícone vermelho desativado.
- Edite um nome de regra clicando duas vezes na célula **Nome** e digitando o novo nome.
- Modifique as configurações de uma regra, como as configurações de origem ou de ação, selecionando a célula apropriada e usando os controles exibidos.
- Exclua uma regra selecionando-a e clicando no botão **Excluir** localizado acima da tabela de regras.
- Mova uma regra para cima ou para baixo na tabela de regras selecionando a regra e clicando nos botões de seta para cima e para baixo localizados acima da tabela de regras.

- 4 Clique em **Salvar Alterações**.

## Gerenciando o DHCP do edge gateway do NSX Data Center for vSphere

Você configura os edge gateways para fornecer serviços de protocolo DHCP para máquinas virtuais conectadas às redes de centros de dados virtuais de organização associadas.

Conforme descrito na [documentação do NSX](#), os recursos de edge gateway do NSX incluem o pool de endereços IP, a alocação de um endereço IP estático de um para um e a configuração do servidor DNS externo. A associação de endereços IP estáticos é baseada no ID do objeto gerenciado e no ID da interface da máquina virtual do cliente solicitante.

O serviço DHCP para um gateway do NSX Edge:

- Escuta a interface interna do edge gateway para a descoberta DHCP.
- Usa o endereço IP da interface interna do edge gateway como o endereço de gateway padrão para todos os clientes.
- Usa os valores de difusão e máscara de sub-rede da interface interna para a rede de contêiner.

Nas situações a seguir, você precisa reiniciar o serviço DHCP nas máquinas virtuais do cliente que têm os endereços IP atribuídos por DHCP:

- Você alterou ou excluiu um pool DHCP, um gateway padrão ou um servidor DNS.
- Você alterou o endereço IP interno da instância do edge gateway.

---

**Observação** Se as configurações de DNS em um edge gateway com DHCP ativado, o edge gateway poderá parar de fornecer serviços DHCP. Se essa situação ocorrer, use a tela **Status do Serviço DHCP** na tela Pools DHCP para desativar e, em seguida, reativar o DHCP nesse edge gateway. Consulte [Adicionar um pool de IPs DHCP](#).

---

### Adicionar um pool de IPs DHCP

Você pode configurar os pools de IPs necessários para um serviço DHCP de um edge gateway do NSX Data Center for vSphere. O DHCP automatiza a atribuição de endereços IP a máquinas virtuais conectadas a redes de data centers virtuais da organização.

Conforme descrito na documentação *Administração do NSX*, o serviço DHCP requer um pool de endereços IP. Um pool de IPs é um intervalo sequencial de endereços IP na rede. As máquinas virtuais protegidas pelo edge gateway que não têm uma associação de endereço recebem um endereço IP desse pool. Os intervalos de pools de IPs não podem se interseccionar, portanto, um endereço IP pode pertencer a apenas um pool de IPs.

---

**Observação** Pelo menos um pool de IPs DHCP deve ser configurado para que o status do serviço DHCP seja ativado.

---

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue para **DHCP > Pools**.
- 3 Se o serviço DHCP não estiver ativado no momento, ative a opção **Status do Serviço DHCP**.

**Observação** Adicione pelo menos um pool de IPs DHCP antes de salvar as alterações depois de ativar o **Status do Serviço DHCP**. Se nenhum pool de IPs DHCP estiver listado na tela e você ativar a opção **Status do Serviço DHCP** e salvar as alterações, a tela será exibida com a opção esmaecida.

- 4 Em Pools DHCP, clique no botão **Criar** () , especifique os detalhes do pool de DHCP e clique em **Manter**.

Opção	Descrição
Intervalo de IPs	Digite um intervalo de endereços IP.
Nome de Domínio	Nome do domínio do servidor DNS.
Configurar DNS Automaticamente	Ative esta opção para usar a configuração do serviço DNS para esta associação de DNS do pool de IPs. Se ativados, o <b>Servidor de Nome Primário</b> e o <b>Servidor de Nome Secundário</b> serão definidos para <b>Automático</b> .
Servidor de Nome Primário	Quando você não ativar a opção <b>Configurar DNS Automaticamente</b> , digite seu endereço IP do servidor DNS primário. Este endereço IP é usado para a resolução de nomes de host em endereços IP.
Servidor de Nome Secundário	Quando você não ativar a opção <b>Configurar DNS Automaticamente</b> , digite seu endereço IP do servidor DNS secundário. Este endereço IP é usado para a resolução de nomes de host em endereços IP.
Gateway Padrão	Digite o endereço do gateway padrão. Quando você não especifica o endereço IP do gateway padrão, a interface interna da instância do edge gateway é considerada o gateway padrão.
Máscara de Sub-Rede	Digite a máscara de sub-rede da interface do edge gateway.

Opção	Descrição
<b>Lease Nunca Expira</b>	Habilite essa opção para manter indefinidamente a associação entre os endereços IP atribuídos desse pool a suas máquinas virtuais atribuídas. Quando você seleciona essa opção, o <b>Tempo de Lease</b> fica definido como infinito.
<b>Tempo de Lease (Segundos)</b>	Período de tempo (em segundos) que os endereços IP atribuídos por DHCP são concedidos aos clientes. O tempo de lease padrão é um dia (86.400 segundos).
<b>Observação</b> Não é possível especificar um tempo de lease quando você seleciona <b>Lease Nunca Expira</b> .	

## 5 Clique em **Salvar alterações**.

### Resultados

O VMware Cloud Director atualiza o edge gateway para fornecer serviços DHCP.


## Adicionar vinculações de DHCP

Se você tiver serviços em execução em uma máquina virtual e não quiser que o endereço IP seja alterado, será possível vincular o endereço MAC da máquina virtual ao endereço IP. O endereço IP que você vincular não deve se sobrepor a um pool de IPs DHCP.

### Pré-requisitos

Você tem os endereços MAC das máquinas virtuais para as quais deseja configurar vinculações.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Na guia **DHCP > Vinculações**, clique no botão **Criar** () e, especifique os detalhes da associação e clique em **Manter**.

Opção	Descrição
<b>Endereço MAC</b>	Digite o endereço MAC da máquina virtual que você deseja vincular ao endereço IP.
<b>Nome do Host</b>	Digite o nome do host que deseja definir para essa máquina virtual quando a máquina virtual solicitar uma concessão de DHCP.
<b>Endereço IP</b>	Digite o endereço IP que você deseja vincular ao endereço MAC.
<b>Máscara de Sub-Rede</b>	Digite a máscara de sub-rede da interface do edge gateway.
<b>Nome de Domínio</b>	Digite o nome do domínio do servidor DNS.

Opção	Descrição
<b>Configurar DNS Automaticamente</b>	Ative esta opção para usar a configuração do serviço DNS para esta vinculação de DNS.  Se ativados, o <b>Servidor de Nome Primário</b> e o <b>Servidor de Nome Secundário</b> serão definidos para <b>Automático</b> .
<b>Servidor de Nome Primário</b>	Quando você não selecionar a opção <b>Configurar DNS Automaticamente</b> , digite seu endereço IP do servidor DNS primário.  Este endereço IP é usado para a resolução de nomes de host em endereços IP.
<b>Servidor de Nome Secundário</b>	Quando você não selecionar a opção <b>Configurar DNS Automaticamente</b> , digite seu endereço IP do servidor DNS secundário.  Este endereço IP é usado para a resolução de nomes de host em endereços IP.
<b>Gateway Padrão</b>	Digite o endereço do gateway padrão.  Quando você não especifica o endereço IP do gateway padrão, a interface interna da instância do edge gateway é considerada o gateway padrão.
<b>Lease Nunca Expira</b>	Ative essa opção para manter o endereço IP vinculado a esse endereço MAC para sempre.  Quando você seleciona essa opção, o <b>Tempo de Lease</b> fica definido como infinito.
<b>Tempo de Lease (Segundos)</b>	Período de tempo (em segundos) que os endereços IP atribuídos por DHCP são concedidos aos clientes.  O tempo de lease padrão é um dia (86.400 segundos).  <b>Observação</b> Não é possível especificar um tempo de lease quando você seleciona <b>Lease Nunca Expira</b> .

### 3 Clique em **Salvar alterações**.

## Configurando a retransmissão DHCP para edge gateways do NSX Data Center for vSphere

A capacidade de retransmissão DHCP fornecida pelo NSX no seu ambiente VMware Cloud Director permite que você aproveite a infraestrutura de DHCP existente no seu ambiente VMware Cloud Director sem qualquer interrupção no gerenciamento de endereços IP em sua infraestrutura de DHCP existente. As mensagens DHCP são retransmitidas de máquinas virtuais para os servidores DHCP designados na sua infraestrutura DHCP física, o que permite que os endereços IP controlados pelo software NSX continuem a ser sincronizados com endereços IP no restante dos seus ambientes controlados por DHCP.

A configuração de retransmissão DHCP de um edge gateway pode listar vários servidores DHCP. As solicitações são enviadas para todos os servidores listados. Ao transmitir a solicitação DHCP das VMs, o edge gateway adiciona um endereço IP de gateway à solicitação. O servidor DHCP externo usa esse endereço de gateway para corresponder um pool e alocar um endereço IP para a solicitação. O endereço do gateway deve pertencer a uma sub-rede da interface do edge gateway.



Você pode especificar um servidor DHCP diferente para cada edge gateway e pode configurar vários servidores DHCP em cada edge gateway para oferecer suporte a vários domínios IP.

---

### Observação

- A retransmissão DHCP não oferece suporte à sobreposição de espaços de endereço IP.
  - A retransmissão DHCP e o serviço DHCP não podem ser executados na mesma vNIC ao mesmo tempo. Se um agente de retransmissão estiver configurado em um vNIC, um pool DHCP não poderá ser configurado nas sub-redes dessa vNIC. Consulte o *Guia de Administração do NSX* para obter mais detalhes.
- 

## Especificar uma configuração de retransmissão DHCP para um edge gateway do NSX Data Center for vSphere

O software NSX no seu ambiente VMware Cloud Director fornece a capacidade para o edge gateway retransmitir mensagens de DHCP para servidores DHCP externos ao centro de dados virtual da organização VMware Cloud Director. Você pode configurar a capacidade de retransmissão DHCP do edge gateway.

Conforme descrito na documentação *Administração do NSX*, os servidores DHCP podem ser especificados usando um conjunto de IPs existente, um bloco de endereços IP, um domínio ou uma combinação de todos esses. As mensagens de DHCP são retransmitidas para cada servidor DHCP especificado.


Você também deve configurar pelo menos um agente de retransmissão de DHCP. Um agente de retransmissão de DHCP é uma interface no edge gateway do qual as solicitações de DHCP são retransmitidas para os servidores DHCP externos.


### Pré-requisitos

Se você quiser usar um conjunto de IPs para especificar um servidor DHCP, verifique se existe um conjunto de IPs como um objeto de agrupamento disponível para o edge gateway. Consulte [Criar um conjunto de IPs para uso em regras de firewall e configuração de retransmissão DHCP](#).

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Acesse **DHCP > Retransmissão**.
- 3 Use os campos na tela para especificar os servidores DHCP por endereços IP, nomes de domínio ou conjuntos de IPs.

Você seleciona em conjuntos de IPs existentes usando o botão **Adicionar** () para procurar os conjuntos de IPs disponíveis.

- 4 Configure um agente de retransmissão de DHCP e adicione sua configuração à tabela na tela clicando no botão **Adicionar** () , selecionando um vNIC e seu endereço IP do gateway e clicando em **Manter**.

Por padrão, o endereço IP do gateway corresponde ao endereço principal do vNIC selecionado. Você pode manter o padrão ou selecionar um endereço alternativo se algum estiver disponível nesse vNIC.

- 5 Clique em **Salvar alterações**.

## Gerenciamento da conversão de endereços de rede (NAT) em um Edge Gateway do NSX Data Center for vSphere

O software NSX Data Center for vSphere no seu ambiente VMware Cloud Director permite que os edge gateways forneçam um serviço de conversão de endereços de rede (NAT). Usar esse recurso reduz o número de endereços IP públicos que uma organização deve usar, por fins de economia e de segurança.

O serviço NAT do edge gateway fornece a capacidade de atribuir um endereço público a uma máquina virtual ou a um grupo de máquinas virtuais em uma rede privada. Para permitir que seus edge gateways forneçam acesso a serviços em execução em máquinas virtuais endereçadas privadamente no data center virtual de organização, você deve configurar as regras de NAT nos edge gateways. No caso mais comum, você associa um serviço NAT a uma interface de uplink em um edge gateway no seu ambiente VMware Cloud Director para que os endereços em redes de data centers virtuais de organização não fiquem expostos na rede externa.

A configuração do serviço NAT é separada nas regras de NAT (SNAT) de origem e NAT de destino (DNAT). Ao configurar uma regra de SNAT ou de DNAT em um edge gateway no ambiente do VMware Cloud Director, você sempre configura a regra da perspectiva do data center virtual da sua organização. Especificamente, isso significa que você configura as regras das seguintes maneiras:

- **SNAT:** o tráfego está viajando de uma máquina virtual em uma rede interna no seu data center virtual de organização (a origem) através da Internet para a rede externa (o destino). Uma regra de SNAT converte o endereço IP de origem dos pacotes de saída de uma rede de data center virtual de organização que estão sendo enviadas para uma rede externa ou para outra rede de data center virtual de organização.
- **DNAT:** o tráfego está viajando da Internet (a origem) para uma máquina virtual dentro do data center virtual de organização (o destino). Uma regra de DNAT converte o endereço IP (e, opcionalmente, a porta) de pacotes recebidos por uma rede de data centers virtuais da organização provenientes de uma rede externa ou de outra rede de data centers virtuais da organização.

Você pode configurar as regras de NAT para criar um espaço de endereço IP privado no seu data center virtual de organização. Essa configuração fornece a capacidade de portar um espaço de endereço IP privado de um data center virtual de organização para outro. A configuração de regras de NAT permite que você use os mesmos endereços IP privados para suas máquinas virtuais em um data center virtual da organização que foram usados em outro.

A capacidade da regra de NAT no seu ambiente VMware Cloud Director oferece suporte a:

- Criar sub-redes no espaço de endereço IP privado
- Criar vários espaços de endereço IP privados para um edge gateway
- Configurar várias regras de NAT em várias interfaces de edge gateway

---

**Importante** Você deve configurar as regras de firewall e NAT em um edge gateway para que as máquinas virtuais em uma rede de edge gateway fiquem acessíveis. Por padrão, os edge gateways são implantados com regras de firewall configuradas para negar todo o tráfego de rede de e para as máquinas virtuais nas redes de edge gateway. Além disso, o NAT é desativado por padrão nos edge gateways para que os edge gateways não consigam converter os endereços IP do tráfego de entrada e saída, a menos que você configure o NAT nos edge gateways. A tentativa de efetuar ping em uma máquina virtual em uma rede após a configuração de uma regra de NAT falhará, a menos que você adicione uma regra de firewall para permitir o tráfego correspondente.

---

## Adicionar uma regra de SNAT ou de DNAT

Você pode criar uma regra de NAT (SNAT) de origem para alterar o endereço IP de origem de um endereço IP público para privado ou vice-versa. Você pode criar uma regra de NAT (DNAT) de destino para alterar o endereço IP de destino de um endereço IP público para privado ou vice-versa.

Ao criar regras de NAT, você pode especificar os endereços IP originais e convertidos usando os seguintes formatos:

- Endereço IP; por exemplo, 192.0.2.0
- Intervalo de endereços IP; por exemplo, 192.0.2.0-192.0.2.24
- Endereço IP/máscara de sub-rede; por exemplo, 192.0.2.0/24
- any

Ao configurar uma regra de SNAT ou de DNAT em um edge gateway no ambiente do VMware Cloud Director, você sempre configura a regra da perspectiva do data center virtual da sua organização. Uma regra de SNAT converte o endereço IP de origem dos pacotes enviados de uma rede de data center virtual da organização em uma rede externa ou em outra rede de data centers virtuais da organização. Uma regra de DNAT converte o endereço IP (e, opcionalmente, a porta) de pacotes recebidos por uma rede de data centers virtuais da organização provenientes de uma rede externa ou de outra rede de data centers virtuais da organização.

## Pré-requisitos

Os endereços IP públicos devem ter sido adicionados à interface do edge gateway do NSX Data Center for vSphere na qual você deseja adicionar a regra. Para as regras de DNAT, o endereço IP original (público) deve ter sido adicionado à interface do edge gateway. Para regras de SNAT, o endereço IP convertido (público) deve ter sido adicionado à interface.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique em **NAT** para exibir a tela Regras de NAT.
- 3 Dependendo do tipo de regra de NAT que você está criando, clique em **Regra de DNAT** ou **Regra de SNAT**.
- 4 Configure uma regra de NAT de destino (de fora para dentro).

Opção	Descrição
Aplicado em	Selecione a interface na qual aplicar a regra.
IP/Intervalo Original	Digite o endereço IP necessário ou selecione o endereço IP alocado na lista. Esse endereço deve ser o endereço IP público do edge gateway para o qual você está configurando a regra de DNAT. No pacote que está sendo inspecionado, esse endereço IP ou intervalo seria o que aparece como o endereço IP de destino do pacote. Esses endereços de destino do pacote são aqueles convertidos por essa regra de DNAT.
Protocolo	Selecione o protocolo ao qual a regra se aplica. Para aplicar essa regra a todos os protocolos, selecione <b>Qualquer</b> .
Porta Original	(Opcional) Selecione a porta ou o intervalo de portas que o tráfego de entrada usa no edge gateway para se conectar à rede interna à qual as máquinas virtuais estão conectadas. Esta seleção não está disponível quando o <b>Protocolo</b> está definido como <b>ICMP</b> ou <b>Qualquer</b> .
Tipo de ICMP	Quando você selecionar <b>ICMP</b> (um relatório de erros e um utilitário de diagnóstico usado entre dispositivos para comunicar informações de erro) para o <b>Protocolo</b> , selecione o <b>Tipo de ICMP</b> no menu suspenso. As mensagens de ICMP são identificadas pelo campo de tipo. Por padrão, o tipo de ICMP é definido como Qualquer.
IP/Intervalo Convertido	Digite o endereço IP ou um intervalo de endereços IP nos quais os endereços de destino nos pacotes de entrada serão convertidos. São endereços IP de uma ou mais máquinas virtuais para as quais você está configurando o DNAT de modo que eles possam receber o tráfego da rede externa.
Porta Convertida	(Opcional) Selecione a porta ou o intervalo de portas ao qual o tráfego de entrada está se conectando nas máquinas virtuais da rede interna. Essas portas são aquelas nas quais a regra de DNAT está convertendo os pacotes de entrada para as máquinas virtuais.

Opção	Descrição
Endereço IP de origem	Se quiser que a regra se aplique apenas ao tráfego de um domínio específico, insira um endereço IP para esse domínio ou um intervalo de endereços IP no formato CIDR. Se você deixar esta caixa de texto em branco, a regra de DNAT se aplicará a todos os endereços IP que estiverem na sub-rede local.
Porta de Origem	(Opcional) Insira um número de porta para a origem.
Descrição	(Opcional) Insira uma descrição significativa para a regra de DNAT.
Ativado	Ative esta opção para ativar esta regra.
Ativar log	Ative esta opção para que a conversão de endereços realizada por essa regra seja registrada.

##### 5 Configure uma regra de NAT de origem (na saída externa).

Opção	Descrição
Aplicado em	Selecione a interface na qual aplicar a regra.
IP/Intervalo de Origem Original	Digite o endereço IP original ou o intervalo de endereços IP a ser aplicado a essa regra ou selecione o endereço IP alocado na lista. São endereços IP de uma ou mais máquinas virtuais para as quais você está configurando a regra de SNAT, de modo que eles possam enviar o tráfego para a rede externa.
IP/Intervalo de Origem Convertido	Digite o endereço IP necessário. Esse endereço deve ser sempre o endereço IP público do edge gateway para o qual você está configurando a regra de SNAT. Especifica o endereço IP no qual os endereços de origem (as máquinas virtuais) em pacotes de saída são convertidos quando enviam o tráfego para a rede externa.
Endereço IP de Destino	(Opcional) Se você deseja que a regra se aplique apenas ao tráfego para um domínio específico, insira um endereço IP para esse domínio ou um intervalo de endereços IP no formato CIDR. Se você deixar esta caixa de texto em branco, a regra SNAT se aplicará a todos os destinos fora da sub-rede local.
Porta de Destino	(Opcional) Insira um número de porta para o destino.
Descrição	(Opcional) Insira uma descrição significativa para a regra de SNAT.
Ativado	Ative esta opção para ativar esta regra.
Ativar log	Ative esta opção para que a conversão de endereços realizada por essa regra seja registrada.

##### 6 Clique em **Manter** para adicionar a regra à tabela na tela.

##### 7 Repita as etapas para configurar regras adicionais.

##### 8 Clique em **Salvar alterações** para salvar as regras no sistema.

##### Próximo passo

Adicione as regras de firewall do edge gateway correspondentes para as regras de SNAT ou de DNAT que você acabou de configurar. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

## Configuração de roteamento avançada para Edges Gateways do NSX Data Center for vSphere

Você pode configurar o roteamento estático e dinâmico nos seus edge gateways do NSX Data Center for vSphere.

Para habilitar o roteamento dinâmico, você configura um edge gateway avançado usando o Protocolo de edge gateway (BGP) ou o protocolo Open Shortest Path First (OSPF).

Para obter informações detalhadas sobre os recursos de roteamento que o NSX Data Center for vSphere fornece, consulte a documentação do NSX Data Center for vSphere.

Você pode especificar o roteamento estático e dinâmico para cada edge gateway avançado. O recurso de roteamento dinâmico fornece as informações de encaminhamento necessárias entre domínios de transmissão de camada 2, o que permite reduzir domínios de transmissão de camada 2 e melhorar a eficiência e dimensionamento da rede. O NSX Data Center for vSphere estende essa inteligência aos locais das cargas de trabalho para o roteamento leste-oeste. Esse recurso permite comunicação mais direta de máquina virtual com máquina virtual, sem o custo ou o tempo adicional necessário para estender os saltos.

### Especificar configurações de roteamento padrão para o edge gateway do NSX Data Center for vSphere

Você pode especificar as configurações padrão para roteamento estático e roteamento dinâmico de um edge gateway.

---

**Observação** Para remover todas as configurações de roteamento definidas, use o botão **LIMPAR CONFIGURAÇÃO GLOBAL** na parte inferior da tela **Configuração de Roteamento**. Essa ação exclui todas as configurações de roteamento especificadas atualmente nas subtelas: configurações de roteamento padrão, rotas estáticas, OSPF, BGP e redistribuição de rotas.

---

#### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Roteamento > Configuração de Roteamento**.
- 3 Para habilitar o roteamento de Vários Caminhos de Custo Igual (ECMP) para esse edge gateway, ative o botão de alternância **ECMP**.

Conforme descrito na documentação de *Administração do NSX*, o ECMP é uma estratégia de roteamento que permite que o encaminhamento de pacotes de próximo salto para um único destino ocorra em vários caminhos melhores. O NSX determina esses melhores caminhos estaticamente, usando rotas estáticas configuradas ou como resultado de cálculos de métricas por protocolos de roteamento dinâmico, como o OSPF ou o BGP. Você pode especificar os vários caminhos para rotas estáticas definindo vários próximos saltos na tela Rotas Estáticas.

Para obter mais detalhes sobre o ECMP e o NSX, consulte os tópicos de roteamento no *Guia de Solução de Problemas do NSX*.

- 4 Especifique as configurações para o gateway de roteamento padrão.
  - a Use a lista suspensa **Aplicado em** para selecionar uma interface da qual o próximo salto até a rede de destino pode ser alcançado.  
 Para ver os detalhes sobre a interface selecionada, clique no ícone de informações azul.
  - b Digite o endereço IP do gateway.
  - c Digite a MTU.
  - d (Opcional) Digite uma descrição opcional.
  - e Clique em **Salvar alterações**.
- 5 Especifique as configurações padrão de roteamento dinâmico.

---

**Observação** Se você tem a VPN IPsec configurada no seu ambiente, não deve usar o roteamento dinâmico.

---

- a Selecione um ID de roteador.  
 Você pode selecionar um ID de roteador na lista ou usar o ícone + para inserir um novo. Esse ID de roteador é o primeiro endereço IP de uplink do edge gateway que envia rotas ao kernel para roteamento dinâmico.
  - b Configure o registro em log ativando o botão de alternância **Ativar Log** e selecionando o nível de log.
  - c Clique em **OK**.
- 6 Clique em **Salvar alterações**.

#### Próximo passo

Adicione rotas estáticas. Consulte [Adicionar uma rota estática](#).

Configure a redistribuição de rotas. Consulte [Configurar redistribuições de rota](#).

Configure o roteamento dinâmico. Consulte os seguintes tópicos:

- [Configurar o BGP](#)
- [Configurar o OSPF](#)

## Adicionar uma rota estática


Você pode adicionar uma rota estática para uma sub-rede ou host de destino.

Se o ECMP estiver habilitado na configuração de roteamento padrão, você poderá especificar vários saltos seguintes nas rotas estáticas. Consulte [Especificar configurações de roteamento padrão para o edge gateway do NSX Data Center for vSphere](#) para ver as etapas para habilitar o ECMP.

## Pré-requisitos

Conforme descrito na documentação do NSX, o endereço IP do próximo salto da rota estática deve existir em uma sub-rede associada a uma das interfaces de edge gateway do NSX Data Center for vSphere. Caso contrário, a configuração dessa rota estática falhará.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Roteamento > Rotas Estáticas**.
- 3 Clique no botão **Criar** ().
- 4 Configure as seguintes opções para a rota estática:

Opção	Descrição
Rede	Digite a rede na notação CIDR.
Próximo Salto	Digite o endereço IP do próximo salto. O endereço IP do próximo salto deve existir em uma sub-rede associada a uma das interfaces do edge gateway. Se o ECMP estiver habilitado, você poderá digitar vários saltos seguintes.
MTU	Edite o valor máximo de transmissão para pacotes de dados. O valor de MTU não pode ser maior do que o valor de MTU definido na interface do edge gateway selecionada. Você pode ver o MTU definido na interface do edge gateway por padrão na tela Configuração de Roteamento.
Interface	Opcionalmente, selecione a interface do edge gateway na qual você deseja adicionar uma rota estática. Por padrão, a interface é selecionada e corresponde ao endereço do próximo salto.
Descrição	Opcionalmente, digite uma descrição para a rota estática.

- 5 Clique em **Salvar alterações**.

## Próximo passo

Configure uma regra de NAT para a rota estática. Consulte [Adicionar uma regra de SNAT ou de DNAT](#).

Adicione uma regra de firewall para permitir que o tráfego atravesse a rota estática. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

## Configurar o OSPF

Você pode configurar o protocolo de roteamento Open Shortest Path First (OSPF) para os recursos de roteamento dinâmico de um edge gateway do NSX Data Center for vSphere. Um aplicativo comum do OSPF em um edge gateway em um ambiente do VMware Cloud Director é trocar informações de roteamento entre os edge gateways no VMware Cloud Director.



O gateway do NSX Edge oferece suporte para OSPF, um protocolo de gateway interior que roteia pacotes IP somente dentro de um único domínio de roteamento. Conforme descrito na documentação de *Administração do NSX*, a configuração do OSPF em um edge gateway do NSX permite que o edge gateway aprenda e anuncie rotas. O edge gateway usa OSPF para reunir informações de estado de link de edge gateways disponíveis e construir um mapa de topologia da rede. A topologia determina a tabela de roteamento apresentada à camada da Internet, que toma decisões de roteamento com base no endereço IP de destino encontrado em pacotes IP.

Como resultado, as políticas de roteamento OSPF fornecem um processo dinâmico de balanceamento de carga de tráfego entre rotas de custo igual. Uma rede OSPF é dividida em áreas de roteamento para otimizar o fluxo de tráfego e limitar o tamanho das tabelas de roteamento. Uma área é um conjunto lógico de redes OSPF, roteadores e links que têm a mesma identificação de área. As áreas são identificadas por um ID de área.

### Pré-requisitos


Deve ser configurado um ID de roteador. [Especificar configurações de roteamento padrão para o edge gateway do NSX Data Center for vSphere.](#)

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Roteamento > OSPF**.
- 3 Se o OSPF não estiver habilitado no momento, use a opção **OSPF Ativado** para habilitá-lo.
- 4 Defina as configurações de OSPF de acordo com as necessidades da sua organização.


Opção	Descrição
<b>Ativar Reinicialização Normal</b>	Especifica que o encaminhamento de pacotes deve permanecer sem interrupção quando os serviços OSPF forem reiniciados.
<b>Ativar Origem Padrão</b>	Permite que o edge gateway se anuncie como um gateway padrão aos peers de OSPF.

- 5 (Opcional) Você pode clicar em **Salvar alterações** ou continuar com a configuração de definições de área e mapeamentos de interface.

- 6 Adicione uma definição de área de OSPF clicando no botão **Adicionar** () (botão adicionar), especificando os detalhes para o mapeamento na caixa de diálogo e clicando em **Manter**.

**Observação** Por padrão, o sistema configura uma Área de não muito stub (NSSA) com o ID de área de 51, e essa área é exibida automaticamente na tabela de definições de área na tela do OSPF. Você pode modificar ou excluir a área NSSA.

Opção	Descrição
ID da Área	Digite uma ID de área na forma de um endereço IP ou número decimal.
Tipo de Área	<p>Selecione <b>Normal</b> ou <b>NSSA</b>.</p> <p>As NSSAs impedem a inundação de anúncios de estado de link externos (LSAs) nas NSSAs. Eles dependem do roteamento padrão para destinos externos. Como resultado, as NSSAs devem ser colocadas no edge de um domínio de roteamento OSPF. A NSSA pode importar rotas externas para o domínio de roteamento OSPF, assim, fornecendo serviço de tráfego para domínios de roteamento pequenos que não fazem parte do domínio de roteamento OSPF.</p>
Autenticação de Área	<p>Selecione o tipo de autenticação para OSPF a ser executada no nível de área. Todos os edge gateways na área devem ter a mesma autenticação e a respectiva senha configuradas. Para que a autenticação MD5 funcione, tanto o receptor quanto o transmissor devem ter a mesma chave MD5.</p> <p>As opções são:</p> <ul style="list-style-type: none"> <li>■ <b>Nenhuma</b> <p>Nenhuma autenticação é necessária.</p> </li> <li>■ <b>Senha</b> <p>Com essa opção, a senha especificada no campo <b>Valor de autenticação de área</b> é incluída no pacote transmitido.</p> </li> <li>■ <b>MD5</b> <p>Com essa opção, a autenticação usa a criptografia MD5 (resumo da mensagem tipo 5). Uma soma de verificação MD5 está incluída no pacote transmitido. Digite a chave MD5 no campo <b>Valor de autenticação de área</b>.</p> </li> </ul>

- 7 Clique em **Salvar alterações**, para que as definições de área recentemente configuradas estejam disponíveis para seleção quando você adicionar mapeamentos de interface.
- 8 Adicione um mapeamento de interface clicando no botão **Adicionar** () (botão adicionar), especificando os detalhes para o mapeamento na caixa de diálogo e clicando em **Manter**.
- Esses mapeamentos mapeiam as interfaces do edge gateway para as áreas.
- a Na caixa de diálogo, selecione a interface que você deseja mapear para uma definição de área.
 

A interface especifica a rede externa à qual os dois edge gateways estão conectados.
  - b Selecione a ID da área a ser mapeada para a interface selecionada.

- c (Opcional) Altere as configurações de OSPF dos valores padrão para personalizá-las para este mapeamento de interface.

Ao configurar um novo mapeamento, são exibidos os valores padrão para essas configurações. Na maioria dos casos, recomenda-se manter as configurações padrão. Se você alterar as configurações, certifique-se de que os peers do OSPF usem as mesmas configurações.

Opção	Descrição
<b>Intervalo de Saudação</b>	Intervalo (em segundos) entre os pacotes de saudação enviados na interface.
<b>Intervalo de Encerramento</b>	Intervalo (em segundos) durante o qual pelo menos um pacote de saudação deve ser recebido de um vizinho antes que o vizinho seja declarado inoperante.
<b>Prioridade</b>	Prioridade da interface. A interface com a prioridade mais alta é o roteador de edge gateway designado.
<b>Custo</b>	Sobrecarga necessária para enviar pacotes por essa interface. O custo de uma interface é inversamente proporcional à largura de banda dessa interface. Quanto maior for a largura de banda, menor será o custo.

- d Clique em **Manter**.

## 9 Clique em **Salvar alterações** na tela do OSPF.

### Próximo passo

Configure o OSPF nos outros edge gateways com os quais você deseja trocar informações de roteamento.

Adicione uma regra de firewall que permita o tráfego entre os edge gateways habilitados para OSPF. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

Verifique se a redistribuição de rota e a configuração de firewall permitem que as rotas corretas sejam anunciadas. Consulte [Configurar redistribuições de rota](#).

## Configurar o BGP


Você pode configurar o Border Gateway Protocol (BGP) para os recursos de roteamento dinâmico de um edge gateway do NSX Data Center for vSphere.

Conforme descrito no *NSX Guia de administração*, o BGP toma as decisões principais de roteamento usando uma tabela de redes IP ou prefixos, que designam a alcançabilidade de rede entre vários sistemas autônomos. No campo rede, o termo "BGP speaker" se refere a um dispositivo de rede que está executando o BGP. Dois "BGP speakers" estabelecem uma conexão antes que qualquer informação de roteamento seja trocada. O termo vizinho BGP refere-se a um "BGP speaker" que estabeleceu essa conexão. Depois de estabelecer a conexão, os dispositivos trocam rotas e sincronizam suas tabelas. Cada dispositivo envia mensagens de "keep alive" para manter esta relação em funcionamento.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Roteamento > BGP**.
- 3 Se o BGP não estiver habilitado no momento, use a opção **Habilitar BGP** para habilitá-lo.
- 4 Defina as configurações de BGP de acordo com as necessidades da sua organização.

Opção	Descrição
<b>Ativar Reinicialização Normal</b>	Especifica que o encaminhamento de pacotes deve permanecer sem interrupção quando os serviços BGP forem reiniciados.
<b>Ativar Origem Padrão</b>	Permite que o edge gateway se anuncie como um gateway padrão para seus vizinhos BGP.
<b>AS Local</b>	Obrigatório. Especifique o número de ID do sistema autônomo (AS) a ser usado para o recurso do sistema autônomo local do protocolo. O valor especificado deve ser um número globalmente exclusivo entre 1 e 65534. O sistema autônomo local é um recurso do BGP. O sistema atribui o número do sistema autônomo local ao edge gateway que você está configurando. O edge gateway anuncia essa ID quando o edge gateway faz o peer com seus vizinhos BGP em outros sistemas autônomos. O caminho dos sistemas autônomos que uma rota percorreria é usado como uma métrica no algoritmo de roteamento dinâmico ao selecionar o melhor caminho para um destino.

- 5 Você pode clicar em **Salvar as alterações** ou continuar a definir as configurações dos vizinhos de roteamento BGP.
- 6 Adicione uma configuração de vizinho BGP clicando no botão **Adicionar** () , especificando os detalhes para o vizinho na caixa de diálogo e clicando em **Manter**.

Opção	Descrição
<b>Endereço IP</b>	Digite o endereço IP de um vizinho BGP para este edge gateway.
<b>AS Remoto</b>	Digite um número exclusivo global entre 1 e 65534 para o sistema autônomo ao qual esse vizinho BGP pertence. Esse número de sistema autônomo remoto é usado na entrada do vizinho BGP na tabela de vizinhos BGP do sistema.
<b>Peso</b>	O peso padrão para a conexão vizinha. Ajuste conforme apropriado para as necessidades da sua organização.
<b>Tempo de Keep Alive</b>	A frequência na qual o software envia mensagens de "keep alive" para seu peer. A frequência padrão é de 60 segundos. Ajuste conforme apropriado para as necessidades da sua organização.

Opção	Descrição
<b>Tempo de Pressionamento</b>	<p>O intervalo para o qual o software declara um peer inoperante após não receber uma mensagem de "keep alive". Esse intervalo deve ser três vezes o intervalo de "keep alive". O intervalo padrão é de 180 segundos. Ajuste conforme apropriado para as necessidades da sua organização.</p> <p>Quando o peer entre dois vizinhos BGP for estabelecido, o edge gateway iniciará um timer de desativação. Toda mensagem de "keep alive" recebida do vizinho redefine o timer de desativação como 0. Se o edge gateway falhar ao receber três mensagens de "keep alive" consecutivas, para que o timer de desativação atinja três vezes o intervalo de "keep alive", o edge gateway considerará o vizinho inoperante e excluirá as rotas desse vizinho.</p>
<b>Senha</b>	<p>Se esse vizinho BGP exigir autenticação, digite a senha de autenticação.</p> <p>Cada segmento enviado na conexão entre os vizinhos é verificado. A autenticação MD5 deve ser configurada com a mesma senha nos dois vizinhos de BGP. Caso contrário, a conexão entre eles não será estabelecida.</p>
<b>Filtros BGP</b>	<p>Use esta tabela para especificar a filtragem de rota usando uma lista de prefixos desse vizinho BGP.</p> <hr/> <p><b>Cuidado</b> Uma regra de bloquear todos é aplicada no final dos filtros.</p> <hr/> <p>Adicione um filtro à tabela clicando no ícone + e configurando as opções. Clique em <b>Manter</b> para salvar cada filtro.</p> <ul style="list-style-type: none"> <li>■ Selecione a direção para indicar se você está filtrando o tráfego de ou para o vizinho.</li> <li>■ Selecione a ação para indicar se você está permitindo ou negando o tráfego.</li> <li>■ Digite a rede que você deseja filtrar para ou a partir do vizinho. Digite <code>ANY</code> ou uma rede em um formato CIDR.</li> <li>■ Digite o <b>GE de Prefixo do IP</b> e o <b>LE de Prefixo do IP</b> para usar as palavras-chave <code>le</code> e <code>ge</code> na lista de prefixos de IP.</li> </ul>

7 Clique em **Salvar alterações** para salvar as configurações no sistema.

#### Próximo passo

Configure o BGP nos outros edge gateways com os quais você deseja trocar informações de roteamento.


Adicione uma regra de firewall que permita o tráfego de e para os edge gateways configurados por BGP. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#) para obter informações.


## Configurar redistribuições de rota

Por padrão, o roteador só compartilha rotas com outros roteadores que executam o mesmo protocolo. Quando você tiver configurado um ambiente de vários protocolos, deverá configurar a redistribuição de rota para ter o compartilhamento de rota entre protocolos. Você pode configurar a redistribuição de rota para um edge gateway do NSX Data Center for vSphere.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Roteamento > Redistribuição de Rota**.
- 3 Use os botões de alternância de protocolo para ativar os protocolos para os quais você deseja habilitar a redistribuição de rota.
- 4 Adicione prefixos de IP à tabela na tela.

- a Clique no botão **Adicionar** ()
- b Digite um nome e o endereço IP da rede no formato CIDR.
- c Clique em **Manter**.

- 5 Especifique critérios de redistribuição para cada prefixo de IP clicando no botão **Adicionar** () , especificando os critérios na caixa de diálogo e clicando em **Manter**.

As entradas na tabela são processadas sequencialmente. Use as setas para cima e para baixo para ajustar a sequência.

Opção	Descrição
<b>Nome do Prefixo</b>	Selecione um prefixo de IP específico ao qual aplicar esses critérios ou selecione <b>Qualquer</b> para aplicar os critérios a todas as rotas de rede.
<b>Protocolo do Aluno</b>	Selecione o protocolo que deve aprender rotas de outros protocolos sob esses critérios de redistribuição.
<b>Permitir aprendido de</b>	Selecione os tipos de rede dos quais rotas podem ser aprendidas para o protocolo selecionado na lista <b>Protocolo do Aluno</b> .
<b>Ação</b>	Selecione se deseja permitir ou negar a redistribuição dos tipos de redes selecionados.

- 6 Clique em **Salvar alterações**.

## Balanceamento de carga com o NSX Data Center for vSphere

O balanceador de carga distribui solicitações de serviço de entrada entre vários servidores de forma que a distribuição de carga seja transparente para os usuários. O balanceamento de carga fornece alta disponibilidade de aplicativos e ajuda a obter a melhor utilização dos recursos, maximizando a taxa de transferência, minimizando o tempo de resposta e evitando a sobrecarga.

### Sobre o balanceamento de carga

O balanceador de carga distribui solicitações de serviço de entrada entre vários servidores de forma que a distribuição de carga seja transparente para os usuários. O balanceamento de carga

ajuda a obter o melhor uso dos recursos, maximizando a taxa de transferência, minimizando o tempo de resposta e evitando a sobrecarga.

O balanceador de carga do NSX oferece suporte a dois mecanismos de balanceamento de carga. O balanceador de carga de camada 4 é baseado em pacote e fornece processamento rápido de caminhos. O balanceador de carga de camada 7 é baseado em soquete e oferece suporte para estratégias avançadas de gerenciamento de tráfego e mitigação de DDOS para serviços de back-end.

O balanceamento de carga para um edge gateway do NSX Data Center for vSphere é configurado na interface externa porque esse edge gateway equilibra a carga do tráfego de entrada proveniente da rede externa. Ao configurar servidores virtuais para balanceamento de carga, especifique um dos endereços IP disponíveis no VDC da organização.

### **Estratégias e conceitos de balanceamento de carga**

Uma estratégia de balanceamento de carga baseada em pacote é implementada na camada TCP e UDP. O balanceamento de carga baseado em pacote não interrompe a conexão nem armazena em buffer a solicitação inteira. Em vez disso, depois de manipular o pacote, ele o envia diretamente ao servidor selecionado. As sessões TCP e UDP são mantidas no balanceador de carga, para que os pacotes de uma única sessão sejam direcionados para o mesmo servidor. Você pode selecionar a opção Aceleração Habilitada tanto na configuração global quanto na configuração de servidor virtual relevante para habilitar o balanceamento de carga baseado em pacote.

Uma estratégia de balanceamento de carga baseada em soquete é implementada sobre a interface do soquete. Duas conexões são estabelecidas para uma única solicitação: uma voltada para o cliente e outra voltada para o servidor. A conexão voltada para o servidor é estabelecida após a seleção do servidor. Para a implantação baseada em soquete HTTP, a solicitação inteira é recebida antes do envio ao servidor selecionado com a manipulação L7 opcional. Para uma implementação baseada em soquetes HTTPS, as informações de autenticação são trocadas na conexão voltada para o cliente ou na conexão voltada para o servidor. O balanceamento de carga baseado em soquete é o modo padrão para servidores virtuais TCP, HTTP e HTTPS.

Os principais conceitos do balanceador de carga do NSX são o servidor virtual, o pool de servidores, o membro do pool de servidores e o monitor de serviços.

#### **Servidor virtual**

Resumo de um serviço de aplicativo, representado por uma combinação exclusiva de IP, porta, protocolo e perfil de aplicativo, como TCP ou UDP.

#### **Pool de servidores**

Grupo de servidores back-end.

#### **Membro do pool de servidores**

Representa o servidor back-end como membro em um pool.

#### **Monitor de serviços**

Define como testar o status de integridade de um servidor back-end.

## Perfil de Aplicativo

Representa a configuração de TCP, UDP, persistência e certificado para um determinado aplicativo.

## Visão geral da configuração

Comece definindo opções globais para o balanceador de carga. Em seguida, crie um pool de servidores que consista em membros do servidor back-end e associe um monitor de serviços a esse pool para gerenciar e compartilhar os servidores back-end de forma eficiente.

Em seguida, crie um perfil de aplicativo para definir o comportamento do aplicativo comum em um balanceador de carga, como SSL do cliente, SSL do servidor, x-forwarded-for ou persistência. Persistência envia solicitações subsequentes com características semelhantes, como IP ou o cookie de origem, que devem ser distribuídas para o mesmo membro do pool, sem executar o algoritmo de balanceamento de carga. O perfil do aplicativo pode ser reutilizado em servidores virtuais.

Em seguida, crie uma regra de aplicativo opcional para definir as configurações específicas do aplicativo para manipulação de tráfego, como corresponder uma determinada URL ou um nome de host, para que solicitações diferentes possam ser manipuladas por pools diferentes. Em seguida, você cria um monitor de serviços específico para o seu aplicativo ou pode usar um monitor de serviços existente se ele atender às suas necessidades.

Opcionalmente, você pode criar uma regra de aplicativo para oferecer suporte à funcionalidade avançada de servidores virtuais L7. Alguns casos de uso para regras de aplicativo incluem comutação de conteúdo, manipulação de cabeçalho, regras de segurança e proteção DOS.

Por último, crie um servidor virtual que conecte seu pool de servidores, o perfil de aplicativo e qualquer regra de aplicativo potencial.

Quando o servidor virtual recebe uma solicitação, o algoritmo de balanceamento de carga considera a configuração do membro do pool e o status do tempo de execução. Em seguida, o algoritmo calcula o pool apropriado para distribuir o tráfego que inclui um ou mais membros. A configuração de membros do pool inclui definições como peso, conexão máxima e status da condição. O status de tempo de execução inclui as informações atuais de status de resposta, tempo de resposta e status da verificação de integridade. Os métodos de cálculo podem ser round-robin, round-robin ponderado, menor conexão, hash de IP de origem, menores conexões ponderadas, URL, URI ou cabeçalho HTTP.

Cada pool é monitorado pelo monitor de serviços associado. Quando o balanceador de carga detecta um problema com um membro do pool, ele é marcado como DOWN. Somente o servidor no estado UP é selecionado ao escolher um membro do pool de servidores. Se o pool de servidores não estiver configurado com um monitor de serviços, todos os membros do pool serão considerados UP.



## Configurar o serviço de balanceador de carga

Os parâmetros globais de configuração do balanceador de carga incluem habilitação geral, a seleção do mecanismo de camada 4 ou camada 7 e a especificação dos tipos de eventos para registrar.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Balanceador de Carga > Configuração Global**.
- 3 Selecione as opções que você deseja habilitar:

Opção	Ação
Status	<p>Habilite o balanceador de carga clicando no ícone de botão de alternância.</p> <p>Ative <b>Aceleração Habilitada</b> para configurar o balanceador de carga para usar o mecanismo L4 mais rápido em vez do mecanismo L7. O VIP TCP L4 é processado antes do firewall do edge gateway e, portanto, nenhuma regra de firewall para permissão é necessária.</p> <hr/> <p><b>Observação</b> Os VIPs L7 para HTTP e HTTPS são processados após o firewall e, portanto, quando você não habilita a aceleração, deve existir uma regra de firewall de edge gateway para permitir o acesso ao VIP L7 para esses protocolos. Quando você habilita a aceleração, e o pool de servidores está em um modo não transparente, uma regra de SNAT é adicionada e, portanto, é necessário garantir que o firewall esteja habilitado no edge gateway.</p>
Ativar Log	Habilite o registro em log para que o balanceador de carga do edge gateway colete logs de tráfego.
Nível de Log	Escolha a gravidade dos eventos a serem coletados nos logs.

- 4 Clique em **Salvar alterações**.

### Próximo passo

Configure perfis de aplicativo para o balanceador de carga. Consulte [Criar um perfil de aplicativo](#).


### Criar um perfil de aplicativo

Um perfil de aplicativo define o comportamento do balanceador de carga para um determinado tipo de tráfego de rede. Depois de configurar um perfil, associe-o a um servidor virtual. Em seguida, o servidor virtual processará o tráfego de acordo com os valores especificados no perfil. O uso de perfis aumenta seu controle sobre o gerenciamento do tráfego de rede e torna as tarefas de gerenciamento de tráfego mais fáceis e eficientes.

Quando você cria um perfil para o tráfego HTTPS, os seguintes padrões de tráfego HTTPS são permitidos:

- Cliente -> HTTPS-> LB (encerrar SSL)-> HTTP -> servidores
- Cliente -> HTTPS-> LB (encerrar SSL)-> HTTPS -> servidores
- Cliente -> HTTPS -> LB (SSL passagem)-> -> HTTPS -> servidores
- Cliente -> HTTP-> LB -> HTTP -> servidores

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Balancedor de Carga > Perfis de Aplicativo**.
- 3 Clique no botão **Criar** ().
- 4 Insira um nome para o perfil.
- 5 Configure o perfil do aplicativo.

Opção	Descrição
<b>Tipo</b>	Selecione o tipo de protocolo usado para enviar solicitações ao servidor. A lista de parâmetros necessários depende do protocolo selecionado. Não é possível inserir os parâmetros que não são aplicáveis ao protocolo selecionado. Todos os outros parâmetros são obrigatórios.
<b>Permitir Passagem SSL</b>	Clique para habilitar que a autenticação SSL seja transmitida ao servidor virtual. Caso contrário, a autenticação SSL ocorrerá no endereço de destino.
<b>URL de Redirecionamento HTTP</b>	(HTTP e HTTPS) Insira a URL para o qual o tráfego que chega no endereço de destino deve ser redirecionado.

Opção	Descrição
Persistência	<p>Especifique um mecanismo de persistência para o perfil.</p> <p>A persistência rastreia e armazena dados da sessão, como o membro do pool específico que atendeu a uma solicitação de cliente. Isso garante que as solicitações do cliente sejam direcionadas ao mesmo membro do pool durante toda a vida útil de uma sessão ou durante as sessões subsequentes. As opções são:</p> <ul style="list-style-type: none"> <li>■ <b>IP de Origem</b> <p>A persistência de IP de origem rastreia sessões com base no endereço IP de origem. Quando um cliente solicita uma conexão com um servidor virtual que oferece suporte à persistência de afinidade de endereço de origem, o balanceador de carga verifica se esse cliente já estava anteriormente conectado e, em caso positivo, o retorna ao mesmo membro do pool.</p> </li> <li>■ <b>MSRDP</b> <p>(Somente TCP) A persistência do protocolo MSRDP mantém sessões persistentes entre clientes Windows e servidores que estão executando o serviço de protocolo RDP da Microsoft. O cenário recomendado para ativar a persistência do MSRDP é criar um pool de balanceamento de carga composto por membros que executam o SO convidado Windows Server no qual todos os membros pertencem a um cluster do Windows e participam de um diretório de sessão do Windows.</p> </li> <li>■ <b>ID da Sessão SSL</b> <p>A persistência do ID da Sessão SSL está disponível quando você ativa a passagem SSL. A persistência do ID da Sessão SSL garante que as conexões repetidas do mesmo cliente sejam enviadas ao mesmo servidor. A persistência do ID da Sessão permite o uso da retomada de sessão SSL, o que poupa tempo de processamento para o cliente e o servidor.</p> </li> </ul>
Nome do Cookie	<p>(HTTP e HTTPS) Se você especificou <b>Cookie</b> como o mecanismo de persistência, insira o nome do cookie. A persistência do cookie usa um cookie para identificar de forma exclusiva a sessão na primeira vez que um cliente acessa o site. O balanceador de carga se refere a esse cookie ao conectar solicitações subsequentes na sessão, para que todas sejam direcionadas ao mesmo servidor virtual.</p>

Opção	Descrição
Modo	<p>Selecione o modo pelo qual o cookie deve ser inserido. Os seguintes modos são compatíveis:</p> <ul style="list-style-type: none"> <li>■ <b>Inserir</b> <p>O edge gateway envia um cookie. Quando o servidor enviar um ou mais cookies, o cliente receberá um cookie extra (os cookies do servidor mais o cookie do edge gateway). Quando o servidor não enviar um cookie, o cliente receberá apenas o cookie do edge gateway.</p> </li> <li>■ <b>Prefixo</b> <p>Selecione essa opção quando o cliente não oferecer suporte a mais de um cookie.</p> <p><b>Observação</b> Todos os navegadores aceitam vários cookies. Porém, você pode ter um aplicativo patenteado usando um cliente proprietário com suporte apenas para um cookie. O servidor Web envia seu cookie como de costume. O edge gateway injeta (como um prefixo) suas informações de cookie no valor do cookie do servidor. Essas informações adicionadas por cookies são removidas quando o edge gateway as envia ao servidor.</p> </li> <li>■ <b>Sessão do Aplicativo</b> Para essa opção, o servidor não envia um cookie. Em vez disso, ele envia as informações da sessão do usuário como uma URL. Por exemplo, <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, em que <code>JSESSIONID</code> são as informações da sessão do usuário usadas para a persistência. Não é possível ver a tabela de persistência da sessão do aplicativo para solução de problemas.</li> </ul>
Expira em (segundos)	<p>Insira um período de tempo em segundos durante o qual a persistência permanecerá em vigor. Deve ser um número inteiro positivo no intervalo de 1-86400.</p> <p><b>Observação</b> Para o balanceamento de carga L7 usando a persistência de IP de origem TCP, a entrada de persistência expirará se nenhuma nova conexão TCP for feita por um período de tempo, mesmo se as conexões existentes ainda estiverem ativas.</p>
Inserir cabeçalho HTTP X-Forwarded-For	<p>(HTTP e HTTPS) Selecione o cabeçalho <b>Insert X-Forwarded-For HTTP</b> para identificar o endereço IP de origem de um cliente que se conecta a um servidor Web por meio do balanceador de carga.</p> <p><b>Observação</b> O uso desse cabeçalho não terá suporte se você tiver ativado a passagem SSL.</p>
Ativar SSL no Lado do Pool	<p>(Somente HTTPS) Selecione <b>Ativar SSL no Lado do Pool</b> para definir o certificado, as CAs ou as CRLs usados para autenticar o balanceador de carga no lado do servidor na guia Certificados do Pool.</p>

- 6 (Somente HTTPS) Configure os certificados a serem usados com o perfil do aplicativo. Se os certificados necessários não existirem, você poderá criá-los na guia **Certificados**.

Opção	Descrição
<b>Certificados de Servidor Virtual</b>	Selecione o certificado, as CAs ou as CRLs usadas para descriptografar o tráfego HTTPS.
<b>Certificados de Pool</b>	Defina o certificado, as CAs ou as CRLs usadas para autenticar o balanceador de carga no lado do servidor.  <b>Observação</b> Selecione <b>Habilitar SSL no Lado do Pool</b> para ativar essa guia.
<b>Codificação</b>	Selecione os algoritmos de codificação (ou o pacote de codificação) negociados durante o handshake SSL/TLS.
<b>Autenticação de Cliente</b>	Especifique se a autenticação do cliente deve ser ignorada ou se é necessária.  <b>Observação</b> Quando definido como <b>Obrigatório</b> , o cliente deve fornecer um certificado após a solicitação ou o handshake ser cancelado.

- 7 Para preservar as alterações, clique em **Manter**.


#### Próximo passo

Adicione monitores de serviço para o balanceador de carga para definir verificações de integridade para diferentes tipos de tráfego de rede. Consulte [Criar um monitor de serviço](#).

#### Criar um monitor de serviço

Você cria um monitor de serviço para definir parâmetros de verificação de integridade para um determinado tipo de tráfego de rede. Quando você associa um monitor de serviço a um pool, os membros desse pool são monitorados de acordo com os parâmetros do monitor de serviços.

#### Procedimentos

- Abra Serviços de Edge Gateway.
  - Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- Navegue até **Balanceador de Carga > Monitoramento de Serviços**.
- Clique no botão **Criar** ().
- Insira um nome para o monitor de serviços.

## 5 (Opcional) Configure as seguintes opções para o monitor de serviços:

Opção	Descrição
Intervalo	Digite o intervalo no qual um servidor deve ser monitorado usando o <b>Método</b> especificado.
Tempo Limite	Digite o tempo máximo em segundos no qual uma resposta do servidor deve ser recebida.
Máx. de Novas Tentativas	Digite o número de vezes que o <b>Método</b> de monitoramento especificado deve falhar sequencialmente antes de o servidor ser declarado como inoperante.
Tipo	Selecione de que forma você deseja enviar a solicitação de verificação de integridade ao servidor: HTTP, HTTPS, TCP, ICMP ou UDP. Dependendo do tipo selecionado, as opções restantes na caixa de diálogo <b>Novo Monitor de Serviço</b> serão ativadas ou desativadas.
Esperado	(HTTP e HTTPS) Digite a cadeia de caracteres que o monitor espera corresponder na linha de status da resposta HTTP ou HTTPS (por exemplo, HTTP/1.1).
Método	(HTTP e HTTPS) Selecione o método a ser usado para detectar o status do servidor.
URL	(HTTP e HTTPS) Digite a URL a ser usada na solicitação de status do servidor. <b>Observação</b> Ao selecionar o método POST, você deve especificar um valor para <b>Enviar</b> .
Enviar	(HTTP, HTTPS, UDP) Digite os dados a serem enviados.
Receber	(HTTP, HTTPS e UDP) Digite a cadeia de caracteres a ser correspondida no conteúdo da resposta. <b>Observação</b> Quando <b>Esperado</b> não corresponde, o monitor não tenta corresponder o conteúdo <b>Receber</b> .
Extensão	(TODOS) Digite parâmetros avançados de monitor como pares de chave=valor. Por exemplo, aviso=10 indica que, quando um servidor não responde dentro de 10 segundos, seu status é definido como aviso. Todos os itens de extensão devem ser separados por um caractere de retorno de carro. Por exemplo: <pre>&lt;extension&gt;delay=2 critical=3 escape&lt;/extension&gt;</pre>

## 6 Para preservar as alterações, clique em **Manter**.

**Exemplo: Extensões com suporte para cada protocolo****Tabela 5-4. Extensões para protocolos HTTP/HTTPS**

Extensão de monitor	Descrição
no-body	Não aguarda um corpo de documento e interrompe a leitura após o cabeçalho HTTP/HTTPS.  <b>Observação</b> Um HTTP GET ou HTTP POST ainda é enviado; não é um método HEAD.
max-age= <i>SEGUNDOS</i>	Avisa quando um documento tem mais de um número especificado de SEGUNDOS de idade. O número pode estar no formato 10m para minutos, 10h para horas ou 10d para dias.
content-type= <i>CADEIA</i>	Especifica um tipo de mídia de cabeçalho Content-Type em chamadas POST.
linespan	Permite que regex ocupe novas linhas (deve preceder -r ou -R).
regex= <i>CADEIA</i> ou ereg= <i>CADEIA</i>	Procura a regex CADEIA na página.
eregi= <i>CADEIA</i>	Procura a regex CADEIA sem distinção entre maiúsculas e minúsculas.
invert-regex	Retorna CRITICAL quando encontrado e OK quando não encontrado.
proxy-authorization= <i>AUTH_PAIR</i>	Especifica o nome de usuário:senha em servidores proxy com autenticação básica.
useragent= <i>CADEIA</i>	Envia a cadeia no cabeçalho HTTP como User Agent.
header= <i>CADEIA</i>	Envia quaisquer outras marcas no cabeçalho HTTP. Use várias vezes para cabeçalhos adicionais.
onredirect=ok warning critical follow sticky stickyport	Indica como lidar com páginas redirecionadas. <i>sticky</i> é como <i>follow</i> , mas fixo no endereço IP especificado. <i>stickyport</i> garante que a porta permaneça a mesma.
pagesize= <i>INTEIRO:INTEIRO</i>	Especifica os tamanhos de página mínimo e máximo necessários, em bytes.
warning=DUPLO	Especifica o tempo de resposta em segundos para gerar um status de aviso.
critical=DUPLO	Especifica o tempo de resposta em segundos para gerar um status crítico.

Tabela 5-5. Extensões somente para o protocolo HTTPS

Extensão de monitor	Descrição
sni	Habilita o suporte à extensão de nome de host SSL/TLS (SNI).
certificate=INTEIRO	Especifica o número mínimo de dias que um certificado deve ser válido. A porta padrão é 443. Quando essa opção é usada, a URL não é verificada.
authorization=AUTH_PAIR	Especifica o nome de usuário:senha em sites com autenticação básica.

Tabela 5-6. Extensões para o protocolo TCP

Extensão de monitor	Descrição
escape	Permite o uso de \n, \r, \t ou \ em uma cadeia send ou quit. Deve vir antes de uma opção send ou quit. Por padrão, nada é adicionado a send, e \r\n é adicionado ao final de quit.
all	Especifica que todas as cadeias esperadas precisam ocorrer em uma resposta do servidor. Por padrão, any é usado.
quit=CADEIA	Envia uma cadeia ao servidor para encerrar a conexão de forma limpa.
refuse=ok warn crit	Aceita recusas de TCP com estados ok, warn ou crit. Por padrão, usa o estado crit.
mismatch=ok warn crit	Aceita incompatibilidades de cadeias esperadas com estados ok, warn ou crit. Por padrão, usa o estado warn.
jail	Oculto a saída do soquete TCP.
maxbytes=INTEIRO	Encerra a conexão quando mais que o número especificado de bytes são recebidos.
delay=INTEIRO	Aguarda o número especificado de segundos entre o envio da cadeia e a sondagem por uma resposta.
certificate=INTEIRO[,INTEIRO]	Especifica o número mínimo de dias que um certificado deve ser válido. O primeiro valor é #days para aviso e o segundo valor é crítico (se não especificado - 0).
ssl	Usa SSL para a conexão.
warning=DUPLO	Especifica o tempo de resposta em segundos para gerar um status de aviso.
critical=DUPLO	Especifica o tempo de resposta em segundos para gerar um status crítico.

### Próximo passo


Adicione pools de servidores ao seu balanceador de carga. Consulte [Adicionar um pool de servidores para balanceamento de carga](#).



## Adicionar um pool de servidores para balanceamento de carga

Você pode adicionar um pool de servidores para gerenciar e compartilhar servidores back-end de forma flexível e eficiente. Um pool gerencia métodos de distribuição do balanceador de carga e tem um monitor de serviço anexado a ele para parâmetros de verificação de integridade.


### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **Balanceador de Carga > Pools**.
- 3 Clique no botão **Criar** ().
- 4 Digite um nome e, opcionalmente, uma descrição para o novo pool de balanceadores de carga.
- 5 Selecione um método de balanceamento para o serviço no menu suspenso **Algoritmo**:

Opção	Descrição
<b>ROUND-ROBIN</b>	Cada servidor é usado de cada vez, de acordo com o peso atribuído a ele. Esse é o algoritmo mais simples e mais justo quando o tempo de processamento do servidor permanece igualmente distribuído.
<b>IP-HASH</b>	Selecione um servidor com base em um hash do endereço IP de origem e de destino de cada pacote.
<b>LEASTCONN</b>	Distribui solicitações de clientes a vários servidores com base no número de conexões já abertas no servidor. Novas conexões são enviadas ao servidor com o menor número de conexões abertas.
<b>URI</b>	A parte esquerda do URI (antes do ponto de interrogação) recebe um hash e é dividida pelo peso total dos servidores em execução. O resultado designa qual servidor receberá a solicitação. Essa opção garante que um URI seja sempre direcionado ao mesmo servidor, desde que o servidor não fique desativado.

Opção	Descrição
HTTPHEADER	O nome do cabeçalho HTTP é pesquisado em cada solicitação HTTP. O nome do cabeçalho entre parênteses não diferencia maiúsculas de minúsculas, assim como a função 'hdr()' da ACL. Se o cabeçalho estiver ausente ou não contiver nenhum valor, o algoritmo Round Robin será aplicado. O parâmetro de algoritmo HTTP HEADER tem uma opção <code>headerName=&lt;name&gt;</code> . Por exemplo, você pode usar <b>host</b> como parâmetro do algoritmo HTTP HEADER.
URL	O parâmetro de URL especificado no argumento é pesquisado na cadeia de caracteres de consulta de cada solicitação HTTP GET. Se o parâmetro for seguido por um sinal de igual = e um valor, o valor receberá um hash e será dividido pelo peso total dos servidores em execução. O resultado designa qual servidor recebe a solicitação. Esse processo é usado para rastrear identificadores de usuário em solicitações e garantir que uma mesma ID de usuário seja sempre enviada para o mesmo servidor, desde que nenhum servidor seja ativado ou desativado. Se nenhum valor ou parâmetro for encontrado, será aplicado um algoritmo Round Robin. O parâmetro do algoritmo URL tem uma opção <code>urlParam=&lt;url&gt;</code> .

## 6 Adicione membros ao pool.

- a Clique no botão **Adicionar** ().
- b Insira o nome do membro do pool.
- c Insira o endereço IP do membro do pool.
- d Insira a porta na qual o membro deve receber o tráfego do balanceador de carga.
- e Insira a porta do monitor na qual o membro deve receber solicitações do monitor de integridade.
- f Na caixa de texto **Peso**, digite a proporção de tráfego que esse membro deve manipular. Deve ser um número inteiro no intervalo de 1 a 256.
- g (Opcional) Na caixa de texto **Máx. de Conexões**, digite o número máximo de conexões simultâneas que o membro pode manipular.

Quando o número de solicitações de entrada excede o máximo, as solicitações são enfileiradas e o balanceador de carga aguarda a liberação de uma conexão.

- h (Opcional) Na caixa de texto **Mín. de Conexões**, digite o número mínimo de conexões simultâneas que um membro deve sempre aceitar.
- i Clique em **Manter** para adicionar o novo membro ao pool.

A operação pode levar um minuto para ser concluída.

## 7 (Opcional) Para tornar os endereços IP de cliente visíveis para os servidores de back-end, selecione **Transparente**.

Quando **Transparente** não está selecionado (o valor padrão), os servidores de back-end veem o endereço IP da origem do tráfego como o endereço IP interno do balanceador de carga.

Quando **Transparente** é selecionado, o endereço IP de origem é o endereço IP real do cliente, e o edge gateway deve ser definido como o gateway padrão para garantir que os pacotes de retorno passem pelo edge gateway.

8 Para preservar as alterações, clique em **Manter**.


#### Próximo passo

Adicione servidores virtuais ao seu balanceador de carga. Um servidor virtual tem um endereço IP público e atende a todas as solicitações de cliente recebidas. Consulte [Adicionar um servidor virtual](#).

### Adicionar uma regra de aplicativo

Você pode gravar uma regra de aplicativo para manipular e gerenciar diretamente o tráfego de aplicativos IP.

#### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Acesse **Balanceador de Carga > Regras do Aplicativo**.
- 3 Clique no botão **Adicionar** ().
- 4 Insira o nome da regra de aplicativo.
- 5 Insira o script da regra de aplicativo.
 

Para obter informações sobre a sintaxe da regra de aplicativo, consulte <http://cbonte.github.io/haproxy-dconv/2.2/configuration.html>.
- 6 Para preservar as alterações, clique em **Manter**.

#### Próximo passo


Associe a nova regra de aplicativo a um servidor virtual adicionado ao balanceador de carga. Consulte [Adicionar um servidor virtual](#).

### Adicionar um servidor virtual


Adicione uma interface de uplink ou interna do edge gateway do NSX Data Center for vSphere como um servidor virtual. Um servidor virtual tem um endereço IP público e atende a todas as solicitações de cliente recebidas.

Por padrão, o balanceador de carga fecha a conexão TCP do servidor após cada solicitação de cliente.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Acesse **Balanceador de Carga > Servidores Virtuais**.
- 3 Clique no botão **Adicionar** ().
- 4 Na guia **Geral**, configure as seguintes opções para o servidor virtual:

Opção	Descrição
<b>Ativar Servidor Virtual</b>	Clique para ativar o servidor virtual.
<b>Ativar Aceleração</b>	Clique para ativar a aceleração.
<b>Perfil de Aplicativo</b>	Selecione um perfil de aplicativo a ser associado ao servidor virtual.
<b>Nome</b>	Digite um nome para o servidor virtual.
<b>Descrição</b>	Digite uma descrição opcional para o servidor virtual.
<b>Endereço IP</b>	Digite ou procure para selecionar o endereço IP que o balanceador de carga detecta.
<b>Protocolo</b>	Selecione o protocolo que o servidor virtual aceita. Você deve selecionar o mesmo protocolo usado pelo <b>Perfil de Aplicativo</b> selecionado.
<b>Porta</b>	Digite o número da porta que o balanceador de carga escuta.
<b>Pool Padrão</b>	Escolha o pool de servidores que o balanceador de carga vai usar.
<b>Limite de Conexão</b>	(Opcional) Digite o máximo de conexões simultâneas que o servidor virtual pode processar.
<b>Limite de Taxa de Conexão (CPS)</b>	(Opcional) Digite o número máximo de novas solicitações de conexão recebidas por segundo.

- 5 (Opcional) Para associar regras de aplicativo ao servidor virtual, clique na guia **Avançado** e siga estas etapas:
  - a Clique no botão **Adicionar** ().  
 As regras de aplicativo criadas para o balanceador de carga são exibidas. Se necessário, adicione regras de aplicativo para o balanceador de carga. Consulte [Adicionar uma regra de aplicativo](#).
- 6 Para preservar as alterações, clique em **Manter**.

## Próximo passo

Crie uma regra de firewall de edge gateway para permitir o tráfego para o novo servidor virtual (o endereço IP de destino). Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#)

## Configurar o acesso seguro usando VPN em um edge gateway do NSX Data Center for vSphere

Você pode configurar os recursos de VPN fornecidos pelo software NSX Data Center for vSphere em seus edge gateways do NSX Data Center for vSphere. Você pode configurar conexões de VPN com o data center virtual da sua organização usando um túnel SSL VPN-Plus, um túnel VPN IPsec ou um túnel VPN L2.

Conforme descrito no *NSX Administration Guide*, o gateway do NSX Edge oferece suporte a estes serviços de VPN:

- SSL VPN-Plus, que permite que os usuários remotos acessem aplicativos corporativos privados.
- VPN IPsec, que oferece conectividade de site a site entre um gateway do NSX Edge e sites remotos que também têm o NSX ou que têm roteadores de hardware ou gateways VPN de terceiros.
- VPN L2, que permite a extensão do data center virtual da organização, possibilitando que as máquinas virtuais mantenham a conectividade de rede e mantenham o mesmo endereço IP entre limites geográficos.

Em um ambiente do VMware Cloud Director, você pode criar túneis de VPN entre:

- Redes de data centers virtuais de organização na mesma organização
- Redes de data centers virtuais de organização em diferentes organizações
- Entre uma rede de data center virtual de organização e uma rede externa

---

**Observação** O VMware Cloud Director não oferece suporte a vários túneis VPN entre os mesmos dois edge gateways. Se houver um túnel entre dois edge gateways e você quiser adicionar outra sub-rede ao túnel, exclua o túnel VPN existente e crie um novo que inclua a nova sub-rede.

---

Depois de configurar túneis de VPN para um edge gateway, você pode usar um cliente VPN de um local remoto para se conectar ao data center virtual da organização que conta com o suporte desse edge gateway.

### Configurar o SSL VPN-Plus

Os serviços SSL VPN-Plus para um edge gateway do NSX Data Center for vSphere em um ambiente do VMware Cloud Director permitem que os usuários remotos se conectem com segurança às redes privadas e aos aplicativos nos centros de dados virtuais da organização com suporte por esse edge gateway. Você pode configurar vários serviços SSL VPN-Plus num edge gateway.

No seu ambiente VMware Cloud Director, o recurso SSL VPN-Plus de edge gateway oferece suporte ao modo de acesso à rede. Os usuários remotos devem instalar um cliente SSL para fazer conexões seguras e acessar as redes e aplicativos atrás do edge gateway. Como parte da configuração do SSL VPN-Plus do edge gateway, você adiciona os pacotes de instalação para o sistema operacional e configura determinados parâmetros. Consulte [Adicionar um pacote de instalação do cliente de SSL VPN-Plus](#) para obter mais detalhes.

A configuração do SSL VPN-Plus em um edge gateway é um processo de várias etapas.

#### Pré-requisitos

Verifique se todos os certificados SSL necessários para o SSL VPN-Plus foram adicionados à tela **Certificados**. Consulte [Gerenciamento de certificado SSL em um edge gateway do NSX Data Center for vSphere](#).

---

**Observação** Em um edge gateway, a porta 443 é a porta padrão para HTTPS. Para a funcionalidade da VPN SSL, a porta HTTPS do edge gateway deve ser acessível em redes externas. O cliente de VPN SSL exige que o endereço IP do edge gateway e a porta configurados na tela Configurações do servidor, na guia **SSL VPN-Plus**, sejam acessíveis no sistema cliente. Consulte [Definir configurações do servidor VPN SSL](#).

---

#### Procedimentos

##### 1 Navegar até a tela SSL-VPN Plus

Você pode navegar até a tela SSL-VPN Plus para começar a configurar o serviço SSL-VPN Plus para um edge gateway do NSX Data Center for vSphere.

##### 2 Definir configurações do servidor VPN SSL

Essas configurações do servidor definem o servidor VPN SSL, como o endereço IP e a porta na qual o serviço escuta, a lista de codificação do serviço e seu certificado de serviço. Ao se conectarem ao edge gateway do NSX Data Center for vSphere, os usuários remotos especificam o mesmo endereço IP e a porta definidos nessas configurações de servidor.

##### 3 Criar um pool de IPs para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere

Os usuários remotos recebem endereços IP virtuais dos pools de IPs estáticos que você configura usando a tela **Pools de IPs** na guia **SSL VPN-Plus**.

##### 4 Adicionar uma rede privada para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere

Use a tela Redes privadas na guia **SSL VPN-Plus** para configurar as redes privadas. As redes privadas são aquelas às quais você deseja que os clientes VPN tenham acesso quando os usuários remotos se conectam usando seus clientes VPN e o túnel VPN SSL. As redes privadas ativadas serão instaladas na tabela de roteamento do cliente VPN.

## 5 [Configurar um serviço de autenticação para SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere](#)

Use a tela **Autenticação** na guia **SSL VPN-Plus** para configurar um servidor de autenticação local para o serviço SSL VPN do edge gateway e, se desejar, habilite a autenticação de certificado de cliente. Este servidor de autenticação é usado para autenticar os usuários conectados. Todos os usuários configurados no servidor de autenticação local serão autenticados.

## 6 [Adicionar usuários do SSL VPN-Plus ao servidor de autenticação do SSL VPN-Plus local](#)

Use a tela **Usuários** na guia **SSL VPN-Plus** para adicionar contas de usuários remotos ao servidor de autenticação local para o serviço SSL VPN do edge gateway do NSX Data Center for vSphere.

## 7 [Adicionar um pacote de instalação do cliente de SSL VPN-Plus](#)

Use a tela Pacotes de Instalação na guia **SSL VPN-Plus** para criar pacotes de instalação nomeados do cliente SSL VPN-Plus para os usuários remotos.

## 8 [Editar configuração do cliente SSL VPN-Plus](#)

Use a tela **Configuração do Cliente** na guia **SSL VPN-Plus** para personalizar a forma como o túnel de cliente VPN SSL responde quando o usuário remoto faz login na VPN SSL.

## 9 [Personalizar as configurações gerais de SSL VPN-Plus para um edge gateway do NSX Data Center for vSphere](#)

Por padrão, o sistema define algumas configurações de SSL VPN-Plus em um edge gateway no seu ambiente VMware Cloud Director. Você pode usar a tela **Configurações Gerais** na guia **SSL VPN-Plus** no portal do tenant do VMware Cloud Director para personalizar essas configurações.

### Navegar até a tela SSL-VPN Plus

Você pode navegar até a tela SSL-VPN Plus para começar a configurar o serviço SSL-VPN Plus para um edge gateway do NSX Data Center for vSphere.

#### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **SSL VPN-Plus**.

#### Próximo passo

Na tela **Geral**, defina as configurações padrão de SSL VPN-Plus. Consulte [Personalizar as configurações gerais de SSL VPN-Plus para um edge gateway do NSX Data Center for vSphere](#).

## Definir configurações do servidor VPN SSL

Essas configurações do servidor definem o servidor VPN SSL, como o endereço IP e a porta na qual o serviço escuta, a lista de codificação do serviço e seu certificado de serviço. Ao se conectarem ao edge gateway do NSX Data Center for vSphere, os usuários remotos especificam o mesmo endereço IP e a porta definidos nessas configurações de servidor.

Se o seu edge gateway estiver configurado com várias redes de endereços IP sobrepostas em sua interface externa, o endereço IP selecionado para o servidor VPN SSL poderá ser diferente da interface externa padrão do edge gateway.

Ao definir as configurações do servidor VPN SSL, você deve escolher quais algoritmos de criptografia usar para o túnel VPN SSL. Você pode escolher uma ou mais criptografias. Escolha cuidadosamente as criptografias de acordo com os pontos fortes e fracos das suas seleções.

Por padrão, o sistema usa o certificado autoassinado padrão que ele gera para cada edge gateway como o certificado de identidade do servidor padrão para o túnel VPN SSL. Em vez disso, você pode optar por usar um certificado digital adicionado ao sistema na tela **Certificados**.

### Pré-requisitos

- Verifique se você cumpriu com os pré-requisitos descritos em [Configurar o SSL VPN-Plus](#).
- Se você optar por usar um certificado de serviço diferente do padrão, importe o certificado necessário para o sistema. Consulte [Adicionar um certificado de serviço ao edge gateway](#).
- [Navegar até a tela SSL-VPN Plus](#).

### Procedimentos

- 1 Na tela **SSL VPN-Plus**, clique em **Configurações do Servidor**.
- 2 Clique em **Habilitado**.
- 3 Selecione um endereço IP no menu suspenso.
- 4 (Opcional) Insira um número de porta TCP.

O número de porta TCP é usado pelo pacote de instalação do cliente SSL. Por padrão, o sistema usa a porta 443, que é a porta padrão para o tráfego HTTPS/SSL. Mesmo que um número de porta seja necessário, você pode definir qualquer porta TCP para comunicações.

---

**Observação** O cliente VPN SSL exige que o endereço IP e a porta configurada aqui sejam acessíveis nos sistemas clientes dos seus usuários remotos. Se você alterar o número de porta padrão, certifique-se de que a combinação de endereço IP e porta esteja acessível nos sistemas dos usuários pretendidos.

---

- 5 Selecione um método de criptografia na lista de codificação.
- 6 Configure a política de log Syslog do serviço.

O registro em log está ativado por padrão. Você pode alterar o nível de mensagens para registrar ou desativar logs.



- 7 (Opcional) Se você quiser usar um certificado de serviço em vez do certificado autoassinado padrão gerado pelo sistema, clique em **Alterar certificado do servidor**, selecione um certificado e clique em **OK**.
- 8 Clique em **Salvar alterações**.

#### Próximo passo

---

**Observação** O endereço IP do edge gateway e o número da porta TCP que você define devem ser acessíveis pelos usuários remotos. Adicione uma regra de firewall de edge gateway que permita o acesso ao endereço IP do SSL VPN-Plus e à porta configurada neste procedimento. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

---

Adicione um pool de IPs para que os usuários remotos recebam endereços IP ao se conectarem usando o SSL VPN-Plus. Consulte [Criar um pool de IPs para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere](#).

#### Criar um pool de IPs para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere

Os usuários remotos recebem endereços IP virtuais dos pools de IPs estáticos que você configura usando a tela **Pools de IPs** na guia **SSL VPN-Plus**.

Cada pool de IPs adicionado nessa tela resulta em uma sub-rede de endereços IP configurada no edge gateway. Os intervalos de endereços IP usados nesses pools de IPs devem ser diferentes de todas as outras redes configuradas no edge gateway.

---


**Observação** A VPN SSL atribui endereços IP aos usuários remotos dos pools de IPs com base na ordem em que os pools de IPs aparecem na tabela na tela. Depois de adicionar os pools de IPs à tabela na tela, você pode ajustar suas posições na tabela usando as setas para cima e para baixo.

---

#### Pré-requisitos

- [Navegar até a tela SSL-VPN Plus.](#)
- [Definir configurações do servidor VPN SSL.](#)

#### Procedimentos

- 1 Na guia **SSL VPN-Plus**, clique em **Pools de IPS**.
- 2 Clique no botão **Criar** ()

### 3 Defina as configurações do pool de IPs.

Opção	Ação
<b>Intervalo de IPs</b>	Insira um intervalo de endereços IP para este pool de IPs, como <b>127.0.0.1-127.0.0.9..</b>  Esses endereços IP serão atribuídos aos clientes VPN quando eles autenticarem e se conectarem ao túnel VPN SSL.
<b>Máscara de Rede</b>	Insira a máscara de rede do pool de IPs, como <b>255.255.255.0.</b>
<b>Gateway</b>	Insira o endereço IP que você deseja que o edge gateway crie e atribua como o endereço de gateway para este pool de IPs.  Quando o pool de IPs é criado, um adaptador virtual é criado na máquina virtual do edge gateway, e esse endereço IP é configurado nessa interface virtual. Esse endereço IP pode ser qualquer IP dentro da sub-rede que também não esteja no intervalo do campo <b>Intervalo de IPs.</b>
<b>Descrição</b>	(Opcional) Insira uma descrição para este pool de IPs.
<b>Status</b>	Selecione se deseja ativar ou desativar este pool de IPs.
<b>DNS Primário</b>	(Opcional) Insira o nome do servidor DNS primário que será usado para a resolução de nomes desses endereços IP virtuais.
<b>DNS Secundário</b>	(Opcional) Insira o nome do servidor DNS secundário a ser usado.
<b>Sufixo DNS</b>	(Opcional) Insira o sufixo DNS para o domínio no qual os sistemas cliente estão hospedados, para resolução de nome de host baseada em domínio.
<b>Servidor WINS</b>	(Opcional) Insira o endereço do servidor WINS conforme as necessidades da sua organização.

### 4 Clique em **Manter**.

#### Resultados

A configuração do pool de IPs é adicionada à tabela na tela.

#### Próximo passo

Adicione redes privadas que você deseja que sejam acessíveis aos usuários remotos que se conectam com o SSL VPN-Plus. Consulte [Adicionar uma rede privada para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere](#).

#### Adicionar uma rede privada para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere

Use a tela Redes privadas na guia **SSL VPN-Plus** para configurar as redes privadas. As redes privadas são aquelas às quais você deseja que os clientes VPN tenham acesso quando os usuários remotos se conectam usando seus clientes VPN e o túnel VPN SSL. As redes privadas ativadas serão instaladas na tabela de roteamento do cliente VPN.


As redes privadas são uma lista de todas as redes IP acessíveis atrás do edge gateway cujo tráfego você deseja criptografar para um cliente VPN ou excluir da criptografia. Cada rede privada que requer acesso por meio de um túnel VPN SSL deve ser adicionada como uma entrada separada. Você pode usar técnicas de sumarização de rota para limitar o número de entradas.

- O SSL VPN-Plus permite que usuários remotos acessem redes privadas com base na ordem de cima para baixo na qual os pools de IPs aparecem na tabela na tela. Depois de adicionar as redes privadas à tabela na tela, você pode ajustar suas posições na tabela usando as setas para cima e para baixo.
- Se você selecionar para ativar a otimização de TCP para uma rede privada, alguns aplicativos, como o FTP no modo ativo, poderão não funcionar nessa sub-rede. Para adicionar um servidor FTP configurado no modo ativo, você deve adicionar outra rede privada para esse servidor FTP e desativar a otimização de TCP para essa rede privada. Além disso, a rede privada desse servidor FTP deve ser ativada e exibida na tabela na tela acima da rede privada otimizada para TCP.

#### Pré-requisitos

- [Navegar até a tela SSL-VPN Plus.](#)
- [Criar um pool de IPs para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere.](#)

#### Procedimentos

- 1 Na guia **SSL VPN-Plus**, clique em **Redes Privadas**.
- 2 Clique no botão **Adicionar** ()
- 3 Defina as configurações de rede privada.

Opção	Ação
Rede	Digite o endereço IP da rede privada em um formato CIDR, como <b>192169.1.0/24</b> .
Descrição	(Opcional) Digite uma descrição para a rede.
Enviar Tráfego	<p>Especifique como deseja que o cliente VPN envie a rede privada e o tráfego de Internet.</p> <ul style="list-style-type: none"> <li>■ <b>Pelo Túnel</b> O cliente VPN envia a rede privada e o tráfego de Internet por meio do edge gateway ativado para SSL VPN-Plus.</li> <li>■ <b>Ignorar Túnel</b> O cliente VPN ignora o edge gateway e envia o tráfego diretamente para o servidor privado.</li> </ul>

Opção	Ação
<b>Ativar Otimização de TCP</b>	<p>(Opcional) Para otimizar a velocidade da Internet, ao selecionar <b>Pelo Túnel</b> para enviar o tráfego, você também deve selecionar <b>Ativar Otimização de TCP</b>.</p> <p>Selecionar essa opção melhora o desempenho dos pacotes TCP no túnel VPN, mas não melhora o desempenho do tráfego UDP.</p> <p>O túnel de VPNs SSL de acesso completo convencional envia dados de TCP/IP em uma segunda pilha TCP/IP para criptografia pela Internet. Esse método convencional encapsula os dados da camada de aplicativo em dois fluxos de TCP separados. Quando ocorre a perda de pacotes, o que pode acontecer mesmo em condições de Internet ideais, ocorre um efeito de degradação de desempenho chamado "TCP-over-TCP meltdown". Nesse efeito, dois instrumentos TCP corrigem o mesmo pacote único de dados IP, o que reduz a taxa de transferência da rede e causa tempos limite de conexão. Selecionar <b>Ativar Otimização de TCP</b> elimina o risco de esse problema ocorrer.</p> <hr/> <p><b>Observação</b> Quando você ativa a otimização de TCP:</p> <ul style="list-style-type: none"> <li>■ Você deve inserir os números de porta para otimizar o tráfego de Internet.</li> <li>■ O servidor VPN SSL abre a conexão TCP em nome do cliente VPN. Quando o servidor VPN SSL abre a conexão TCP, a primeira regra de firewall do edge gerada automaticamente é aplicada, o que permite que todas as conexões abertas do edge gateway sejam aprovadas. O tráfego que não é otimizado é avaliado pelas regras de firewall do edge comuns. A regra TCP gerada padrão permite qualquer conexão.</li> </ul> <hr/>
<b>Portas</b>	<p>Quando você selecionar <b>Pelo Túnel</b>, digite um intervalo de números de porta que deseja abrir para o usuário remoto acessar os servidores internos, como <b>20–21</b>, para o tráfego de FTP, e <b>80–81</b>, para o tráfego HTTP.</p> <p>Para conceder acesso irrestrito aos usuários, deixe o campo em branco.</p> <hr/>
<b>Status</b>	<p>Ative ou desative a rede privada.</p> <hr/>

4 Clique em **Manter**.

5 Clique em **Salvar alterações** para salvar a configuração no sistema.

#### Próximo passo

Adicione um servidor de autenticação. Consulte [Configurar um serviço de autenticação para SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere](#).

**Importante** Adicione as regras de firewall correspondentes para permitir o tráfego de rede para as redes privadas que você adicionou nesta tela. Consulte [Adicionar uma regra de firewall do edge gateway do NSX Data Center for vSphere](#).

#### Configurar um serviço de autenticação para SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere

Use a tela **Autenticação** na guia **SSL VPN-Plus** para configurar um servidor de autenticação local para o serviço SSL VPN do edge gateway e, se desejar, habilite a autenticação de certificado de

cliente. Este servidor de autenticação é usado para autenticar os usuários conectados. Todos os usuários configurados no servidor de autenticação local serão autenticados.

Você pode ter apenas um servidor de autenticação do SSL VPN-Plus local configurado no edge gateway. Se você clicar em **+ LOCAL** e especificar servidores de autenticação adicionais, uma mensagem de erro será exibida quando tentar salvar a configuração.

O tempo máximo de autenticação por VPN SSL é de três (3) minutos. Esse máximo é determinado pelo tempo limite de não autenticação, que é de três minutos por padrão e não é configurável. Como resultado, se você tiver vários servidores de autenticação na autorização da cadeia e a autenticação do usuário demorar mais de três minutos, o usuário não será autenticado.

#### Pré-requisitos

- [Navegar até a tela SSL-VPN Plus.](#)
- [Adicionar uma rede privada para uso com SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere.](#)
- Se você pretende habilitar a autenticação de certificados de cliente, verifique se um certificado de CA foi adicionado ao edge gateway. Consulte [Adicionar um certificado de CA ao Edge Gateway para verificação de confiança do certificado SSL.](#)

#### Procedimentos

- 1 Clique na guia **SSL VPN-Plus e Autenticação**.
- 2 Clique em **Local**.

### 3 Defina as configurações do servidor de autenticação.

#### a (Opcional) Habilite e configure a política de senha.

Opção	Descrição
<b>Ativar política de senha</b>	Ative a aplicação das configurações de política de senha que você configurar aqui.
<b>Tamanho da Senha</b>	Insira o número mínimo e máximo de caracteres permitidos para a senha.
<b>Nº mínimo de letras</b>	(Opcional) Digite o número mínimo de caracteres alfabéticos necessários na senha.
<b>Nº mínimo de dígitos</b>	(Opcional) Digite o número mínimo de caracteres numéricos necessários na senha.
<b>Nº mínimo de caracteres especiais</b>	(Opcional) Digite o número mínimo de caracteres especiais, como e comercial (&), marca hash (#), sinal de porcentagem (%) e assim por diante, que são necessários na senha.
<b>Senha não deve conter a ID de usuário</b>	(Opcional) Ative esta opção para que a senha não contenha a ID de usuário.
<b>Senha expira em</b>	(Opcional) Digite o número máximo de dias que uma senha pode existir antes de o usuário ter de alterá-la.
<b>Notificação de expiração em</b>	(Opcional) Digite o número de dias antes da expiração da senha em <b>Senha expira em</b> para que o usuário seja notificado de que a senha está prestes a expirar.

#### b (Opcional) Habilite e configure a política de bloqueio de conta.

Opção	Descrição
<b>Ativar política de bloqueio de conta</b>	Ative a aplicação das configurações de política de bloqueio de conta que você configurar aqui.
<b>Contagem de Tentativas</b>	Insira o número de vezes que um usuário pode tentar acessar sua conta.
<b>Duração da Nova Tentativa</b>	Insira o período de tempo em minutos em que a conta de usuário é bloqueada devido a tentativas de login malsucedidas. Por exemplo, se você especificar o <b>Contagem de Tentativas</b> como 5 e <b>Duração da Nova Tentativa</b> como 1 minuto, a conta do usuário será bloqueada após cinco tentativas de login malsucedidas dentro de um minuto.
<b>Duração do Bloqueio</b>	Insira o período de tempo durante o qual a conta de usuário permanecerá bloqueada. Após esse tempo, a conta será desbloqueada automaticamente.

#### c Na seção Status, habilite este servidor de autenticação.

- d (Opcional) Configure a autenticação secundária.

Opções	Descrição
Usar este servidor para autenticação secundária	(Opcional) Especifique se o servidor deve ser usado como o segundo nível de autenticação.
Encerrar sessão se houver falha na autenticação	(Opcional) Especifique se deseja encerrar a sessão VPN quando a autenticação falhar.

- e Clique em **Manter**.

- 4 (Opcional) Para habilitar a autenticação de certificação do cliente, clique em **Alterar certificado** e, em seguida, ative a alternância de ativação, selecione o certificado de CA a ser usado e clique em **OK**.

#### Próximo passo

Adicione usuários locais ao servidor de autenticação local para que eles possam se conectar ao SSL VPN-Plus. Consulte [Adicionar usuários do SSL VPN-Plus ao servidor de autenticação do SSL VPN-Plus local](#).

Crie um pacote de instalação contendo o cliente SSL para que os usuários remotos possam instalá-lo em seus sistemas locais. Consulte [Adicionar um pacote de instalação do cliente de SSL VPN-Plus](#).

#### Adicionar usuários do SSL VPN-Plus ao servidor de autenticação do SSL VPN-Plus local

Use a tela **Usuários** na guia **SSL VPN-Plus** para adicionar contas de usuários remotos ao servidor de autenticação local para o serviço SSL VPN do edge gateway do NSX Data Center for vSphere.

**Observação** Se um servidor de autenticação local ainda não estiver configurado, adicionar um usuário na tela **Usuários** adicionará automaticamente um servidor de autenticação local com valores padrão. É possível usar o botão Editar na tela **Autenticação** para exibir e editar os valores padrão. Para obter informações sobre como usar a tela **Autenticação**, consulte [Configurar um serviço de autenticação para SSL VPN-Plus em um edge gateway do NSX Data Center for vSphere](#).

#### Pré-requisitos

Navegar até a tela **SSL-VPN Plus**.

#### Procedimentos

- 1 Na guia **SSL VPN-Plus**, clique em **Usuários**.

- 2 Clique no botão **Criar** ()

### 3 Configure as seguintes opções para o usuário.

Opção	Descrição
ID de usuário	Insira a ID de usuário.
Senha	Insira a senha do usuário.
Digite a senha novamente	Insira a senha novamente.
Nome	(Opcional) Insira o nome do usuário.
Sobrenome	(Opcional) Insira o sobrenome do usuário.
Descrição	(Opcional) Insira uma descrição para o usuário.
Ativado	Especifique se o usuário está ativado ou desativado.
Senha nunca expira	(Opcional) Especifique se a mesma senha deve ser mantida para este usuário para sempre.
Permitir alteração de senha	(Opcional) Especifique se deseja permitir que o usuário altere a senha.
Alterar senha no próximo login	(Opcional) Especifique se deseja que esse usuário altere a senha no próximo login.

#### 4 Clique em **Manter**.

#### 5 Repita as etapas para adicionar outros usuários.

#### Próximo passo

Adicione usuários locais ao servidor de autenticação local para que eles possam se conectar ao SSL VPN-Plus. Consulte [Adicionar usuários do SSL VPN-Plus ao servidor de autenticação do SSL VPN-Plus local](#).

Crie um pacote de instalação contendo o cliente SSL para que os usuários remotos possam instalá-lo em seus sistemas locais. Consulte [Adicionar um pacote de instalação do cliente de SSL VPN-Plus](#).

#### Adicionar um pacote de instalação do cliente de SSL VPN-Plus

Use a tela Pacotes de Instalação na guia **SSL VPN-Plus** para criar pacotes de instalação nomeados do cliente SSL VPN-Plus para os usuários remotos.

Você pode adicionar um pacote de instalação de cliente SSL VPN-Plus ao edge gateway do NSX Data Center for vSphere. Novos usuários são solicitados a baixar e instalar esse pacote quando fazem login para usar a conexão VPN pela primeira vez. Quando adicionados, esses pacotes de instalação de cliente podem ser baixados do FQDN usando a interface pública do edge gateway.

Você pode criar pacotes de instalação executados nos sistemas operacionais Windows, Linux e Mac. Se precisar de parâmetros de instalação diferentes por cliente VPN SSL, crie um pacote de instalação para cada configuração.

#### Pré-requisitos

[Navegar até a tela SSL-VPN Plus](#)




## Procedimentos

1 Na guia **SSL VPN-Plus** no portal de tenant, clique em **Pacotes de Instalação**.

2 Clique no botão **Adicionar** (.

3 Defina as configurações do pacote de instalação.

Opção	Descrição
Nome do Perfil	Insira um nome de perfil para este pacote de instalação. Esse nome é exibido para o usuário remoto para identificar essa conexão VPN SSL com o edge gateway.
Gateway	Insira o endereço IP ou FQDN da interface pública do edge gateway. O endereço IP ou FQDN que você inserir estará vinculado ao cliente VPN SSL. Quando o cliente é instalado no sistema local do usuário remoto, esse endereço IP ou FQDN é exibido nesse cliente VPN SSL. Para vincular interfaces de uplink de edge gateway adicionais a esse cliente VPN SSL, clique no botão <b>Adicionar</b> (  ) para adicionar linhas e digitar os endereços IP de interface ou FQDNs e portas.
Porta	(Opcional) Para modificar o valor da porta do padrão exibido, clique duas vezes no valor e insira um novo valor.
Windows Linux Mac	Selecione os sistemas operacionais para os quais você deseja criar os pacotes de instalação.
Descrição	(Opcional) Digite uma descrição para o usuário.
Ativado	Especifique se este pacote está ativado ou desativado.

4 Selecione os parâmetros de instalação para o Windows.

Opção	Descrição
Iniciar cliente no login	Inicia o cliente VPN SSL quando o usuário remoto faz login no sistema local.
Permitir memorização de senha	Permite que o cliente memorize a senha do usuário.
Ativar instalação no modo silencioso	Ocultar os comandos de instalação dos usuários remotos.
Ocultar adaptador de rede do cliente SSL	Ocultar o adaptador de SSL VPN-Plus da VMware, que está instalado no computador do usuário remoto com o pacote de instalação do cliente VPN SSL.
Ocultar ícone de bandeja do sistema do cliente	Ocultar o ícone da bandeja VPN SSL que indica se a conexão VPN está ativa ou não.
Criar ícone da área de trabalho	Cria um ícone na área de trabalho do usuário para invocar o cliente SSL.
Ativar operação no modo silencioso	Ocultar a janela que indica que a instalação foi concluída.
Validação do certificado de segurança do servidor	O cliente VPN SSL valida o certificado do servidor VPN SSL antes de estabelecer a conexão segura.

5 Clique em **Manter**.

## Próximo passo

Edite a configuração do cliente. Consulte [Editar configuração do cliente SSL VPN-Plus](#).

## Editar configuração do cliente SSL VPN-Plus

Use a tela **Configuração do Cliente** na guia **SSL VPN-Plus** para personalizar a forma como o túnel de cliente VPN SSL responde quando o usuário remoto faz login na VPN SSL.

### Pré-requisitos

[Navegar até a tela SSL-VPN Plus](#)

### Procedimentos

- 1 Na guia **SSL VPN-Plus**, clique em **Configuração do Cliente**.
- 2 Selecione o **Modo de encapsulamento**.
  - No modo de túnel dividido, apenas o tráfego de VPN flui através do edge gateway.
  - No modo de túnel completo, o edge gateway se torna o gateway padrão para o usuário remoto e todo o tráfego, como VPN, local e Internet, flui através do edge gateway.
- 3 Se você selecionar o modo de túnel completo, insira o endereço IP para o gateway padrão usado pelos clientes dos usuários remotos e, opcionalmente, selecione se deseja excluir o tráfego de sub-rede local do fluxo por meio do túnel de VPN.
- 4 (Opcional) Desative a reconexão automática.

A opção **Ativar reconexão automática** está ativada por padrão. Se a reconexão automática estiver ativada, o cliente VPN SSL reconectará automaticamente os usuários quando eles forem desconectados.
- 5 (Opcional) Opcionalmente, habilite a capacidade do cliente de notificar os usuários remotos quando uma atualização do cliente estiver disponível.

Essa opção está desativada por padrão. Ao ativar essa opção, os usuários remotos poderão optar por instalar o upgrade.
- 6 Clique em **Salvar alterações**.

## Personalizar as configurações gerais de SSL VPN-Plus para um edge gateway do NSX Data Center for vSphere

Por padrão, o sistema define algumas configurações de SSL VPN-Plus em um edge gateway no seu ambiente VMware Cloud Director. Você pode usar a tela **Configurações Gerais** na guia **SSL VPN-Plus** no portal do tenant do VMware Cloud Director para personalizar essas configurações.

### Pré-requisitos

[Navegar até a tela SSL-VPN Plus](#).

### Procedimentos

- 1 Na guia **SSL VPN-Plus**, clique em **Configurações Gerais**.

## 2 Edite as configurações gerais conforme necessário para as necessidades da sua organização.

Opção	Descrição
<b>Impedir vários logins com o mesmo nome de usuário</b>	Ative para restringir um usuário remoto a ter apenas uma sessão de login ativa com o mesmo nome de usuário.
<b>Compactação</b>	Ative para habilitar a compactação inteligente de dados baseada em TCP e melhorar a velocidade de transferência de dados.
<b>Ativar Log</b>	Ative para manter um log do tráfego que passa pelo gateway VPN SSL. O registro em log está habilitado por padrão.
<b>Forçar teclado virtual</b>	Ative para exigir que os usuários remotos usem um teclado virtual (na tela) apenas para inserir informações de login.
<b>Tornar aleatórias as chaves do teclado virtual</b>	Ative para que o teclado virtual use um layout de teclas aleatório.
<b>Tempo limite de sessão ociosa</b>	Insira o tempo limite ocioso da sessão, em minutos. Se não houver atividade em uma sessão de usuário pelo período de tempo especificado, o sistema desconectará a sessão do usuário. O padrão do sistema é de 10 minutos.
<b>Notificação do usuário</b>	Digite a mensagem a ser exibida aos usuários remotos após o login.
<b>Ativar acesso à URL pública</b>	Ative para permitir que usuários remotos acessem sites que não estão explicitamente configurados por você para acesso remoto de usuários.
<b>Ativar tempo limite forçado</b>	Ative para que o sistema desconecte usuários remotos após o período de tempo especificado no campo <b>Tempo limite forçado</b> .
<b>Tempo limite forçado</b>	Digite o período de tempo limite em minutos. Este campo é exibido quando o botão de alternância <b>Ativar tempo limite forçado</b> está ativado.

## 3 Clique em **Salvar alterações**.

### Configurar VPN IPsec

Os edge gateways do NSX Data Center for vSphere em um ambiente do VMware Cloud Director oferecem suporte à Segurança de Protocolo IP (IPsec) site a site para proteger os túneis VPN entre as redes de centros de dados virtuais da organização ou entre uma rede de centros de dados virtuais da organização e um endereço IP externo. É possível configurar o serviço VPN IPsec num edge gateway.

A configuração de uma conexão VPN IPsec a partir de uma rede remota para o seu datacenter virtual da organização é o cenário mais comum. O software NSX fornece recursos de VPN IPsec de edge gateway, incluindo suporte para autenticação de certificado, modo de chave pré-compartilhada e tráfego unicast de IP entre si e roteadores VPN remotos. Você também pode

configurar várias sub-redes para se conectar por meio de túneis IPsec à rede interna atrás de um edge gateway. Quando você configura várias sub-redes para se conectar por meio de túneis IPsec à rede interna, essas sub-redes e a rede interna atrás do edge gateway não devem ter intervalos de endereços que se sobrepõem.

---

**Observação** Se o peer local e remoto em um túnel IPsec tiver endereços IP sobrepostos, o encaminhamento de tráfego pelo túnel pode não ser consistente, dependendo se as rotas conectadas localmente e se as rotas de conexão automática existem.

---

Os seguintes algoritmos de VPN IPsec são compatíveis:

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- DES triplo (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Grupo Diffie-Hellman 2)
- DH-5 (Grupo Diffie-Hellman 5)
- DH-14 (Grupo Diffie-Hellman 14)

---

**Observação** Os protocolos de roteamento dinâmico não são compatíveis com VPN IPsec. Quando você configura um túnel VPN IPsec entre um edge gateway do datacenter virtual da organização e um VPN de gateway físico num local remoto, não é possível configurar o roteamento dinâmico para essa conexão. O endereço IP desse site remoto não pode ser aprendido pelo roteamento dinâmico no uplink do edge gateway.

---

Conforme descrito no tópico *Visão geral de VPN IPsec* no *Guia de administração do NSX*, o número máximo de túneis suportados em um edge gateway é determinado pelo tamanho configurado: compacto, grande, muito grande e quádruplo.

Para exibir o tamanho da configuração do seu edge gateway, navegue até o edge gateway e clique em seu nome.

A configuração do VPN IPsec num edge gateway é um processo de várias etapas.

---

**Observação** Se um firewall estiver entre os endpoints do túnel, depois que você configurar o serviço VPN IPsec, atualize as regras de firewall para permitir os seguintes protocolos IP e portas UDP:

- ID do protocolo IP 50 (ESP)
  - ID do protocolo IP 51 (AH)
  - Porta UDP 500 (IKE)
  - Porta UDP 4500
- 

## Procedimentos

### 1 Navegar até a tela VPN IPsec

Na tela **VPN IPsec**, você pode começar a configurar o serviço VPN IPsec para um edge gateway do NSX Data Center for vSphere.

### 2 Configurar as conexões de sites VPN IPsec para o edge gateway do NSX Data Center for vSphere

Use a tela **Sites VPN IPsec** no portal do tenant do VMware Cloud Director para definir as configurações necessárias para criar uma conexão VPN IPsec entre o data center virtual da organização e outro site usando os recursos de VPN IPsec do edge gateway.

### 3 Habilitar o serviço de VPN IPsec em um edge gateway do NSX Data Center for vSphere

Quando pelo menos uma conexão de VPN IPsec está configurada, você pode habilitar o serviço de VPN IPsec no edge gateway.

### 4 Especificar configurações de VPN IPsec globais

Use a tela **Configuração Global** para definir as configurações de autenticação de VPN IPsec em um nível de edge gateway. Nessa tela, você pode definir uma chave pré-compartilhada global e habilitar a autenticação de certificação.

## Navegar até a tela VPN IPsec

Na tela **VPN IPsec**, você pode começar a configurar o serviço VPN IPsec para um edge gateway do NSX Data Center for vSphere.

## Procedimentos

### 1 Abra Serviços de Edge Gateway.

- a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
- b Selecione o edge gateway que você deseja editar e clique em **Serviços**.

### 2 Navegue até **VPN > VPN IPsec**.

**Próximo passo**

Use a tela **Sites VPN IPsec** para configurar uma conexão VPN IPsec. Pelo menos uma conexão deve ser configurada para que você possa habilitar o serviço VPN IPsec no edge gateway. Consulte [Configurar as conexões de sites VPN IPsec para o edge gateway do NSX Data Center for vSphere](#).

**Configurar as conexões de sites VPN IPsec para o edge gateway do NSX Data Center for vSphere**

Use a tela **Sites VPN IPsec** no portal do tenant do VMware Cloud Director para definir as configurações necessárias para criar uma conexão VPN IPsec entre o data center virtual da organização e outro site usando os recursos de VPN IPsec do edge gateway.

Ao configurar uma conexão VPN IPsec entre sites, você configura a conexão do ponto de vista do seu local atual. A configuração da conexão requer que você entenda os conceitos no contexto do ambiente VMware Cloud Director para configurar a conexão VPN corretamente.


- As sub-redes locais e de peer especificam as redes às quais a VPN se conecta. Ao especificar essas sub-redes nas configurações dos sites VPN IPsec, insira um intervalo de rede, e não um endereço IP específico. Use o formato CIDR, como **192.168.99.0/24**.
- O ID de peer é um identificador que identifica exclusivamente o dispositivo remoto que encerra a conexão VPN, normalmente seu endereço IP público. Para os peers que usam a autenticação de certificado, esse ID deve ser o nome diferenciado definido no certificado do peer. Para peers PSK, esse ID pode ser qualquer cadeia de caracteres. Uma prática recomendada do NSX é usar o endereço IP público do dispositivo remoto ou o FQDN como o ID do peer. Se o endereço IP do peer for de outra rede de data center virtual de organização, insira o endereço IP nativo do peer. Se a NAT estiver configurada para o peer, insira o endereço IP privado do peer.
- O endpoint do peer especifica o endereço IP público do dispositivo remoto ao qual você está se conectando. O endpoint do peer pode ser um endereço diferente do ID do par quando o gateway do par não está diretamente acessível na Internet, mas se conectar por meio de outro dispositivo. Se a NAT estiver configurada para o peer, insira o endereço IP público que os dispositivos usam para a NAT.
- O ID local especifica o endereço IP público do edge gateway do data center virtual da organização. Você pode inserir um endereço IP ou um nome de host junto com o firewall do edge gateway.
- O endpoint local especifica a rede no data center virtual da organização no qual o edge gateway faz transmissões. Normalmente, a rede externa do edge gateway é o endpoint local.

**Pré-requisitos**

- [Navegar até a tela VPN IPsec.](#)
- [Configurar VPN IPsec.](#)

- Se você pretende usar um certificado global como o método de autenticação, verifique se a autenticação de certificado está habilitada na tela **Configuração Global**. Consulte [Especificar configurações de VPN IPsec globais](#).

## Procedimentos

- Abra Serviços de Edge Gateway.
  - Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- Na guia **VPN IPsec**, clique em **Sites VPN IPsec**.
- Clique no botão **Adicionar** ().
- Defina as configurações de conexões de VPN IPsec.

Opção	Ação
<b>Ativado</b>	Habilite essa conexão entre os dois endpoints de VPN.
<b>Ativar Perfect Forward Secrecy (PFS)</b>	<p>Habilite essa opção para que o sistema gere chaves públicas exclusivas para todas as sessões de VPN IPsec que os seus usuários iniciarem.</p> <p>Habilitar o PFS garante que o sistema não crie um link entre a chave privada do edge gateway e cada chave de sessão.</p> <p>O comprometimento de uma chave de sessão não afetará os dados que não sejam os dados trocados na sessão específica protegida por essa chave específica. Não é possível usar o comprometimento da chave privada do servidor para descriptografar sessões arquivadas ou sessões futuras.</p> <p>Quando o PFS está habilitado, as conexões de VPN IPsec com esse edge gateway apresentam uma pequena sobrecarga de processamento.</p> <p><b>Importante</b> As chaves de sessão exclusivas não devem ser usadas para derivar qualquer chave adicional. Além disso, ambos os lados do túnel VPN IPsec devem oferecer suporte ao PFS para que ele funcione.</p>
<b>Nome</b>	(Opcional) Insira um nome para a conexão.
<b>ID Local</b>	<p>Insira o endereço IP externo da instância do edge gateway, que é o endereço IP público desse edge gateway.</p> <p>O endereço IP é aquele usado para o ID do peer na configuração de VPN IPsec no site remoto.</p>
<b>Endpoint Local</b>	<p>Insira a rede que é o endpoint local dessa conexão.</p> <p>O endpoint local especifica a rede no data center virtual da organização no qual o edge gateway faz transmissões. Normalmente, a rede externa é o endpoint local.</p> <p>Se você adicionar um túnel de IP para IP usando uma chave pré-compartilhada, o ID local e o IP do endpoint local poderão ser os mesmos.</p>
<b>Sub-Redes Locais</b>	<p>Insira as redes a serem compartilhadas entre os sites e use uma vírgula como separador para inserir várias sub-redes.</p> <p>Insira um intervalo de rede (e não um endereço IP específico) inserindo o endereço IP no formato CIDR. Por exemplo, <b>192.168.99.0/24</b>.</p>

Opção	Ação
<b>ID de Peer</b>	<p>Insira uma ID de peer para identificar exclusivamente o site do peer.</p> <p>O ID de peer é um identificador que assinala exclusivamente o dispositivo remoto que encerra a conexão VPN, normalmente seu endereço IP público.</p> <p>Para os peers que usam autenticação de certificado, o ID deve ser o nome diferenciado no certificado do peer. Para peers PSK, esse ID pode ser qualquer cadeia de caracteres. Uma prática recomendada do NSX é usar o endereço IP público ou o FQDN do dispositivo remoto como o ID do peer.</p> <p>Se o endereço IP do peer for de outra rede de data center virtual de organização, insira o endereço IP nativo do peer. Se a NAT estiver configurada para o peer, insira o endereço IP privado do peer.</p>
<b>Endpoint de Peer</b>	<p>Insira o endereço IP ou o FQDN do site do peer, que é o endereço público do dispositivo remoto ao qual você está se conectando.</p> <p><b>Observação</b> Quando a NAT estiver configurada para o peer, insira o endereço IP público que o dispositivo usa para a NAT.</p>
<b>Sub-Redes de Peer</b>	<p>Insira a rede remota à qual a VPN se conecta e use uma vírgula como separador para inserir várias sub-redes.</p> <p>Insira um intervalo de rede (e não um endereço IP específico) inserindo o endereço IP no formato CIDR. Por exemplo, <b>192.168.99.0/24</b>.</p>
<b>Algoritmo de Criptografia</b>	<p>Selecione o tipo de algoritmo de criptografia no menu suspenso.</p> <p><b>Observação</b> O tipo de criptografia selecionado deve corresponder ao tipo de criptografia configurado no dispositivo de VPN do site remoto.</p>
<b>Autenticação</b>	<p>Selecione uma autenticação. As opções são:</p> <ul style="list-style-type: none"> <li>■ <b>PSK</b> <p>A chave pré-compartilhada (PSK) especifica que a chave secreta compartilhada entre o edge gateway e o site do peer deve ser usada para autenticação.</p> </li> <li>■ <b>Certificado</b> <p>A autenticação de certificado especifica que o certificado definido no nível global deve ser usado para autenticação. Essa opção só estará disponível se você tiver configurado o certificado global na tela <b>Configuração Global</b> da guia <b>VPN IPsec</b>.</p> </li> </ul>
<b>Alterar Chave Compartilhada</b>	<p>(Opcional) Ao atualizar as configurações de uma conexão existente, você pode ativar essa opção para tornar o campo <b>Chave Pré-compartilhada</b> disponível e, assim, poder atualizar a chave compartilhada.</p>
<b>Chave Pré-Compartilhada</b>	<p>Se você selecionou <b>PSK</b> como tipo de autenticação, digite uma cadeia de caracteres de segredo alfanumérica, que pode ter um comprimento máximo de 128 bytes.</p> <p><b>Observação</b> A chave compartilhada deve corresponder à chave configurada no dispositivo de VPN do site remoto. Uma prática recomendada é configurar uma chave compartilhada quando sites anônimos forem ser conectados ao serviço de VPN.</p>
<b>Exibir Chave Compartilhada</b>	<p>(Opcional) Habilite essa opção para tornar a chave compartilhada visível na tela.</p>



Opção	Ação
Grupo Diffie-Hellman	<p>Selecione o esquema de criptografia que permite que o site do peer e esse edge gateway estabeleçam um segredo compartilhado em um canal de comunicação inseguro.</p> <p><b>Observação</b> O Grupo Diffie-Hellman deve corresponder ao que está configurado no dispositivo de VPN do site remoto.</p>
Extensão	<p>(Opcional) Digite uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>■ <code>securelocaltrafficbyip=IPAddress</code> para redirecionar o tráfego local do edge gateway pelo túnel de VPN IPsec.</li> </ul> <p>Esse é o valor padrão.</p> <ul style="list-style-type: none"> <li>■ <code>passthroughSubnets=PeerSubnet/IPAddress</code> para oferecer suporte a sub-redes sobrepostas.</li> </ul>

5 Clique em **Manter**.

6 Clique em **Salvar alterações**.

#### Próximo passo

Configure a conexão para o site remoto. Você deve configurar a conexão de VPN IPsec em ambos os lados da conexão: no data center virtual da organização e no site do peer.

Habilite o serviço de VPN IPsec nesse edge gateway. É possível habilitar o serviço quando pelo menos uma conexão de VPN IPsec está configurada. Consulte [Habilitar o serviço de VPN IPsec em um edge gateway do NSX Data Center for vSphere](#).

#### Habilitar o serviço de VPN IPsec em um edge gateway do NSX Data Center for vSphere

Quando pelo menos uma conexão de VPN IPsec está configurada, você pode habilitar o serviço de VPN IPsec no edge gateway.

#### Pré-requisitos

- [Navegar até a tela VPN IPsec](#).
- Verifique se pelo menos uma conexão de VPN IPsec está configurada para esse edge gateway. Consulte as etapas descritas em [Configurar as conexões de sites VPN IPsec para o edge gateway do NSX Data Center for vSphere](#).

#### Procedimentos

- 1 Na guia **VPN IPsec**, clique em **Status de Ativação**.
- 2 Clique em **Status do Serviço de VPN IPsec** para habilitar o serviço de VPN IPsec.
- 3 Clique em **Salvar alterações**.

#### Resultados

O serviço de VPN IPsec do edge gateway está ativo.

## Especificar configurações de VPN IPsec globais

Use a tela **Configuração Global** para definir as configurações de autenticação de VPN IPsec em um nível de edge gateway. Nessa tela, você pode definir uma chave pré-compartilhada global e habilitar a autenticação de certificação.

Uma chave pré-compartilhada global é usada para esses sites cujo endpoint do peer está definido como **qualquer**.

### Pré-requisitos

- Se pretende habilitar a autenticação de certificado, verifique se tem pelo menos um certificado de serviço e os certificados assinados pela autoridade de certificação correspondentes na tela **Certificados**. Certificados autoassinados não podem ser usados para VPNs IPsec. Consulte [Adicionar um certificado de serviço ao edge gateway](#).
- [Navegar até a tela VPN IPsec](#).

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Na guia **VPN IPsec**, clique em **Configuração Global**.
- 3 (Opcional) Defina uma chave pré-compartilhada global:
  - a Habilite a opção **Alterar Chave Compartilhada**.
  - b Insira uma chave pré-compartilhada.
 

A chave pré-compartilhada global (PSK) é compartilhada por todos os sites cujo endpoint de peer está definido como `any`. Se uma PSK global já estiver definida, altere a PSK para um valor vazio e salvá-la não terá efeito sobre a configuração existente.
  - c (Opcional) Opcionalmente, habilite **Exibir Chave Compartilhada** para tornar a chave pré-compartilhada visível.
  - d Clique em **Salvar alterações**.
- 4 Configure a autenticação de certificação:
  - a Ative **Ativar Autenticação de Certificado**.
  - b Selecione os certificados de serviço, certificados de CA e CRLs apropriados.
  - c Clique em **Salvar alterações**.

### Próximo passo

Opcionalmente, você pode habilitar o registro em log para o serviço VPN IPsec do edge gateway. Consulte [Estatísticas e logs para um Edge Gateway do NSX Data Center for vSphere](#).

## Configurar o VPN L2

Os edge gateways do NSX Data Center for vSphere em um ambiente do VMware Cloud Director suportam VPN L2. Com a VPN L2, você pode estender o centro de dados virtual de organização, permitindo que as máquinas virtuais mantenham a conectividade de rede e mantenham o mesmo endereço IP independente das fronteiras geográficas. Você pode configurar o serviço de VPN L2 em um edge gateway.

O NSX Data Center for vSphere fornece os recursos de VPN L2 de um edge gateway. Com a VPN L2, você pode configurar um túnel entre dois locais. As máquinas virtuais permanecem na mesma sub-rede, apesar de serem movidas entre esses locais, o que permite que você estenda o datacenter virtual da organização alongando sua rede usando VPN L2. Um edge gateway num site pode fornecer todos os serviços para máquinas virtuais no outro site.

Para criar o túnel VPN L2, você configura um servidor VPN L2 e um cliente VPN L2. Conforme descrito no *Guia de administração do NSX*, o servidor VPN L2 é o edge gateway de destino e o cliente de VPN L2 é o edge gateway de origem. Depois de definir as configurações de VPN L2 em cada edge gateway, você deve habilitar o serviço VPN L2 no servidor e no cliente.

---

**Observação** Uma rede de centro de dados virtuais da organização roteada, criada como uma subinterface, deve existir nos edge gateways.

---

### Navegar até a tela VPN L2

Para começar a configurar o serviço de VPN L2 para um edge gateway do NSX Data Center for vSphere, você deve navegar até a tela **VPN L2**.

#### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Navegue até **VPN > VPN L2**.

#### Próximo passo

Configure o servidor VPN L2. Consulte [Configurar o edge gateway do NSX Data Center for vSphere como um servidor VPN L2](#).

### Configurar o edge gateway do NSX Data Center for vSphere como um servidor VPN L2

O servidor VPN L2 é o edge do NSX de destino à qual o cliente VPN L2 vai se conectar.

Conforme descrito no *Guia de administração do NSX*, você pode conectar vários sites pares a esse servidor VPN L2.

---

**Observação** Alterar as definições de configuração do site faz com que o edge gateway se desconecte e reconecte todas as conexões existentes.

---

## Pré-requisitos

- Verifique se o edge gateway tem uma rede do centro de dados virtual de organização roteada e configurada como uma subinterface no edge gateway.
- [Navegar até a tela VPN L2.](#)
- Se você quiser associar um certificado de serviço à conexão VPN L2, verifique se o certificado do servidor já foi carregado no edge gateway. Consulte [Adicionar um certificado de serviço ao edge gateway.](#)
- Você deve ter o IP de ouvinte do servidor, a porta de ouvinte, o algoritmo de criptografia e pelo menos um site par configurado antes de poder habilitar o serviço VPN L2.

## Procedimentos

- 1 Na guia **VPN L2**, selecione **Servidor** para o modo VPN L2.
- 2 Na guia **Servidor global**, configure os detalhes de configuração global do servidor VPN L2.

Opção	Ação
IP do Ouvinte	Selecione o endereço IP primário ou secundário de uma interface externa do edge gateway.
Porta do Ouvinte	Edite o valor exibido conforme apropriado para as necessidades da organização. A porta padrão para o serviço VPN L2 é 443.
Algoritmo de Criptografia	Selecione o algoritmo de criptografia para a comunicação entre o servidor e o cliente.
Detalhes do Certificado de Serviço	Clique em <b>Alterar o certificado do servidor</b> para selecionar o certificado a ser vinculado ao servidor VPN L2. Na janela <b>Alterar certificado do servidor</b> , ative <b>Validar certificado do servidor</b> , selecione um certificado do servidor na lista e clique em <b>OK</b> .

- 3 Para configurar os sites pares, clique na guia **Sites do servidor**.

- 4 Clique no botão **Adicionar** ().

- 5 Defina as configurações para um site par do VPN L2.

Opção	Ação
Ativado	Habilite este site par.
Nome	Insira um nome exclusivo para o site par.
Descrição	(Opcional) Digite uma descrição.
ID de usuário	Insira o nome de usuário e a senha de autenticação do site par.
Senha	As credenciais do usuário no site par devem ser as iguais às credenciais no lado do cliente.
Confirmar Senha	

Opção	Ação
<b>Interfaces Estendidas</b>	Selecione pelo menos uma subinterface a ser estendida com o cliente. As subinterfaces disponíveis para seleção são aquelas redes de datacenters virtuais da organização configuradas como subinterfaces no edge gateway.
<b>Endereço do Gateway de Otimização de Saída</b>	(Opcional) Se o gateway padrão para máquinas virtuais for o mesmo nos dois sites, insira os endereços IP do gateway das subinterfaces para as quais você deseja que o tráfego seja roteado localmente ou bloqueado pelo túnel VPN L2.

6 Clique em **Manter**.

7 Clique em **Salvar alterações**.

#### Próximo passo

Habilite o serviço VPN L2 neste edge gateway. Consulte [Habilitar o serviço de VPN L2 em um edge gateway do NSX Data Center for vSphere](#).

### Configurar o edge gateway do NSX Data Center for vSphere como um cliente VPN L2

O cliente VPN L2 é o NSX Edge de origem que inicia a comunicação com o NSX Edge de destino, o servidor VPN L2.

#### Pré-requisitos

- [Navegar até a tela VPN L2](#).
- Se esse cliente VPN L2 estiver conectado a um servidor VPN L2 que usa um certificado de servidor, verifique se o Certificado de Autoridade de Certificação correspondente foi carregado no edge gateway para habilitar a validação do certificado do servidor para esse cliente VPN L2. Consulte [Adicionar um certificado de CA ao Edge Gateway para verificação de confiança do certificado SSL](#).

#### Procedimentos

- 1 Na guia **VPN L2**, selecione **Cliente** para o modo VPN L2.
- 2 Na guia **Cliente global**, configure os detalhes de configuração global do cliente VPN L2.

Opção	Descrição
<b>Endereço do Servidor</b>	Insira o endereço IP do servidor VPN L2 ao qual este cliente deve ser conectado.
<b>Porta do Servidor</b>	Insira a porta do servidor VPN L2 à qual o cliente deve se conectar. A porta padrão é 443.
<b>Algoritmo de Criptografia</b>	Selecione o algoritmo de criptografia para comunicação com o servidor.
<b>Interfaces Estendidas</b>	Selecione as subinterfaces a serem estendidas para o servidor. As subinterfaces disponíveis para seleção são as redes do datacenter virtual da organização configuradas como subinterfaces no edge gateway.

Opção	Descrição
<b>Endereço do Gateway de Otimização de Saída</b>	(Opcional) Se o gateway padrão para máquinas virtuais for o mesmo nos dois sites, digite os endereços IP de gateway das subinterfaces ou os endereços IP nos quais o tráfego não deve fluir pelo túnel.
<b>Detalhes do Usuário</b>	Insira a ID de usuário e a senha para autenticação com o servidor.

3 Clique em **Salvar alterações**.

4 (Opcional) Para configurar opções avançadas, clique na guia **Cliente avançado**.

5 Se esse edge do cliente VPN L2 não tiver acesso direto à Internet e for necessário acessar o edge do servidor VPN L2 usando um servidor proxy, especifique as configurações de proxy.

Opção	Descrição
<b>Ativar Proxy Seguro</b>	Selecione para habilitar o proxy seguro.
<b>Endereço</b>	Insira o endereço IP do servidor proxy.
<b>Porta</b>	Insira a porta do servidor proxy.
<b>Nome de Usuário</b>	Insira as credenciais de autenticação do servidor proxy.
<b>Senha</b>	

6 Para habilitar a validação de certificação do servidor, clique em **Alterar Certificado de CA** e selecione o Certificado de Autoridade de Certificação apropriado.

7 Clique em **Salvar alterações**.

#### Próximo passo

Habilite o serviço VPN L2 neste edge gateway. Consulte [Habilitar o serviço de VPN L2 em um edge gateway do NSX Data Center for vSphere](#).

#### Habilitar o serviço de VPN L2 em um edge gateway do NSX Data Center for vSphere

Quando as configurações de VPN L2 necessárias estiverem concluídas, você poderá habilitar o serviço de VPN L2 no edge gateway.

**Observação** Se o HA já estiver configurado nesse edge gateway, certifique-se de que o edge gateway tenha mais de uma interface interna configurada nele. Se apenas uma interface existir e essa já tiver sido usada pelo recurso de HA, a configuração da VPN L2 na mesma interface interna falhará.

#### Pré-requisitos

- Se esse edge gateway for um servidor de VPN L2, o NSX Edge de destino, verifique se as configurações do servidor de VPN L2 necessárias e pelo menos um site de peer de VPN L2 estão configurados. Consulte as etapas descritas em [Configurar o edge gateway do NSX Data Center for vSphere como um servidor VPN L2](#).

- Se esse edge gateway for um cliente VPN L2, o NSX Edge de origem, verifique se as configurações do cliente de VPN L2 estão definidas. Consulte as etapas descritas em [Configurar o edge gateway do NSX Data Center for vSphere como um cliente VPN L2](#).
- [Navegar até a tela VPN L2](#).

#### Procedimentos

- 1 Na guia **VPN L2**, clique na opção **Habilitar**.
- 2 Clique em **Salvar alterações**.

#### Resultados

O serviço VPN L2 do edge gateway ficará ativo.

#### Próximo passo

Crie regras de NAT ou de firewall no lado do firewall voltado para a Internet para permitir que o servidor VPN L2 se conecte ao cliente VPN L2.

## Remover a configuração do serviço de VPN L2 de um edge gateway do NSX Data Center for vSphere

Você pode remover a configuração do serviço VPN L2 existente do edge gateway. Essa ação também desativa o serviço de VPN L2 no edge gateway.

#### Pré-requisitos

[Navegar até a tela VPN L2](#)

#### Procedimentos

- 1 Role para baixo até a parte inferior da tela VPN L2 e clique em **Excluir configuração**.
- 2 Para confirmar a exclusão, clique em **OK**.

#### Resultados

O serviço VPN L2 é desativado, e os detalhes de configuração são removidos do edge gateway.

## Gerenciamento de certificado SSL em um edge gateway do NSX Data Center for vSphere

O software NSX Data Center for vSphere no ambiente VMware Cloud Director fornece a capacidade de usar certificados SSL (Secure Sockets Layer) com os túneis de VPN-Plus SSL e VPN IPsec que você configura para seus gateways de borda.

Os edge gateways no seu ambiente VMware Cloud Director oferecem suporte para certificados autoassinados, certificados assinados por uma autoridade de certificação (CA) e certificados gerados e assinados por uma CA. Você pode gerar solicitações de assinatura de certificado (CSRs), importar os certificados, gerenciar os certificados importados e criar listas de certificados revogados (CRLs).

## Sobre o uso de certificados com seu centro de dados virtual de organização

Você pode gerenciar certificados para as seguintes áreas de rede no data center virtual de organização do VMware Cloud Director.

- Túneis de VPN IPsec entre uma rede de data center virtual de organização e uma rede remota.
- Conexões SSL VPN-Plus entre usuários remotos com redes privadas e recursos da Web no seu data center virtual de organização.
- Um túnel VPN L2 entre dois edge gateways do NSX Data Center for vSphere.
- Os servidores virtuais e servidores de pools configurados para balanceamento de carga no data center virtual da organização

### Como usar certificados de cliente

Você pode criar um certificado de cliente por meio de um comando CAI ou de uma chamada REST. Em seguida, pode distribuir esse certificado aos seus usuários remotos, que podem instalar o certificado em seus navegadores da Web.

O principal benefício de implementar certificados de cliente é que um certificado de cliente de referência para cada usuário remoto pode ser armazenado e verificado em relação ao certificado de cliente apresentado pelo usuário remoto. Para evitar conexões futuras de um determinado usuário, você pode excluir o certificado de referência da lista de certificados de cliente do servidor seguro. Excluir o certificado nega as conexões desse usuário.

### Gerar uma solicitação de assinatura de certificado para um edge gateway

Para solicitar um certificado assinado de uma autoridade de certificação ou criar um certificado autoassinado, você deve gerar uma solicitação de assinatura de certificado (CSR) para o seu edge gateway.

Uma CSR é um arquivo codificado que você precisa gerar em um gateway do NSX Edge que requer um certificado SSL. Usar uma CSR padroniza a maneira como as empresas enviam suas chaves públicas junto com informações que identificam seus nomes de empresa e nomes de domínio.

Você gera uma CSR com um arquivo de chave privada correspondente que deve permanecer no edge gateway. A CSR contém a chave pública correspondente e outras informações, como o nome, o local e o nome de domínio da sua organização.

#### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Na guia **Certificados**, clique em **CSR**.



#### 4 Configure as seguintes opções para a CSR:

Opção	Descrição
<b>Nome Comum</b>	Insira o nome de domínio totalmente qualificado (FQDN) da organização para a qual você usará o certificado (por exemplo, <code>www.example.com</code> ). Não inclua os prefixos <code>http://</code> ou <code>https://</code> no seu nome comum.
<b>Unidade Organizacional</b>	Use esse campo para diferenciar as divisões na sua organização VMware Cloud Director com a qual esse certificado está associado. Por exemplo, Engenharia ou Vendas.
<b>Nome da Organização</b>	Insira o nome sob o qual sua empresa está legalmente registrada. A organização listada deve ser o inscrito legal do nome do domínio na solicitação de certificado.
<b>Localidade</b>	Insira a cidade ou localidade na qual sua empresa está legalmente registrada.
<b>Nome do Estado ou Província</b>	Insira o nome completo (não use abreviação) do estado, da província, da região ou do território no qual sua empresa está legalmente registrada.
<b>Código do País</b>	Insira o nome do país no qual sua empresa está legalmente registrada.
<b>Algoritmo de Private Key</b>	Digite o tipo de chave, RSA ou DSA, para o certificado. A RSA normalmente é usada. O tipo de chave define o algoritmo de criptografia para a comunicação entre os hosts.  <b>Observação</b> O SSL VPN-Plus só é compatível com certificados RSA.
<b>Tamanho da Chave</b>	Insira o tamanho da chave em bits. O mínimo é de 2048 bits.
<b>Descrição</b>	(Opcional) Insira uma descrição para o certificado.

#### 5 Clique em **Manter**.

O sistema gera a CSR e adiciona uma nova entrada com o tipo CSR à lista na tela.

#### Resultados

Na lista na tela, quando você seleciona uma entrada com o tipo CSR, os detalhes da CSR são exibidos na tela. Você pode copiar os dados exibidos com formatação PEM da CSR e enviá-los a uma autoridade de certificação (CA) para obter um certificado assinado por essa CA.

#### Próximo passo

Use a CSR para criar um certificado de serviço usando uma destas duas opções:

- Transmita a CSR a uma CA para obter um certificado assinado pela CA. Quando a CA lhe enviar o certificado assinado, importe-o para o sistema. Consulte [Importar o certificado assinado pela autoridade de certificação correspondente à CSR gerada para um edge gateway](#).
- Use a CSR para criar um certificado autoassinado. Consulte [Configurar um certificado de serviço autoassinado](#).

## Importar o certificado assinado pela autoridade de certificação correspondente à CSR gerada para um edge gateway

Depois de gerar uma Solicitação de Assinatura de Certificado (CSR) e obter o certificado assinado pela autoridade de certificação com base nessa CSR, você pode importar o certificado assinado pela CA para uso pelo edge gateway.

### Pré-requisitos

Verifique se você obteve o certificado assinado pela autoridade de certificação que corresponde à CSR. Se a chave privada no certificado assinado pela CA não corresponder àquela da CSR selecionada, o processo de importação falhará.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Selecione a CSR na tabela na tela para a qual você está importando o certificado assinado pela CA.
- 4 Importe o certificado assinado.
  - a Clique em **Certificado assinado gerado para CSR**.
  - b Forneça os dados do PEM do certificado assinado pela CA.
    - Se os dados estiverem em um arquivo PEM em um sistema para o qual você possa navegar, clique no botão **Carregar** para navegar até o arquivo e selecione-o.
    - Se você puder copiar e colar os dados do PEM, cole-os no campo **Certificado Assinado (formato PEM)**.  
 Inclua as linhas `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`.
  - c (Opcional) Digite uma descrição.
  - d Clique em **Manter**.

---

**Observação** Se a chave privada no certificado assinado pela CA não corresponder à da CSR selecionada na tela Certificados, o processo de importação falhará.

---

### Resultados

O certificado assinado pela CA com o tipo Certificado de Serviço é exibido na lista na tela.

### Próximo passo

Anexe o certificado assinado pela CA aos túneis de SSL VPN-Plus ou VPN IPsec conforme necessário. Consulte [Definir configurações do servidor VPN SSL](#) e [Especificar configurações de VPN IPsec globais](#).

## Configurar um certificado de serviço autoassinado

Você pode configurar certificados de serviço autoassinados com seus edge gateways do para usar em seus recursos relacionados à VPN. Você pode criar, instalar e gerenciar certificados autoassinados.

Se o certificado de serviço estiver disponível na tela certificados, você poderá especificar esse certificado de serviço ao definir as configurações relacionadas à VPN do edge gateway. A VPN apresenta o certificado de serviço especificado para os clientes que acessam a VPN.

### Pré-requisitos

Verifique se pelo menos um CSR está disponível na tela **Certificados** para o edge gateway. Consulte [Gerar uma solicitação de assinatura de certificado para um edge gateway](#).

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Selecione o CSR na lista que você deseja usar para esse certificado autoassinado e clique em **Autoassinar CSR**.
- 4 Digite o número de dias pelos quais o certificado autoassinado é válido.
- 5 Clique em **Manter**.

O sistema gera o certificado autoassinado e adiciona uma nova entrada com o tipo Certificado de Serviço à lista na tela.

### Resultados

O certificado autoassinado está disponível no edge gateway. Na lista na tela, quando você seleciona uma entrada com o tipo de certificado de serviço, seus detalhes são exibidos na tela.

## Adicionar um certificado de CA ao Edge Gateway para verificação de confiança do certificado SSL

Adicionar um certificado de CA a um edge gateway permite a verificação de confiança dos certificados SSL que são apresentados ao edge gateway para autenticação, normalmente os certificados de cliente usados em conexões VPN com o edge gateway.

Você normalmente adiciona o certificado raiz de sua empresa ou organização como um certificado de CA. Um uso típico é para a VPN SSL, onde você deseja autenticar clientes VPN usando certificados. Os certificados de cliente podem ser distribuídos para os clientes VPN. Quando os clientes VPN se conectam, seus certificados de cliente são validados com base no certificado de CA.

---

**Observação** Ao adicionar um certificado de CA, você normalmente configura uma Lista de Revogação de Certificados (CRL) relevante. A CRL protege os clientes que apresentam certificados revogados. Consulte [Adicionar uma Lista de Revogação de Certificados a um Edge Gateway](#).

---

### Pré-requisitos

Verifique se você tem os dados do certificado de CA no formato PEM. Na interface do usuário, você pode colar os dados PEM do certificado de CA ou navegar até um arquivo que contém os dados e que está disponível na rede do seu sistema local.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Clique em **Certificado de CA**.
- 4 Forneça os dados do certificado de CA.
  - Se os dados estiverem em um arquivo PEM em um sistema para o qual você possa navegar, clique no botão **Carregar** para navegar até o arquivo e selecione-o.
  - Se você puder copiar e colar os dados do PEM, cole-os no campo **Certificado de CA (Formato PEM)**.  
 Inclua as linhas `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`.
- 5 (Opcional) Digite uma descrição.
- 6 Clique em **Manter**.

### Resultados

O certificado de CA é exibido na lista da tela com o tipo de certificado. Esse certificado de CA agora está disponível para você especificar quando definir as configurações relacionadas à VPN do edge gateway.

## Adicionar uma Lista de Revogação de Certificados a um Edge Gateway

Uma Lista de Revogação de Certificados (CRL) é uma lista de certificados digitais que a Autoridade de Certificação (CA) emissora solicita que sejam revogados, para que os sistemas

possam ser atualizados de modo a não confiar em usuários que apresentem certificados revogados. Você pode adicionar CRLs ao edge gateway.

Conforme descrito no *Guia de Administração do NSX*, a CRL contém os seguintes itens:

- Os certificados revogados e os motivos da revogação
- As datas em que os certificados foram emitidos
- As entidades que emitiram os certificados
- Uma data proposta para a próxima versão

Quando um usuário em potencial tenta acessar um servidor, o servidor permite ou nega o acesso com base na entrada desse usuário específico na CRL.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Clique em **CRL**.
- 4 Forneça os dados da CRL.
  - Se os dados estiverem em um arquivo PEM em um sistema para o qual você possa navegar, clique no botão **Carregar** para navegar até o arquivo e selecione-o.
  - Se você puder copiar e colar os dados PEM, cole-os no campo **CRL (Formato PEM)**.  
Inclua as linhas `-----BEGIN X509 CRL-----` e `-----END X509 CRL-----`.
- 5 (Opcional) Digite uma descrição.
- 6 Clique em **Manter**.

### Resultados

A CRL é exibida na lista na tela.

## Adicionar um certificado de serviço ao edge gateway

Adicionar certificados de serviço a um edge gateway torna esses certificados disponíveis para uso nas configurações relacionadas à VPN do edge gateway. Você pode adicionar um certificado de serviço à tela **Certificados**.

### Pré-requisitos

Verifique se você tem o certificado de serviço e sua chave privada no formato PEM. Na interface do usuário, você pode colar nos dados PEM ou navegar até um arquivo que contém os dados e que está disponível na sua rede do seu sistema local.

## Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Certificados**.
- 3 Clique em **Certificado de serviço**.
- 4 Insira os dados formatados por PEM do certificado de serviço.
  - Se os dados estiverem em um arquivo PEM em um sistema para o qual você possa navegar, clique no botão **Carregar** para navegar até o arquivo e selecione-o.
  - Se você puder copiar e colar os dados do PEM, cole-os no campo **Certificado de Serviço (formato PEM)**.  
 Inclua as linhas `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`.
- 5 Insira os dados formatados por PEM da chave privada do certificado.
 

Quando o modo FIPS está ativo, os tamanhos de chaves RSA devem ser superiores ou iguais a 2048 bits.

  - Se os dados estiverem em um arquivo PEM em um sistema para o qual você possa navegar, clique no botão **Carregar** para navegar até o arquivo e selecione-o.
  - Se você puder copiar e colar os dados do PEM, cole-os no campo **Private Key (formato PEM)**.  
 Inclua as linhas `-----BEGIN RSA PRIVATE KEY-----` e `-----END RSA PRIVATE KEY-----`.
- 6 Insira uma frase-chave da private key e confirme-a.
- 7 (Opcional) Insira uma descrição.
- 8 Clique em **Manter**.

## Resultados

O certificado do tipo Certificado de Serviço é exibido na lista na tela. Este certificado de serviço agora está disponível para você selecionar quando definir as configurações relacionadas à VPN do edge gateway.

## Objetos de agrupamento personalizados para edge gateways do NSX Data Center for vSphere

O software NSX Data Center for vSphere no seu ambiente VMware Cloud Director fornece a capacidade de definir conjuntos e grupos de determinadas entidades, que você pode usar ao especificar outras configurações relacionadas à rede, como em regras de firewall.

## Criar um conjunto de IPs para uso em regras de firewall e configuração de retransmissão DHCP

Um conjunto de IP é um grupo de endereços IP que você pode criar em um nível de centro de dados virtual da organização. Você pode usar um conjunto de IP como origem ou destino em uma regra de firewall ou em uma configuração de retransmissão de DHCP.

Você cria um conjunto de IPs usando a página **Objetos de Agrupamento** do portal do tenant do VMware Cloud Director. A página **Objetos de Agrupamento** está disponível nas telas Serviços e Edge Gateway.


### Procedimentos

- 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
<b>Abrir por meio de serviços de Edge Gateway</b>	a Navegue até <b>Rede &gt; Edges</b> . b Selecione o edge gateway que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .
<b>Abrir por meio de serviços de segurança</b>	a Navegue até <b>Rede &gt; Segurança</b> . b Selecione o serviço de segurança que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .

- 2 Clique na guia **Conjuntos de IPs**.

Os conjuntos de IPs já definidos são exibidos na tela.

- 3 Para adicionar um conjunto de IPs, clique no botão **Criar** ().
- 4 Digite um nome e, opcionalmente, uma descrição para o conjunto de IPs, e os endereços IP a serem incluídos no conjunto.
- 5 (Opcional) Se você estiver especificando o conjunto de IPs usando a página **Objetos de Agrupamento** na tela Serviços, use a opção **Herança** para ativar a herança e permitir a visibilidade em escopos subjacentes.

A herança está habilitada por padrão.

- 6 Para salvar o conjunto de IPs, clique em **Manter**.

### Resultados

O novo conjunto de IPs estará disponível para seleção como origem ou destino nas regras de firewall ou nas configurações de retransmissão de DHCP.

## Criar um conjunto de MACs para uso em regras de firewall

Um conjunto de MACs é um grupo de endereços MAC que você pode criar em um nível de centro de dados virtual de organização. Você pode usar um conjunto de MACs como a origem ou o destino em uma regra de firewall.

Você cria um conjunto de MACs usando a página **Objetos de Agrupamento** do portal do tenant do VMware Cloud Director. A página **Objetos de Agrupamento** está disponível nas telas **Serviços** e **Edge Gateway**.


### Procedimentos

- 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
<b>Abrir por meio de serviços de Edge Gateway</b>	<ol style="list-style-type: none"> <li>a Navegue até <b>Rede &gt; Edges</b>.</li> <li>b Selecione o edge gateway que você deseja editar e clique em <b>Configurar Serviços</b>.</li> <li>c Clique em <b>Objetos de Agrupamento</b>.</li> </ol>
<b>Abrir por meio de serviços de segurança</b>	<ol style="list-style-type: none"> <li>a Navegue até <b>Rede &gt; Segurança</b>.</li> <li>b Selecione o serviço de segurança que você deseja editar e clique em <b>Configurar Serviços</b>.</li> <li>c Clique em <b>Objetos de Agrupamento</b>.</li> </ol>

- 2 Clique na guia **Conjuntos de MACs**.

Os conjuntos de MACs já definidos são exibidos na tela.

- 3 Para adicionar um conjunto de MACs, clique no botão **Criar** ().
- 4 Digite um nome para o conjunto e, opcionalmente, uma descrição, bem como os endereços MAC a serem incluídos nele.
- 5 (Opcional) Se você estiver especificando o conjunto de MACs usando a página **Objetos de Agrupamento** na tela **Serviços**, use a opção **Herança** para habilitar a herança e permitir a visibilidade em escopos subjacentes.

A herança está habilitada por padrão.

- 6 Para salvar o conjunto de MACs, clique em **Manter**.

### Resultados

O novo conjunto de MACs está disponível para seleção como origem ou destino em regras de firewall.

## Exibir serviços disponíveis para regras de firewall

É possível visualizar a lista de serviços disponíveis para uso nas regras de firewall. Nesse contexto, um serviço é uma combinação de porta com protocolo.



Você pode visualizar os serviços disponíveis usando a página Objetos de Agrupamento do portal de tenants do VMware Cloud Director. A página Objetos de Agrupamento está disponível nas telas Serviços e Edge Gateway.

Não é possível adicionar novos serviços à lista usando-se o portal de tenants. O conjunto de serviços disponíveis para uso é gerenciado pelo administrador de sistema do VMware Cloud Director.

## Procedimentos

### 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
<b>Abrir por meio de serviços de Edge Gateway</b>	a Navegue até <b>Rede &gt; Edges</b> . b Selecione o edge gateway que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .
<b>Abrir por meio de serviços de segurança</b>	a Navegue até <b>Rede &gt; Segurança</b> . b Selecione o serviço de segurança que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .

### 2 Clique na guia **Serviços**.

## Resultados

Os serviços disponíveis aparecem na tela.

## Exibir grupos de serviços disponíveis para regras de firewall

É possível visualizar a lista de grupos de serviços disponíveis para uso nas regras de firewall. Nesse contexto, um serviço é uma combinação de porta com protocolo, e um grupo de serviços é um grupo de serviços ou outros grupos de serviços.

Você pode visualizar os grupos de serviços disponíveis usando a página Objetos de Agrupamento do portal de tenants do VMware Cloud Director. A página Objetos de Agrupamento está disponível nas telas Serviços e Edge Gateway.

Não é possível criar grupos de serviços usando o portal de tenants. O conjunto de grupos de serviços disponíveis para uso é gerenciado pelo administrador de sistema do VMware Cloud Director.

## Procedimentos

### 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
<b>Abrir por meio de serviços de Edge Gateway</b>	a Navegue até <b>Rede &gt; Edges</b> . b Selecione o edge gateway que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .
<b>Abrir por meio de serviços de segurança</b>	a Navegue até <b>Rede &gt; Segurança</b> . b Selecione o serviço de segurança que você deseja editar e clique em <b>Configurar Serviços</b> . c Clique em <b>Objetos de Agrupamento</b> .

### 2 Clique na guia **Grupos de Serviços**.

## Resultados

Os grupos de serviços disponíveis aparecem na tela. A coluna Descrição exibe os serviços agrupados em cada grupo de serviços.

## Estatísticas e logs para um Edge Gateway do NSX Data Center for vSphere

Você pode exibir estatísticas e logs para um edge gateway do NSX Data Center for vSphere.

## Visualizar estatísticas

Você pode visualizar as estatísticas na tela **Serviços do Edge Gateway**.

## Procedimentos

- Abra Serviços de Edge Gateway.
  - Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- Clique na guia **Estatísticas**.
- Navegue pelas guias dependendo do tipo de estatística que deseja ver.

Opção	Descrição
<b>Conexões</b>	A tela Conexões fornece visibilidade operacional. A tela exibe gráficos para o tráfego que flui pelas interfaces do edge gateway selecionado e para o firewall. Selecione o período cujas estatísticas deseja visualizar.
<b>VPN IPsec</b>	A tela VPN IPsec exibe o status e as estatísticas da VPN IPsec, bem como o status e as estatísticas de cada túnel.
<b>VPN L2</b>	A tela VPN L2 exibe o status e as estatísticas da VPN L2.

## Ativar Log

Você pode ativar o log para um edge gateway. Além de habilitar o log para os recursos para os quais você deseja coletar dados de log, para concluir a configuração, você deve ter um servidor de syslog para receber os dados de log coletados. Quando você configura um servidor de syslog na tela Configurações do Edge, é possível acessar os dados registrados desse servidor de syslog.

### Pré-requisitos

- Verifique se você é um **administrador da organização** ou se recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se a sua função inclui o direito **Configurar Log do Sistema**.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.

- 2 Na guia **Configurações do Edge**, clique no botão **Editar Servidor de Syslog**.

Você pode personalizar o servidor de syslog para os logs relacionados à rede do seu edge gateway dos serviços que tenham o log habilitado.

Se o administrador do sistema do VMware Cloud Director já tiver configurado um servidor de syslog para o ambiente VMware Cloud Director, o sistema usará esse servidor de syslog por padrão, e seu endereço IP será exibido na tela **Configurações do Edge**.

- 3 Habilite o registro em log por recurso.
  - Na guia **NAT**, clique no botão **Regra de DNAT** e ative o botão de alternância **Ativar log**.  
Registra a conversão de endereços.
  - Na guia **NAT**, clique no botão **Regra de SNAT** e ative o botão de alternância **Ativar log**.  
Registra a conversão de endereços.
  - Na guia **Roteamento**, clique em **Configuração de Roteamento** e, em Configuração de Roteamento Dinâmico, ative o botão de alternância **Ativar log**.  
Registra as atividades de roteamento dinâmico. No menu suspenso **Nível de Log**, você pode selecionar o limite inferior do nível de status da mensagem a ser registrado.
  - Na guia **Balanceador de Carga**, clique em **Configuração Global** e ative a opção **Ativar log**.  
Registra o fluxo de tráfego do balanceador de carga. No menu suspenso **Nível de Log**, você pode selecionar o limite inferior do nível de status da mensagem a ser registrado.
  - Na guia **VPN**, navegue até **VPN IPSec > Configurações de Log** e ative o botão de alternância **Ativar log**.

Registra o fluxo de tráfego entre a sub-rede local e a sub-rede do peer. No menu suspenso **Nível de Log**, você pode selecionar o limite inferior do nível de status da mensagem a ser registrado.

- Na guia **SSL VPN-Plus**, clique em **Configurações Gerais** e ative o botão de alternância **Ativar log**.

Mantém um log do tráfego transmitido pelo gateway de VPN SSL.

- Na guia **SSL VPN-Plus**, clique em **Configurações do Servidor** e ative a opção **Ativar log**.

Registra as atividades que ocorrem no servidor VPN SSL para o syslog. No menu suspenso **Nível de Log**, você pode selecionar o limite inferior do nível de status da mensagem a ser registrado.

## Ativar o acesso pela linha de comando SSH a um edge gateway do NSX Data Center for vSphere

É possível ativar o acesso pela linha de comando SSH para um edge gateway.

### Procedimentos

- 1 Abra Serviços de Edge Gateway.
  - a Na barra de navegação superior, clique em **Rede** e, depois, em **Edge Gateways**.
  - b Selecione o edge gateway que você deseja editar e clique em **Serviços**.
- 2 Clique na guia **Configurações do Edge**.
- 3 Defina as configurações de SSH.

Opção	Descrição
Nome de usuário	Digite as credenciais de acesso SSH a este edge gateway.
Senha	Por padrão, o nome de usuário SSH é <b>admin</b> .
Digite a senha novamente	
Expiração de Senha	Insira o período de expiração da senha, em dias.
Banner de Login	Insira o texto a ser exibido aos usuários quando eles iniciarem uma conexão SSH com o edge gateway.

- 4 Ative o botão de alternância **Habilitado**.

### Próximo passo

Configure as regras de NAT ou de firewall apropriadas para permitir o acesso SSH a esse edge gateway.

## Trabalho com tags de segurança para edge gateways do NSX Data Center for vSphere

As marcas de segurança são rótulos que podem ser associados a uma máquina virtual ou a um grupo de máquinas virtuais. As marcas de segurança devem ser usadas com grupos de

segurança. Depois de criar as marcas de segurança, associe-as a um grupo de segurança que pode ser usado em regras de firewall. Você pode criar, editar ou atribuir uma marca de segurança definida pelo usuário. Você também pode ver quais máquinas virtuais ou grupos de segurança têm uma determinada marca de segurança aplicada.

Um caso de uso comum para marcas de segurança é agrupar os objetos dinamicamente para simplificar as regras de firewall. Por exemplo, você pode criar várias marcas de segurança diferentes com base no tipo de atividade que deverá ocorrer em uma determinada máquina virtual. Você cria uma marca de segurança para servidores de banco de dados e outra para servidores de e-mail. Em seguida, aplique a marca apropriada a máquinas virtuais que abrigam servidores de banco de dados ou servidores de e-mail. Depois, você poderá atribuir a marca a um grupo de segurança e gravar uma regra de firewall nele, aplicando configurações de segurança diferentes, dependendo se a máquina virtual estiver executando um servidor de banco de dados ou um servidor de e-mail. Após isso, se você alterar a funcionalidade da máquina virtual, poderá remover a máquina virtual da marca de segurança em vez de editar a regra de firewall.


## Criar e atribuir marcas de segurança

É possível criar uma marca de segurança e atribuí-la a uma máquina virtual ou a um grupo de máquinas virtuais.

Você cria uma marca de segurança e a atribui a uma máquina virtual ou a um grupo de máquinas virtuais.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione um serviço de segurança e clique em **Configurar serviços**.
- 3 Clique na guia **Marcas de Segurança**.

- 4 Clique no botão **Criar** () e insira um nome para a marca de segurança.

- 5 (Opcional) Insira uma descrição para a marca de segurança.

- 6 (Opcional) Atribua a marca de segurança a uma máquina virtual ou a um grupo de máquinas virtuais.

No menu suspenso **Procurar objetos do tipo**, a opção **Máquinas Virtuais** está selecionada por padrão.

- a Selecione uma máquina virtual no painel esquerdo.
- b Atribua a marca de segurança à máquina virtual selecionada clicando na seta para a direita.

A máquina virtual é movida para o painel direito e recebe a marca de segurança.

- 7 Quando você concluir a atribuição da marca às máquinas virtuais selecionadas, clique em **Manter**.

## Resultados

A marca de segurança é criada e, se você escolher, é atribuída às máquinas virtuais selecionadas.

## Próximo passo

As marcas de segurança são projetadas para funcionar com um grupo de segurança. Para obter mais informações sobre como criar grupos de segurança, consulte [Criar um grupo de segurança](#).

## Alterar a atribuição de marca de segurança

Depois de criar uma marca de segurança, você pode atribuí-la manualmente a máquinas virtuais. Você também pode editar uma marca de segurança para remover a marca das máquinas virtuais às quais você já a atribuiu.

Se você tiver criado marcas de segurança, poderá atribuí-las a máquinas virtuais. Você pode usar marcas de segurança para agrupar máquinas virtuais para salvar regras de firewall. Por exemplo, você pode atribuir uma marca de segurança a um grupo de máquinas virtuais com dados altamente sensíveis.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione um serviço de segurança e clique em **Configurar serviços**.
- 3 Clique na guia **Marcas de Segurança**.
- 4 Na lista de marcas de segurança, selecione a marca de segurança que você deseja editar e clique no botão **Editar**.
- 5 Selecione máquinas virtuais no painel esquerdo e atribua a marca de segurança a elas clicando na seta para a direita.

As máquinas virtuais no painel direito são atribuídas à marca de segurança.

- 6 Selecione máquinas virtuais no painel direito e remova a marca delas clicando na seta para a esquerda.

As máquinas virtuais no painel esquerdo não têm a marca de segurança atribuída.

- 7 Quando terminar de adicionar as alterações, clique em **Manter**.

## Resultados

A marca de segurança é atribuída às máquinas virtuais selecionadas.

## Próximo passo

As marcas de segurança são projetadas para funcionar com um grupo de segurança. Para obter mais informações sobre como criar grupos de segurança, consulte [Criar um grupo de segurança](#).

## Exibir marcas de segurança aplicadas

Você pode visualizar as marcas de segurança aplicadas às máquinas virtuais no seu ambiente. Também é possível ver as marcas de segurança aplicadas aos grupos de segurança no seu ambiente.

### Pré-requisitos

Uma marca de segurança deve ter sido criada e aplicada a uma máquina virtual ou a um grupo de segurança.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione um serviço de segurança e clique em **Configurar serviços**.
- 3 Visualize as marcas atribuídas na guia **Marcas de Segurança**.
  - a Na guia **Marcas de Segurança**, selecione a marca de segurança cujas atribuições deseja ver e clique no ícone **Editar**.
  - b Em **Atribuir/Cancelar atribuição de VMs**, você vê a lista de máquinas virtuais atribuídas à marca de segurança.
  - c Clique em **Descartar**.
- 4 Visualize as marcas atribuídas na guia **Grupos de Segurança**.
  - a Clique na guia **Objetos de Agrupamento** e clique em **Grupos de Segurança**.
  - b Selecione um grupo de segurança.
  - c Na lista sob **Incluir Membros**, você vê a marca de segurança atribuída a um grupo de segurança.

### Resultados

Você pode visualizar as marcas de segurança existentes e os grupos de segurança e máquinas virtuais associados. Dessa forma, você pode determinar uma estratégia para a criação de regras de firewall com base em marcas e grupos de segurança.

## Editar uma marca de segurança

Você pode editar uma marca de segurança definida pelo usuário.

Se você alterar o ambiente ou a função de uma máquina virtual, talvez também queira usar uma marca de segurança diferente para que as regras de firewall estejam corretas para a nova configuração de máquina. Por exemplo, se você tiver uma máquina virtual na qual não deseja mais armazenar dados confidenciais, talvez queira atribuir uma marca de segurança diferente para que as regras de firewall que se aplicam a dados confidenciais não sejam mais executadas nessa máquina virtual.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione um serviço de segurança e clique em **Configurar serviços**.
- 3 Clique na guia **Marcas de Segurança**.
- 4 Na lista de marcas de segurança, selecione a marca de segurança que você deseja editar.
- 5 Clique no botão **Editar**.
- 6 Edite o nome e a descrição da marca de segurança.
- 7 Atribua a marca ou remova a atribuição das máquinas virtuais que você selecionar.
- 8 Para salvar as alterações, clique em **Manter**.

## Próximo passo

Se você editar uma marca de segurança, talvez também precise editar um grupo de segurança ou as regras de firewall associadas. Para obter mais informações sobre grupos de segurança, consulte [Trabalho com grupos de segurança para edge gateways do NSX Data Center for vSphere](#).

## Excluir uma marca de segurança

Você pode excluir uma marca de segurança definida pelo usuário.

Talvez você queira excluir uma marca de segurança se a função ou o ambiente da máquina virtual for alterado. Por exemplo, se você tiver uma marca de segurança para bancos de dados Oracle, mas decidir usar um servidor de banco de dados diferente, poderá remover a marca de segurança para que as regras de firewall que se aplicam aos bancos de dados Oracle não sejam mais executadas na máquina virtual.

## Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Rede**, selecione **Segurança**.
- 2 Selecione um serviço de segurança e clique em **Configurar serviços**.
- 3 Clique na guia **Marcas de Segurança**.
- 4 Na lista de marcas de segurança, selecione a marca de segurança que você deseja excluir.
- 5 Clique no botão **Excluir**.
- 6 Para confirmar a exclusão, clique em **OK**.

## Resultados

A marca de segurança é excluída.



## Próximo passo

Se você excluir uma marca de segurança, talvez também precise editar um grupo de segurança ou as regras de firewall associadas. Para obter mais informações sobre grupos de segurança, consulte [Trabalho com grupos de segurança para edge gateways do NSX Data Center for vSphere](#).

## Trabalho com grupos de segurança para edge gateways do NSX Data Center for vSphere

Um grupo de segurança é um conjunto de ativos ou objetos de agrupamento, como máquinas virtuais, redes de centros de dados virtuais da organização ou marcas de segurança.

Os grupos de segurança podem ter critérios de associação dinâmica com base em marcas de segurança, nome da máquina virtual, nome do SO convidado da máquina virtual ou nome do host convidado da máquina virtual. Por exemplo, todas as máquinas virtuais que têm a marca de segurança "web" serão automaticamente adicionadas a um grupo de segurança específico destinado a servidores Web. Após a criação de um grupo de segurança, uma política de segurança será aplicada a esse grupo.

### Criar um grupo de segurança

Você pode criar grupos de segurança definidos pelo usuário.

#### Pré-requisitos

Se quiser usar marcas de segurança com grupos de segurança, [Criar e atribuir marcas de segurança](#).

#### Procedimentos

- 1 Abra os Serviços de Segurança.
  - a Navegue até **Rede > Segurança**.
  - b Selecione o VDC de organização ao qual você deseja aplicar configurações de segurança e clique em **Configurar Serviços**.

O portal do tenant abre Serviços de Segurança.

- 2 Navegue até **Objetos de Agrupamento > Grupos de Segurança**


A página **Grupos de Segurança** é aberta.

- 3 Clique no botão **Criar** ().

- 4 Insira um nome e, opcionalmente, uma descrição para o novo grupo de segurança.

A descrição é exibida na lista de grupos de segurança; portanto, adicionar uma descrição significativa pode facilitar a identificação rápida do grupo de segurança.

## 5 (Opcional) Adicione um conjunto de membros dinâmicos.

- a Clique no botão **Adicionar** () em Conjuntos de Membros Dinâmicos.
- b Selecione se deseja correspondências com **Qualquer** ou **Todos** os critérios da sua instrução.
- c Insira o primeiro objeto a ser correspondido.  
As opções são **Marca de Segurança**, **Nome do SO Convidado da VM**, **Nome da VM** e **Nome do Host Convidado da VM**.
- d Selecione um operador, como **Contém**, **Começa com** ou **Termina com**.
- e Insira um valor.
- f (Opcional) Para adicionar outra instrução, use um operador booleano **And** ou **Or**.

## 6 (Opcional) Inclua membros.

- a No menu suspenso **Navegar por objetos do tipo**, selecione o tipo de objeto, como **Máquinas Virtuais**, **Redes de VDC da organização**, **Conjuntos de IPs**, **Conjuntos de MACs** ou **Marcas de segurança**.
- b Para incluir um objeto na lista Incluir Membros, selecione-o no painel esquerdo e mova-o até o painel direito clicando na seta para a direita.

## 7 (Opcional) Exclua membros.

- a No menu suspenso **Navegar por objetos do tipo**, selecione o tipo de objeto, como **Máquinas Virtuais**, **Redes de VDC da organização**, **Conjuntos de IPs**, **Conjuntos de MACs** ou **Marcas de segurança**.
- b Para incluir um objeto na lista Excluir Membros, selecione-o no painel esquerdo e mova-o até o painel direito clicando na seta para a direita.

## 8 Para preservar as alterações, clique em **Manter**.

### Resultados

O grupo de segurança agora pode ser usado em regras, como regras de firewall.

## Editar um grupo de segurança

Você pode editar grupos de segurança definidos pelo usuário.

### Procedimentos

#### 1 Abra os Serviços de Segurança.

- a Navegue até **Rede > Segurança**.
- b Selecione o VDC de organização ao qual você deseja aplicar configurações de segurança e clique em **Configurar Serviços**.

O portal do tenant abre Serviços de Segurança.

## 2 Navegue até **Objetos de Agrupamento > Grupos de Segurança**

A página **Grupos de Segurança** é aberta.

### 3 Selecione o grupo de segurança que você deseja editar.

Os detalhes do grupo de segurança são exibidos abaixo da lista de grupos de segurança.

### 4 (Opcional) Edite o nome e a descrição do grupo de segurança.

### 5 (Opcional) Adicione um conjunto de membros dinâmicos.

- a Clique no botão **Adicionar** em **Conjuntos de Membros Dinâmicos**.
- b Selecione se deseja correspondências com **Qualquer** ou **Todos** os critérios da sua instrução.
- c Insira o primeiro objeto a ser correspondido.

As opções são **Marca de Segurança**, **Nome do SO Convidado da VM**, **Nome da VM** e **Nome do Host Convidado da VM**.

- d Selecione um operador, como **Contém**, **Começa com** ou **Termina com**.
- e Insira um valor.
- f (Opcional) Para adicionar outra instrução, use um operador booleano **And** ou **Or**.

### 6 (Opcional) Edite um conjunto de membros dinâmicos clicando no ícone **Editar** ao lado do conjunto de membros que você deseja editar.

- a Aplique as alterações necessárias ao conjunto de membros dinâmico.
- b Clique em **OK**.

### 7 (Opcional) Exclua um conjunto de membros dinâmico clicando no ícone **Excluir** ao lado do conjunto de membros que você deseja excluir.

### 8 (Opcional) Edite a lista de membros incluídos clicando no ícone **Editar** ao lado da lista Incluir Membros.

- a No menu suspenso **Navegar por objetos do tipo**, selecione o tipo de objeto, como **Máquinas Virtuais**, **Redes de VDC da organização**, **Conjuntos de IPs**, **Conjuntos de MACs** ou **Marcas de segurança**.
- b Para incluir um objeto na lista Incluir Membros, selecione-o no painel esquerdo e mova-o até o painel direito clicando na seta para a direita.
- c Para excluir um objeto da lista Incluir Membros, selecione-o no painel direito e mova-o até o painel esquerdo clicando na seta para a esquerda.

- 9 (Opcional) Edite a lista de membros excluídos clicando no ícone **Editar** ao lado da lista Excluir Membros.
  - a No menu suspenso **Navegar por objetos do tipo**, selecione o tipo de objeto, como **Máquinas Virtuais, Redes de VDC da organização, Conjuntos de IPs, Conjuntos de MACs** ou **Marcas de segurança**.
  - b Para incluir um objeto na lista Excluir Membros, selecione-o no painel esquerdo e mova-o até o painel direito clicando na seta para a direita.
  - c Para excluir um objeto da lista Excluir Membros, selecione-o no painel direito e mova-o até o painel esquerdo clicando na seta para a esquerda.

**10** Clique em **Salvar alterações**.

As alterações no grupo de segurança são salvas.

## Excluir um grupo de segurança

Você pode excluir um grupo de segurança definido pelo usuário.

### Procedimentos

- 1 Abra os Serviços de Segurança.
  - a Navegue até **Rede > Segurança**.
  - b Selecione o VDC de organização ao qual você deseja aplicar configurações de segurança e clique em **Configurar Serviços**.

O portal do tenant abre Serviços de Segurança.
- 2 Navegue até **Objetos de Agrupamento > Grupos de Segurança**

A página **Grupos de Segurança** é aberta.
- 3 Selecione o grupo de segurança que você deseja excluir.
- 4 Clique no botão **Excluir**.
- 5 Para confirmar a exclusão, clique em **OK**.

### Resultados

O grupo de segurança é excluído.

## Gerenciando Edge Gateways do NSX-T Data Center

Um edge gateway do NSX-T Data Center fornece uma rede de VDCs de organização roteada ou uma rede de grupos de centros de dados com conectividade com redes externas e propriedades de gerenciamento de IP. Ele também pode fornecer serviços como firewall, conversão de endereços de rede (NAT), VPN IPSec, encaminhamento de DNS e DHCP, que estão ativados por padrão.

## Redes externas dedicadas

Para fornecer uma topologia de rede totalmente roteada em um centro de dados virtual, seu **administrador do sistema** pode dedicar uma rede externa a um edge gateway específico do NSX-T Data Center.

Nessa configuração, existe uma relação de um para um entre a rede externa e o edge gateway do NSX-T Data Center e outro edge gateway não pode se conectar à rede externa.

Um roteador lógico de camada 0 ou um gateway VRF do NSX-T Data Center associado a uma rede externa dedicada faz parte da pilha de rede do tenant. A rede externa é considerada uma parte do domínio de roteamento da rede do VMware Cloud Director.

Uma rede externa dedicada fornece serviços de roteamento adicionais do edge gateway, como o gerenciamento de aviso de rota e a configuração do protocolo de gateway de borda (BGP).

Você pode decidir quais das redes estão conectadas ao edge gateway para avisar à rede externa. Isso possibilita uma mistura de redes de centros de dados virtuais de organizações roteadas e totalmente roteadas por NAT.

## Adicionar um conjunto de IPs a um edge gateway do NSX-T Data Center

Para criar regras de firewall e adicioná-las a um edge gateway do NSX-T Data Center, você deve primeiro criar os conjuntos de IPs. Conjuntos de IPs são grupos de objetos aos quais se aplicam as regras de firewall. A combinação de vários objetos em conjuntos de IPs ajuda a reduzir o número total de regras de firewall a serem criadas.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T.
- 3 Em **Segurança**, clique na guia **Conjuntos de IPs** e em **Novo**.
- 4 Insira um nome e, se desejar, uma descrição para o conjunto de IPs.
- 5 Insira um endereço IP ou um intervalo de endereços IP para as máquinas virtuais que o conjunto de IPs inclui e clique em **Adicionar**.
- 6 Para salvar o grupo de firewalls, clique em **Salvar**.

### Resultados

Você criou um conjunto de IPs e o adicionou ao edge gateway do NSX-T.

### Próximo passo

[Adicionar uma regra de firewall do edge gateway do NSX-T Data Center](#)

## Adicionar uma regra de firewall do edge gateway do NSX-T Data Center

Para controlar o tráfego de rede de entrada e de saída referente a um edge gateway do NSX-T Data Center, crie regras de firewall.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Se a tela **Firewall** ainda não estiver visível na seção **Serviços**, clique na guia **Firewall**.
- 4 Clique em **Editar Regras**.
- 5 Clique no botão **Novo no Topo**.

Uma linha para a nova regra é adicionada acima da regra selecionada.

- 6 Configure a regra de firewall.

Opção	Descrição
<b>Nome</b>	Digite um nome para a regra.
<b>Estado</b>	Para ativar a regra após a criação, ligue o botão de alternância <b>Estado</b> .
<b>Aplicativos</b>	(Opcional) Para selecionar um perfil de porta específico ao qual a regra se aplica, ative a opção <b>Aplicativos</b> e clique em <b>Salvar</b> .
<b>Origem</b>	<p>Selecione uma opção e clique em <b>Manter</b>.</p> <ul style="list-style-type: none"> <li>■ Para permitir ou recusar o tráfego de qualquer endereço de origem, ative a opção <b>Qualquer Origem</b>.</li> <li>■ Para permitir ou negar o tráfego de grupos de firewall específicos, selecione os grupos de firewall na lista.</li> </ul>
<b>Destino</b>	<p>Selecione uma opção e clique em <b>Manter</b>.</p> <ul style="list-style-type: none"> <li>■ Para permitir ou negar o tráfego para qualquer endereço de destino, ative a opção <b>Qualquer Destino</b>.</li> <li>■ Para permitir ou recusar o tráfego de grupos de firewall específicos, selecione os grupos de firewall na lista.</li> </ul>
<b>Ação</b>	<p>No menu suspenso <b>Ação</b>, selecione uma opção.</p> <ul style="list-style-type: none"> <li>■ Para permitir o tráfego de ou para as origens, os destinos e os serviços especificados, selecione <b>Aceitar</b>.</li> <li>■ Para bloquear o tráfego proveniente de ou em direção a origens, destinos e serviços especificados, sem notificar o cliente bloqueado, selecione <b>Descartar</b>.</li> <li>■ Para bloquear o tráfego proveniente de ou em direção a origens, destinos e serviços especificados e notificar o cliente bloqueado de que o tráfego foi rejeitado, selecione <b>Rejeitar</b>.</li> </ul>
<b>Protocolo IP</b>	Selecione se deseja aplicar a regra ao tráfego IPv4 ou IPv6.

Opção	Descrição
Direção	Selecione a direção do tráfego à qual aplicar a regra.  <b>Observação</b> No VMware Cloud Director 10.2.1 e versões posteriores, essa opção não está mais disponível.
Ativar log.	Para que a conversão de endereços realizada por essa regra seja registrada, ative a opção <b>Ativar o log</b> .

7 Clique em **Salvar**.

8 Para configurar regras adicionais, repita essas etapas.

### Resultados

Depois de criadas, as regras de firewall são exibidas na lista Regras de Firewall do Edge Gateway. Você pode mover as regras para cima ou para baixo e pode editá-las ou excluí-las conforme necessário.

## Adicionar uma regra de SNAT ou DNAT a um edge gateway do NSX-T

Para alterar o endereço IP de origem de público para privado, crie uma regra de NAT de origem (SNAT). Para alterar o endereço IP de destino de um endereço IP público para privado, crie uma regra NAT (DNAT) de destino.

Ao configurar uma regra de SNAT ou de DNAT em um edge gateway no ambiente do VMware Cloud Director, você sempre configura a regra da perspectiva do VDC da sua organização.

Uma regra de SNAT converte o endereço IP de origem dos pacotes enviados de uma rede de VDC da organização em uma rede externa ou em outra rede de VDC da organização.

Uma regra NO SNAT impede a conversão do endereço IP interno de pacotes enviados de um VDC de organização para uma rede externa ou para outra rede VDC de organização.

Uma regra de DNAT converte o endereço IP (e, opcionalmente, a porta) de pacotes recebidos por uma rede de VDC da organização provenientes de uma rede externa ou de outra rede de VDC da organização.

Uma regra NO DNAT impede a conversão do endereço IP externo de pacotes recebidos por um VDC de organização de uma rede externa ou de outra rede VDC de organização.

VMware Cloud Director oferece suporte à redistribuição de rota automática quando você usa serviços NAT em um Edge Gateway NSX-T Data Center.

**Importante** Se estiver usando clusters Tanzu Kubernetes, anote a regra de SNAT do sistema criada no edge gateway para evitar a criação de uma regra conflitante.

### Pré-requisitos

Os endereços IP públicos devem ter sido adicionados à interface do edge gateway na qual você deseja adicionar a regra.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway e, em **Serviços**, clique em **NAT**.
- 3 Para adicionar uma regra, clique em **Novo**.
- 4 Configure uma regra SNAT ou NO SNAT (dentro para fora).

Opção	Descrição
Nome	Insira um nome significativo para a regra.
Descrição	(Opcional) Insira uma descrição para a regra.
Tipo de interface	No menu suspenso, selecione SNAT ou NO SNAT.
IP Externo	<p>Dependendo do tipo de regra que você está criando, escolha uma das opções.</p> <ul style="list-style-type: none"><li>■ Se você estiver criando uma regra SNAT, insira o endereço IP público do edge gateway para o qual está configurando a regra SNAT.</li><li>■ Se você estiver criando uma regra NO SNAT, deixe a caixa de texto vazia.</li></ul>
IP Interno	Insira o endereço IP ou uma lista de endereços IP das máquinas virtuais para as quais você está configurando o SNAT, para que elas possam enviar o tráfego para a rede externa.



Opção	Descrição
IP de Destino	(Opcional) Se quiser que a regra seja aplicada apenas ao tráfego para um domínio específico, insira um endereço IP para esse domínio ou uma lista de endereços IP. Se você deixar esta caixa de texto em branco, a regra SNAT se aplicará a todos os destinos fora da sub-rede local.
Configurações Avançadas (opcionais)	<p>Clique na guia <b>Configurações Avançadas</b> para obter algumas configurações adicionais.</p> <p><b>Estado</b></p> <p>Para ativar a regra na criação, ative para a opção <b>Estado</b>.</p> <p><b>Log</b></p> <p>Para que a conversão de endereço realizada por esta regra seja registrada, ative a opção <b>Log</b>.</p> <p><b>Prioridade</b></p> <p>Se um endereço tiver várias regras de NAT, você poderá atribuir diferentes prioridades a essas regras para determinar a ordem em que elas são aplicadas. Um valor inferior significa uma prioridade mais alta para a regra em questão.</p> <p><b>Correspondência de Firewall</b></p> <p>Você pode definir uma regra de correspondência de firewall para determinar como o firewall é aplicado durante a NAT. No menu suspenso, selecione uma das seguintes opções.</p> <ul style="list-style-type: none"> <li>■ Para aplicar regras de firewall ao endereço interno de uma regra de NAT, selecione <b>Corresponder Endereço Interno</b>.</li> <li>■ Para aplicar regras de firewall ao endereço externo de uma regra de NAT, selecione <b>Corresponder Endereço Externo</b>.</li> <li>■ Para ignorar a aplicação de regras de firewall, selecione <b>Ignorar</b>.</li> </ul>

## 5 Configure uma regra DNAT ou NO DNAT (fora para dentro).

Opção	Descrição
Nome	Insira um nome significativo para a regra.
Descrição	(Opcional) Insira uma descrição para a regra.
Tipo de interface	No menu suspenso, selecione DNAT ou NO DNAT.
IP Externo	<p>Insira o endereço IP público do edge gateway para o qual você está configurando a regra de DNAT.</p> <p>Os endereços IP inseridos devem ser subalocados para o edge gateway.</p>
Porta Externa	(Opcional) Insira uma porta na qual a regra de DNAT está convertendo os pacotes de entrada para as máquinas virtuais.

Opção	Descrição
IP Interno	<p>Dependendo do tipo de regra que você está criando, escolha uma das opções.</p> <ul style="list-style-type: none"> <li>■ Se você estiver criando uma regra DNAT, insira o endereço IP ou uma lista de endereços IP das máquinas virtuais para as quais você está configurando o DNAT, para que elas possam receber o tráfego da rede externa.</li> <li>■ Se você estiver criando uma regra NO DNAT, deixe a caixa de texto vazia.</li> </ul>
Aplicativo	<p>(Opcional) Selecione um perfil de porta de aplicação específico ao qual aplicar a regra.</p> <p>O perfil da porta de aplicação inclui uma porta e um protocolo que o tráfego de entrada utiliza no edge gateway para se conectar à rede interna.</p>
Configurações Avançadas (opcionais)	<p>Clique na guia <b>Configurações Avançadas</b> para obter algumas configurações adicionais.</p> <p><b>Estado</b></p> <p>Para ativar a regra na criação, ative para a opção <b>Estado</b>.</p> <p><b>Log</b></p> <p>Para que a conversão de endereço realizada por esta regra seja registrada, ative a opção <b>Log</b>.</p> <p><b>Prioridade</b></p> <p>Se um endereço tiver várias regras de NAT, você poderá atribuir diferentes prioridades a essas regras para determinar a ordem em que elas são aplicadas. Um valor inferior significa uma prioridade mais alta para a regra em questão.</p> <p><b>Correspondência de Firewall</b></p> <p>Você pode definir uma regra de correspondência de firewall para determinar como o firewall é aplicado durante a NAT. No menu suspenso, selecione uma das seguintes opções.</p> <ul style="list-style-type: none"> <li>■ Para aplicar regras de firewall ao endereço interno de uma regra de NAT, selecione <b>Corresponder Endereço Interno</b>.</li> <li>■ Para aplicar regras de firewall ao endereço externo de uma regra de NAT, selecione <b>Corresponder Endereço Externo</b>.</li> <li>■ Para ignorar a aplicação de regras de firewall, selecione <b>Ignorar</b>.</li> </ul>

6 Clique em **Salvar**.

7 Para configurar regras adicionais, repita essas etapas.

## Configurar um serviço de encaminhador de DNS em um edge gateway do NSX-T

Para encaminhar consultas DNS para servidores DNS externos, configure um encaminhador de DNS.

Como parte da configuração do serviço de encaminhador de DNS, você também pode adicionar zonas de encaminhador condicionais. Uma zona de encaminhador condicional é configurada como uma lista contendo até cinco zonas DNS FQDN. Se uma consulta DNS corresponder a um nome de domínio dessa lista, a consulta será encaminhada para os servidores da zona de encaminhador correspondente.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway e, em **Gerenciamento de IP**, clique em **DNS**.
- 3 Na seção **Encaminhador de DNS**, clique em **Editar**.
- 4 Para ativar o serviço de Encaminhador de DNS, ative a opção **Estado**.
- 5 Insira um nome e, opcionalmente, uma descrição para a zona DNS padrão.
- 6 Insira um ou mais endereços IP de servidor upstream, separados por vírgula.
- 7 Clique em **Salvar**.
- 8 (Opcional) Adicione uma zona de encaminhador condicional.
  - a Na seção **Zona de Encaminhador Condicional**, clique em **Adicionar**.
  - b Insira um nome para a zona de encaminhador.
  - c Insira um ou mais endereços IP de servidor upstream, separados por vírgula.
  - d Insira um ou mais nomes de domínio, separados por vírgula, e clique em **Salvar**.

## Criar perfis de portas de aplicativos personalizados

Para criar regras de firewall e NAT, você pode usar perfis de portas de aplicativos pré-configurados e perfis de portas de aplicativos personalizados.

Os perfis de portas de aplicativo incluem uma combinação de um protocolo e uma porta, ou um grupo de portas, que é usado para serviços de firewall e NAT no edge gateway. Além dos perfis de portas padrão que são pré-configurados para o NSX-T Data Center, você pode criar perfis de portas de aplicativos personalizados.

Quando você cria um perfil de porta de aplicativo personalizado em um edge gateway, ele fica visível para todos os outros edge gateways do NSX-T Data Center que estão no mesmo VDC de organização.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Segurança**, clique em **Perfis de Porta de Aplicativo**.
- 4 Na seção **Aplicativos Personalizados**, clique em **Novo**.
- 5 Insira um nome e, opcionalmente, uma descrição para o perfil de porta de aplicativo.

- 6 Selecione um protocolo no menu suspenso.
- 7 Insira uma porta ou um intervalo de portas, separados por vírgula, e clique em **Salvar**.

#### Próximo passo

Use perfis de portas de aplicativo para criar regras de firewall e NAT. Consulte [Adicionar uma regra de firewall do edge gateway do NSX-T Data Center](#) e [Adicionar uma regra de SNAT ou DNAT a um edge gateway do NSX-T](#).

## VPN baseada em políticas IPsec para edge gateways do NSX-T Data Center

A partir da versão 10.1, o VMware Cloud Director oferece suporte à VPN IPsec baseada em política de site a site entre uma instância do edge gateway do NSX-T Data Center e um site remoto.

A VPN IPsec oferece conectividade site a site entre um edge gateway e sites remotos que também usam o NSX-T Data Center ou que têm roteadores de hardware de terceiros ou gateways de VPN que oferecem suporte ao IPsec.

A VPN IPsec baseada em política exige que uma política de VPN seja aplicada aos pacotes para determinar qual tráfego deve ser protegido pelo IPsec antes de passar por um túnel VPN. Esse tipo de VPN é considerado estático porque, quando uma topologia de rede local e uma configuração mudam, as configurações de política de VPN também devem ser atualizadas para acomodar as alterações.

Os edge gateways do NSX-T Data Center oferecem suporte à configuração de túnel dividido, com o tráfego IPsec que realiza a precedência de roteamento.

O VMware Cloud Director oferece suporte à redistribuição automática de rotas quando você usa uma VPN IPsec em um edge gateway NSX-T.

### Configurar VPN IPsec baseada em política do NSX-T

Você pode configurar a conectividade entre sites entre um edge gateway do NSX-T Data Center e sites remotos. Os sites remotos devem usar NSX-T Data Center, ter roteadores de hardware de terceiros ou gateways VPN que oferecem suporte ao IPsec.

O VMware Cloud Director oferece suporte à redistribuição automática de rotas quando você configura uma VPN IPsec em um edge gateway do NSX-T Data Center.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Serviços**, clique em **VPN IPsec**.
- 4 Para configurar um túnel VPN IPsec, clique em **Novo**.
- 5 Insira um nome e, opcionalmente, uma descrição para o túnel VPN IPsec.

- 6 Para ativar o túnel na criação, ative a opção **Ativado**.
- 7 Escolha uma chave pré-compartilhada a ser inserida.

---

**Observação** A chave pré-compartilhada deve ser a mesma na outra extremidade do túnel VPN IPSec.

---

- 8 Insira um dos endereços IP que estão disponíveis para o edge gateway do endpoint local.

---

**Observação** O endereço IP deve ser o IP primário do edge gateway ou um endereço IP que é alocado separadamente a esse edge gateway a partir da rede externa.

---

- 9 Insira pelo menos um endereço de sub-rede IP local na notação CIDR a ser usada para o túnel VPN IPSec.
- 10 Insira o endereço IP para o local remoto.
- 11 Insira pelo menos um endereço de sub-rede IP remoto na notação CIDR para usar para o túnel VPN IPSec.
- 12 (Opcional) Para ativar o registro em log, ative a opção **Log**.
- 13 Clique em **Salvar**.
- 14 Para verificar se o túnel está funcionando, selecione-o e clique em **Exibir Estatísticas**.

Se o túnel estiver funcionando, **Status do Túnel** e **Status do Serviço do IKE** exibem Para cima.

## Resultados

O túnel VPN IPSec recém-criado está listado na exibição **VPN IPSec**. O túnel VPN IPSec é criado com um perfil de segurança padrão.

## Próximo passo

Você pode editar as configurações de túnel VPN IPSec e personalizar o perfil de segurança conforme necessário.

## Personalizar o perfil de segurança de um túnel VPN IPSec

Se você decidir não usar o perfil de segurança gerado pelo sistema que foi atribuído ao seu túnel VPN IPSec após a criação, poderá personalizá-lo.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Serviços**, clique em **VPN IPSec**.
- 4 Selecione o túnel VPN IPSec e clique em **Personalização do Perfil de Segurança**.

## 5 Configure os perfis IKE.

Os perfis Internet Key Exchange (IKE) fornecem informações sobre os algoritmos que são usados para autenticar, criptografar e estabelecer um segredo compartilhado entre os sites de rede quando você estabelece um túnel IKE.

- a Selecione uma versão do protocolo IKE para configurar uma associação de segurança (SA) no conjunto de protocolos IPSec.

Opção	Descrição
<b>IKEv1</b>	Quando você seleciona essa opção, a VPN IPSec inicia e responde somente ao protocolo IKEv1.
<b>IKEv2</b>	A opção padrão. Quando você seleciona esta versão, a VPN IPSec é iniciada e responde somente ao protocolo IKEv2.
<b>IKE-Flex</b>	Quando você seleciona essa opção, se o estabelecimento do túnel falhar com o protocolo IKEv2, o site de origem não retornará e iniciará uma conexão com o protocolo IKEv1. Em vez disso, se o site remoto iniciar uma conexão com o protocolo IKEv1, a conexão será aceita.

- b Selecione um algoritmo de criptografia com suporte a ser usado durante a negociação de Internet Key Exchange (IKE).
- c No menu suspenso **Resumo**, selecione um algoritmo de hashing seguro para usar durante a negociação IKE.
- d No menu suspenso **Grupo Diffie-Hellman**, selecione um dos esquemas de criptografia que permite que o site de mesmo nível e o edge gateway estabeleçam um segredo compartilhado em um canal de comunicação não seguro.
- e (Opcional) Na caixa de texto **Vida Útil da Associação**, modifique o número padrão de segundos antes que o túnel IPSec precise restabelecer.

## 6 Configure o túnel VPN IPSec.

- a Para ativar o Perfect Forward Secrecy, ative a opção.
- b Selecione uma política de desfragmentação.

A política de desfragmentação ajuda a lidar com bits de desfragmentação presentes no pacote interno.

Opção	Descrição
<b>Copiar</b>	Copia o bit de desfragmentação do pacote IP interno para o pacote externo.
<b>Limpar</b>	Ignora o bit de desfragmentação presente no pacote interno.

- c Selecione um algoritmo de criptografia com suporte a ser usado durante a negociação de Internet Key Exchange (IKE).
- d No menu suspenso **Resumo**, selecione um algoritmo de hashing seguro para usar durante a negociação IKE.

- e No menu suspenso **Grupo Diffie-Hellman**, selecione um dos esquemas de criptografia que permite que o site de mesmo nível e o edge gateway estabeleçam um segredo compartilhado em um canal de comunicação não seguro.
  - f (Opcional) Na caixa de texto **Vida Útil da Associação**, modifique o número padrão de segundos antes que o túnel IPsec precise restabelecer.
- 7 (Opcional) Na caixa de texto **Intervalo de Teste**, modifique o número padrão de segundos para a detecção de pares inativos.
- 8 Clique em **Salvar**.

## Resultados

No modo de exibição VPN IPsec, o perfil de segurança do túnel VPN IPsec é exibido como **Definido pelo Usuário**.

## Configurar serviços de rede externa dedicada

Para fornecer uma topologia de rede totalmente roteada em um centro de dados virtual, um **administrador do sistema** pode dedicar uma rede externa a um edge gateway específico do NSX-T Data Center.

Quando você usa uma rede externa dedicada, é possível configurar serviços de roteamento adicionais, como o gerenciamento de aviso de rota e a configuração do protocolo de gateway de borda (BGP).

## Procedimentos

### 1 Gerenciar aviso de rota

Usando o aviso de rota, você pode criar um ambiente de rede totalmente roteado em um centro de dados virtual de organização (VDC).

### 2 Definir configurações gerais de BGP

Você pode configurar uma conexão externa ou interna do Protocolo de Gateway de Borda (eBGP ou iBGP) entre um edge gateway do NSX-T Data Center que tenha uma rede externa dedicada e um roteador em sua infraestrutura física.

### 3 Criar uma lista de prefixos de IP

Você pode criar listas de prefixos de IP que contêm um ou vários endereços IP. Você usa as listas de prefixos de IP para atribuir vizinhos BGP com permissões de acesso para aviso de rota.

### 4 Adicionar um vizinho BGP

Você pode definir configurações individuais para os vizinhos de roteamento BGP quando adicioná-los.

## Gerenciar aviso de rota

Usando o aviso de rota, você pode criar um ambiente de rede totalmente roteado em um centro de dados virtual de organização (VDC).

Você pode decidir quais das sub-redes da rede que estão conectadas ao edge gateway do NSX-T Data Center para avisar à rede externa dedicada.

Se uma sub-rede não for adicionada ao filtro de aviso, a rota para ela não será avisada para a rede externa e a sub-rede permanecerá privada.

---

**Observação** O VMware Cloud Director avisa qualquer rede VDC da organização que se enquadre na rota anunciada. Por isso, você não precisa criar um filtro para cada sub-rede que faz parte de uma rede anunciada.

---

O aviso de rota é configurado automaticamente no edge gateway do NSX-T Data Center.

O VMware Cloud Director oferece suporte à redistribuição de rota automática quando você usa um aviso de rota em um edge gateway do NSX-T. A redistribuição de rota é automaticamente configurada no roteador lógico de camada 0 que representa a rede externa dedicada.

#### Pré-requisitos

- Verifique se o **administrador do sistema** dedicou uma rede externa a um edge gateway do NSX-T Data Center na sua organização.
- Verifique se você é um **administrador da organização** ou se recebeu uma função que inclui um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Roteamento**, clique em **Anúncio de Rota** e **Editar**.
- 4 Para adicionar uma sub-rede a ser avisada, clique em **Adicionar**.
- 5 Adicione uma sub-rede IPv4 ou IPv6.

Use o formato *network\_gateway\_IP\_address/subnet\_prefix\_length*, por exemplo, **192.167.1.1/24**.

## Definir configurações gerais de BGP

Você pode configurar uma conexão externa ou interna do Protocolo de Gateway de Borda (eBGP ou iBGP) entre um edge gateway do NSX-T Data Center que tenha uma rede externa dedicada e um roteador em sua infraestrutura física.

O BGP toma as decisões de roteamento principais usando uma tabela de redes IP ou prefixos, que designam várias rotas entre sistemas autônomos (AS).

O termo "BGP speaker" se refere a um dispositivo de rede que está executando o BGP. Dois "BGP speakers" estabelecem uma conexão antes que qualquer informação de roteamento seja trocada.



O termo vizinho BGP refere-se a um "BGP speaker" que estabeleceu essa conexão. Depois de estabelecer a conexão, os dispositivos trocam rotas e sincronizam suas tabelas. Cada dispositivo envia mensagens keep-alive para manter esta relação em funcionamento.

---

**Observação** Em um edge gateway que está conectado a uma rede externa com suporte de um gateway VRF, as configurações de número AS local e de reinicialização normal são somente leitura. O **administrador do sistema** pode editar essas configurações no gateway de camada 0 principal no NSX-T Data Center.

---

#### Pré-requisitos

- Verifique se o **administrador do sistema** dedicou uma rede externa a um edge gateway do NSX-T Data Center na sua organização.
- Verifique se você é um **administrador da organização** ou se recebeu uma função que inclui um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Roteamento**, clique em **BGP** e, em **Configuração**, clique em **Editar**.
- 4 Alterne a opção **Status** para ativar o BGP.
- 5 Insira um número de ID do sistema autônomo (AS) a ser usado para o recurso do AS local do protocolo.

O VMware Cloud Director atribui o número AS local ao edge gateway. O edge gateway anuncia essa ID quando ele se conecta com seus vizinhos BGP em outros sistemas autônomos.

- 6 No menu suspenso, selecione a opção **Modo de Reinicialização Normal**.

Opção	Descrição
<b>Reinicialização auxiliar e normal</b>	Não é uma prática recomendada ativar o recurso de reinicialização normal no edge gateway, pois os pares BGP de todos os gateways estão sempre ativos. Em caso de um failover, o recurso de reinicialização normal aumenta o tempo que um vizinho remoto leva para selecionar um gateway de camada 0 alternativo. Isso atrasa a convergência baseada em BFD.  <b>Observação</b> A configuração do edge gateway se aplica a todos os vizinhos BGP, a menos que a configuração específica do vizinho a substitua.
<b>Somente auxiliar</b>	Útil para reduzir ou eliminar a interrupção do tráfego associado às rotas aprendidas por um vizinho capaz de reiniciar normalmente. O vizinho deve ser capaz de preservar sua tabela de encaminhamento enquanto ela sofre uma reinicialização.
<b>Desabilitar</b>	Desative o modo de reinicialização normal no edge gateway.

- 7 (Opcional) Altere o valor padrão para o timer de reinicialização normal.

- 8 (Opcional) Altere o valor padrão para o timer de rota obsoleta.
- 9 Altere a opção **ECMP** para ativar o ECMP.
- 10 Clique em **Salvar**.

#### Próximo passo

- [Criar uma lista de prefixos de IP](#)
- [Adicionar um vizinho BGP](#)

## Criar uma lista de prefixos de IP

Você pode criar listas de prefixos de IP que contêm um ou vários endereços IP. Você usa as listas de prefixos de IP para atribuir vizinhos BGP com permissões de acesso para aviso de rota.

As listas de prefixos de IP são referenciadas por meio de filtros de vizinhos BGP para limitar o número de atualizações de BGP que são trocadas entre os pares BGP. Usando a filtragem de rota, você pode reduzir a quantidade de recursos do sistema necessários para as atualizações de BGP.

Por exemplo, você pode adicionar o endereço IP 192.168.100.3/27 à lista de prefixos de IP e negar que a rota seja redistribuída para o edge gateway.

Você também pode anexar um endereço IP com modificadores `less than or equal to (le)` e `greater than or equal to (ge)` para conceder ou limitar a redistribuição de rota. Por exemplo, os modificadores 192.168.100.3/27 ge 26 le 32 correspondem a máscaras de sub-rede maiores ou iguais a 26 bits e menores ou iguais a 32 bits de comprimento.

#### Pré-requisitos

- Verifique se o **administrador do sistema** dedicou uma rede externa a um edge gateway do NSX-T Data Center na sua organização.
- Verifique se você é um **administrador da organização** ou se recebeu uma função que inclui um conjunto equivalente de direitos.
- [Definir configurações gerais de BGP](#).

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Roteamento**, clique em **BGP** e em **Listas de Prefixos de IP**.
- 4 Para adicionar uma lista de prefixos de IP, clique em **Novo**.
- 5 Insira um nome e, opcionalmente, uma descrição para a lista de prefixos.
- 6 Clique em **Novo** e adicione uma notação CIDR ao prefixo.
- 7 No menu suspenso, selecione uma ação a ser aplicada ao prefixo.

- 8 (Opcional) Insira modificadores `greater than or equal to` e `less than or equal to` para conceder ou limitar a redistribuição de rota.

#### Próximo passo

- Você pode editar ou excluir a lista de prefixos de IP conforme necessário.
- Configure a filtragem de rotas. Consulte [Adicionar um vizinho BGP](#).

## Adicionar um vizinho BGP

Você pode definir configurações individuais para os vizinhos de roteamento BGP quando adicioná-los.

#### Pré-requisitos

- Verifique se o **administrador do sistema** dedicou uma rede externa a um edge gateway do NSX-T Data Center na sua organização.
- Verifique se você é um **administrador da organização** ou se recebeu uma função que inclui um conjunto equivalente de direitos.
- Verifique se você definiu as configurações globais de BGP para o edge gateway. Consulte [Definir configurações gerais de BGP](#).
- Se você usar a filtragem de rota, verifique se criou listas de prefixos de IP. Consulte [Criar uma lista de prefixos de IP](#).

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway.
- 3 Em **Roteamento**, clique em **BGP** e em **Vizinhos**.
- 4 Para adicionar um novo vizinho BGP, clique em **Novo**.
- 5 Insira as configurações gerais para o novo vizinho BGP.
  - a Insira um endereço IPv4 ou IPv6 para o novo vizinho BGP.
  - b Insira um número de Sistema Autônomo (AS) remoto no formato ASPLAIN.
  - c Insira um intervalo de tempo entre o envio de mensagens keep-alive para um par BGP.
  - d Insira um intervalo de tempo antes de declarar um par BGP inativo.

- e No menu suspenso, selecione a opção **Modo de Reinicialização Normal** para esse vizinho.

Opção	Descrição
<b>Desabilitar</b>	Substitui as configurações do edge gateway global e desativa o modo de reinicialização normal para esse vizinho.
<b>Somente auxiliar</b>	Substitui as configurações globais do edge gateway e configura o modo de reinicialização normal como <b>Somente auxiliar</b> para esse vizinho.
<b>Reinicialização normal e auxiliar</b>	Substitui as configurações globais do edge gateway e configura o modo de reinicialização normal como <b>Reinicialização normal e auxiliar</b> para esse vizinho.

- f Alterne o botão de **AllowAS-in** para habilitar o recebimento de rotas com o mesmo AS.
- g Se o vizinho BGP exigir autenticação, insira a senha para o vizinho BGP.
- 6 Defina as configurações da Detecção de Encaminhamento Bidirecional (BFD) para o novo vizinho BGP.
- a (Opcional) Alterne a opção **BFD** para habilitar o BFD para detecção de falha.
- b Na caixa de texto Intervalo de BFD, defina o intervalo de tempo para o envio de pacotes de heartbeat.
- c Na caixa de texto **Múltiplos Inativos**, insira o número de vezes que o vizinho BGP pode falhar ao enviar pacotes de heartbeat antes que o BFD declare que está inativo.
- 7 (Opcional) Configure a filtragem de rotas.
- a No menu suspenso **Família de Endereços IP**, selecione uma família de endereços IP.
- b Para configurar um filtro de entrada, selecione uma lista de prefixos de IP.
- c Para configurar um filtro de saída, selecione uma lista de prefixos de IP.
- 8 Clique em **Salvar**.

#### Próximo passo

Você pode exibir o status de cada vizinho BGP, editar ou excluir vizinhos BGP conforme necessário.

## Como trabalhar com o balanceamento de carga avançado do NSX

Como **administrador da organização**, ao configurar serviços virtuais que distribuem o tráfego em vários pools de servidores, você pode equilibrar as cargas de trabalho nos seus centros de dados com suporte pelo NSX-T Data Center.

A partir da versão 10.2, o VMware Cloud Director fornece serviços de balanceamento de carga usando os recursos do VMware NSX Advanced Load Balancer (Avi Networks).

O VMware Cloud Director oferece suporte ao balanceamento de carga L4 e L7 que você pode configurar em um edge gateway do NSX-T Data Center.

O balanceamento de carga de nível 4 (L4) direciona o tráfego com base em dados de protocolos de camada rede e de transporte, como o endereço IP e a porta TCP.

O balanceamento de carga de nível 7 (L7) distribui o tráfego com base em atributos como o cabeçalho HTTP, o identificador de recursos uniforme, o ID da sessão SSL e os dados do formulário HTML.

## Ativar o balanceador de carga em um Edge Gateway do NSX-T Data Center.

Antes que um **administrador da organização** possa configurar serviços de balanceamento de carga, um **administrador do sistema** deve ativar o balanceador de carga no edge gateway do NSX-T Data Center.

### Pré-requisitos

- Verifique se você é um **administrador do sistema**.
- Verifique se você integrou o VMware NSX Advanced Load Balancer na sua infraestrutura de nuvem. Para obter mais informações sobre como gerenciar o NSX Advanced Load Balancer, consulte *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T Data Center no qual você deseja ativar o balanceamento de carga.
- 3 Em Balanceador de Carga, clique em **Configurações Gerais**.
- 4 Clique em **Editar** e ative a opção **Estado do Balanceador de Carga**.
- 5 Insira um CIDR de rede para uma sub-rede da rede de serviços a partir da qual usar endereços IP para a criação de serviços virtuais.  
  
Você pode usar a sub-rede da rede de serviço padrão marcando a caixa de seleção **Usar Padrão**.

- 6 Clique em **Salvar**.

### Próximo passo

[Atribuir um grupo de mecanismos de serviço a um edge gateway do NSX-T Data Center.](#)

## Atribuir um grupo de mecanismos de serviço a um edge gateway do NSX-T Data Center

Antes que um **administrador da organização** possa configurar os serviços de balanceamento de carga em um edge gateway do NSX-T Data Center, um **administrador do sistema** deve atribuir um grupo de mecanismos de serviço ao edge gateway.

A infraestrutura de processamento de balanceamento de carga fornecida pelo NSX Advanced Load Balancer é organizada em grupos de mecanismos de serviço. Um **administrador do sistema** pode atribuir um ou mais grupos de mecanismos de serviço a um edge gateway do NSX-T Data Center.

Todos os grupos de mecanismos de serviço que são atribuídos a um único edge gateway usam a mesma rede de serviço.

#### Pré-requisitos

- Verifique se você é um **administrador do sistema**.
- [Ativar o balanceador de carga em um Edge Gateway do NSX-T Data Center..](#)

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T Data Center ao qual você deseja atribuir um grupo de mecanismos de serviço.
- 3 Em Balanceador de Carga, clique em **Grupos de Mecanismos de Serviço**.
- 4 Clique em **Adicionar**.
- 5 Selecione um grupo de mecanismos de serviço disponível na lista.
- 6 Insira um número para o número máximo de serviços virtuais que podem ser colocados no edge gateway.
- 7 Insira um número para os serviços virtuais garantidos disponíveis para o edge gateway.
- 8 Para confirmar as configurações, clique em **Salvar**.

### Editar as configurações de um grupo de mecanismos de serviço

Um **administrador do sistema** pode editar o número máximo de serviços virtuais compatíveis e o número de serviços virtuais reservados para um grupo de mecanismos de serviço.

Depois de sincronizar um grupo de mecanismos de serviço, se o novo número máximo de serviços virtuais compatíveis for menor que o número de serviços virtuais reservados, o grupo de mecanismos de serviço será marcado como superalocado.

Se um grupo de mecanismos de serviço estiver superalocado, a criação de um novo serviço virtual poderá falhar, mesmo que o edge gateway no qual você criar esse serviço virtual tenha capacidade reservada suficiente.

Para evitar falhas na criação de serviços virtuais, quando você edita as configurações de um grupo de mecanismos de serviço, não reduza o número máximo de serviços virtuais com suporte abaixo do número de serviços virtuais reservados inicialmente.

#### Pré-requisitos

- Verifique se você é um **administrador do sistema**.

- [Ativar o balanceador de carga em um Edge Gateway do NSX-T Data Center..](#)
- [Atribuir um grupo de mecanismos de serviço a um edge gateway do NSX-T Data Center.](#)

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T Data Center ao qual o grupo de mecanismos de serviço está atribuído.
- 3 Em Balanceador de Carga, clique em **Grupos de Mecanismos de Serviço**.
- 4 Clique em **Editar**.
- 5 Edite o número para os serviços virtuais máximos permitidos que o edge gateway pode usar.  
Não reduza o número, a menos que obrigatório. Caso contrário, você poderá se deparar com falhas ao criar serviços virtuais.
- 6 Edite o número para os serviços virtuais garantidos disponíveis para o edge gateway.
- 7 Clique em **Salvar**.

### Adicionar um pool de servidores do balanceador de carga

Um pool de servidores é um grupo de um ou mais servidores que você configura para executar o mesmo aplicativo e fornecer alta disponibilidade.

#### Pré-requisitos

- Verifique se você é um **administrador da organização**.
- Verifique se o **administrador do sistema** ativou o balanceamento de carga no edge gateway do NSX-T.
- Verifique se o **administrador do sistema** atribuiu pelo menos um grupo de mecanismos de serviço ao edge gateway.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T Data Center para o qual você deseja configurar um pool de balanceadores de carga.
- 3 Em Balanceador de Carga, clique em **Pools** e, em seguida, clique em **Adicionar**.

#### 4 Defina as configurações gerais para o pool de balanceadores de carga.

- a Insira um nome significativo e, opcionalmente, uma descrição para o pool de servidores.
- b Selecione um método de balanceamento de algoritmo.

O algoritmo de balanceamento de carga define como as conexões de entrada são distribuídas entre os membros do pool de servidores.

Opção	Descrição
<b>Menos conexões</b>	Novas conexões são enviadas ao servidor que atualmente tem o menor número de conexões.
<b>Round Robin</b>	Novas conexões são enviadas ao próximo servidor elegível no pool em ordem sequencial.
<b>Resposta mais rápida</b>	Novas conexões serão enviadas ao servidor que fornecer a resposta mais rápida para novas conexões ou solicitações.
<b>Hash consistente</b>	Novas conexões são distribuídas pelos servidores usando o endereço IP do cliente para gerar uma chave de hash de IP.
<b>Menor carga</b>	Novas conexões são enviadas ao servidor com a carga mais leve, independentemente do número de conexões que o servidor tem.
<b>Menos servidores</b>	Em vez de tentar distribuir todas as conexões ou solicitações em todos os servidores, o balanceador de carga determina o menor número de servidores necessários para satisfazer a carga atual do cliente.
<b>Aleatório</b>	O balanceador de carga seleciona os servidores aleatoriamente.
<b>Menos tarefas</b>	A carga é de balanceamento adaptável, com base no feedback do servidor.
<b>Afinidade de núcleos</b>	Cada núcleo de CPU usa um subconjunto de servidores, e cada servidor é usado por um subconjunto de núcleos. Essencialmente, ele fornece um mapeamento de muitos para muitos servidores e núcleos.

- c Para ativar o pool de servidores durante a criação, alterne para a opção **Estado**.
- d Insira uma porta do servidor de destino padrão a ser usada para o tráfego para o membro do pool.
- e (Opcional) Na caixa de texto **Tempo Limite de Desativação Normal**, insira o tempo máximo, em minutos, para desativar um membro do pool normalmente.

O serviço virtual aguarda o tempo especificado antes de fechar as conexões existentes com os membros desativados.



- f (Opcional) Para ativar um monitor de integridade passiva, ative a opção **Monitor de Integridade Passiva**.
- g (Opcional) Selecione um monitor de integridade ativo.

Opção	Descrição
HTTP	Uma solicitação HTTP e uma resposta são usadas para validar a integridade.
HTTPS	Usado em servidores da Web criptografados por HTTPS para validar a integridade.
TCP	Uma conexão TCP é usada para validar a integridade.
UDP	Um datagrama UDP é usado para validar a integridade.
PING	Um ping ICMP é usado para validar a integridade.

- 5 Adicione um membro ao pool de servidores.
  - a Clique na guia **Membros** e clique em **Adicionar**.
  - b Insira um endereço IP para o membro do pool.
  - c Ative a opção **Estado** para ativar o membro do pool.
  - d (Opcional) Adicione uma porta personalizada para o membro do pool de servidores.  
O número da porta padrão é a porta de destino que você inseriu para o pool.
  - e Insira uma proporção para o membro do pool.  
A proporção de cada membro de pool denota o tráfego que vai para cada membro do pool de servidores. Um servidor com uma proporção de 2 recebe o dobro de tráfego que um servidor com uma proporção de 1. O valor padrão é 1.
- 6 Na guia **Configurações de SSL**, defina as configurações de SSL para validar os certificados apresentados pelos membros do pool de balanceadores de carga.
  - a Para ativar a SSL, ative a opção **Ativação da SSL**.
  - b Para ocultar certificados com chaves privadas e ver apenas uma lista de certificados de autoridade de certificação, marque a caixa de seleção **Ocultar certificados de serviço**.
- 7 Para ativar a verificação de nome comum para certificados de servidor, ative a opção **Verificação de Nome Comum** e insira até 10 nomes de domínio para o pool.
- 8 Clique em **Salvar**.

Próximo passo

[Criar um serviço virtual.](#)

## Criar um serviço virtual

Um serviço virtual atende ao tráfego para um endereço IP, processa as solicitações do cliente e direciona as solicitações válidas a um membro do pool de servidores do balanceador de carga.

Um serviço virtual é uma combinação de um endereço IP e uma porta que usa um único protocolo de rede. O serviço virtual é anunciado para redes externas e está atendendo às solicitações de clientes. Quando um cliente se conecta ao serviço virtual, o balanceador de carga direciona a solicitação para um membro do pool de servidores do balanceador de carga que você configurou.

Para proteger a terminação SSL para um serviço virtual, você pode usar um certificado da biblioteca de certificados. Para obter mais informações, consulte [Importar certificados para a biblioteca de certificados](#).

#### Pré-requisitos

- Verifique se você é um **administrador da organização**.
- Verifique se o **administrador do sistema** ativou o balanceamento de carga no edge gateway do NSX-T.
- Verifique se o **administrador do sistema** atribuiu pelo menos um grupo de mecanismos de serviço ao edge gateway.
- [Adicionar um pool de servidores do balanceador de carga](#).

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Rede** e, depois, na guia **Edge gateways**.
- 2 Clique no edge gateway do NSX-T Data Center no qual você deseja criar um serviço virtual.
- 3 Em Balanceador de Carga, clique em **Serviços Virtuais** e, em seguida, clique em **Adicionar**.
- 4 Insira um nome significativo e, opcionalmente, uma descrição para o serviço virtual.
- 5 Para ativar o serviço virtual na criação, ative a opção **Ativado**.
- 6 Selecione um grupo de mecanismos de serviço para o serviço virtual.
- 7 Selecione um pool de balanceadores de carga para o serviço virtual.
- 8 Insira um endereço IP para o serviço virtual.
- 9 Selecione o tipo de serviço virtual.

Opção	Descrição
HTTP	O serviço virtual atende às solicitações HTTP de camada 7 não seguras. Quando você seleciona esse tipo de serviço, ele preenche automaticamente a caixa de texto da porta de serviço como 80, que pode substituir por outro número de porta válido.
HTTPS	O serviço virtual atende às solicitações de HTTPS de nível 7 seguras. Quando você seleciona esse tipo de serviço, ele preenche automaticamente a caixa de texto da porta de serviço como porta 443, que pode substituir por outro número de porta válido. Selecione um certificado SSL a ser usado para a terminação SSL.

Opção	Descrição
L4	<p>O serviço virtual atende às solicitações da camada 4.</p> <p>Quando você seleciona esse tipo de serviço, ele preenche automaticamente a caixa de texto da porta de serviço como 80, que pode substituir por outro número de porta válido.</p>
TLS L4	<p>O serviço virtual atende às solicitações do TLS de camada 4 seguras.</p> <p>Quando você seleciona esse tipo de serviço, ele preenche automaticamente a caixa de texto da porta de serviço como porta 443 do TCP, que pode substituir por outro número de porta válido. Selecione um certificado SSL a ser usado para a terminação SSL.</p>

**10** Clique em **Salvar**.

# Usando discos nomeados e revisando políticas de armazenamento

## 6

Você pode criar e gerenciar discos nomeados e revisar as políticas de armazenamento de datacenter virtual da organização usando o portal do tenant do VMware Cloud Director.

Este capítulo inclui os seguintes tópicos:

- [Criando e usando discos nomeados](#)
- [Revisar propriedades de políticas de armazenamento](#)

## Criando e usando discos nomeados

Discos nomeados são discos virtuais independentes que você cria em VDCs de organização.

**Administradores de organizações** e usuários que têm os respectivos direitos podem criar, remover e atualizar discos nomeados e conectá-los a máquinas virtuais.

Quando você cria um disco nomeado, ele é associado a um VDC de organização, mas não a uma máquina virtual. Depois de criar o disco em um VDC, o proprietário do disco ou um administrador pode anexá-lo a qualquer máquina virtual implantada no VDC. Se você tiver o direito **Criar Disco Compartilhado**, poderá criar um disco nomeado compartilhado para anexar a várias VMs. O proprietário do disco também pode modificar as propriedades do disco, desanexá-lo de uma máquina virtual e removê-lo do VDC. Os **administradores de sistema** e **administradores de organização** têm os mesmos direitos de usar e modificar o disco como o proprietário do disco.

---

**Observação** Embora o vSphere ofereça suporte a configurações como o Cluster de Failover do Windows Server (WSFC) e você possa criar um disco compartilhado por meio do compartilhamento do barramento SCSI físico, o VMware Cloud Director 10.2 não oferece suporte para esse recurso. Ao criar um disco compartilhado no VMware Cloud Director, você só cria um disco persistente independente subjacente no vSphere com o modo de vários gravadores ativado.

---

Se você anexar um disco nomeado, não será possível fazer snapshots de VMs. Se um disco compartilhado estiver anexado a uma VM, você não poderá editar sua configuração de disco rígido na exibição de detalhes da VM.

Se o VDC de organização tiver uma política de armazenamento com criptografia de VM habilitada, você poderá criptografar VMs e discos associando-os a políticas de armazenamento que têm o recurso de criptografia de VM. Consulte [Criptografia da máquina virtual](#).

## Criar um disco nomeado

Você pode criar um disco nomeado e anexá-lo a uma ou mais máquinas virtuais em um estágio posterior.

Para criar um disco nomeado, você deve especificar seu nome e tamanho. Como opção, você pode incluir uma descrição e selecionar um perfil de armazenamento a ser usado pelo disco. É possível criar um disco compartilhado que pode ser anexado a várias VMs.

---

**Observação** Embora o vSphere ofereça suporte a configurações como o Cluster de Failover do Windows Server (WSFC) e você possa criar um disco compartilhado por meio do compartilhamento do barramento SCSI físico, o VMware Cloud Director 10.2 não oferece suporte para esse recurso. Ao criar um disco compartilhado no VMware Cloud Director, você só cria um disco persistente independente subjacente no vSphere com o modo de vários gravadores ativado.

---

### Pré-requisitos

- 1 Você deve ter uma função de **administrador de organização** ou direitos de proprietário de disco.
- 2 Se quiser criar um disco compartilhado, você deverá ter o direito **Criar Disco Compartilhado**.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Armazenamento**, no painel esquerdo, selecione **Discos Nomeados**.
- 2 Clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição do disco.
- 4 Selecione a política de armazenamento no menu suspenso **Política de Armazenamento**.
- 5 Insira o tamanho do disco nomeado.
- 6 Selecione o tipo e o subtipo de barramento nos menus suspensos **Tipo de Barramento** e **Subtipo de Barramento**, respectivamente.
- 7 Se quiser anexar o disco nomeado a várias VMs, marque a caixa de seleção **Compartilhável**. Não será possível editar essa configuração mais tarde.
- 8 Clique em **Salvar**.

### Próximo passo

Use a API do VMware Cloud Director para anexar o disco independente a uma máquina virtual. Consulte *Guia de programação da API do VMware Cloud Director* no [VMware {code}](#).

## Editar um disco nomeado

Depois de criar o disco, você pode modificar seu nome, a descrição, sua política de armazenamento e o tamanho.

Não é possível editar a configuração **Compartilhável** de um disco nomeado.

#### Pré-requisitos

- 1 Você deve ter uma função de **administrador de organização** ou direitos de proprietário de disco.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Armazenamento**, no painel esquerdo, selecione **Discos Nomeados**.
- 2 Selecione o disco que você deseja modificar e clique em **Editar**.
- 3 Edite as configurações, como nome, descrição, política de armazenamento e tamanho.
- 4 Clique em **Salvar**.

## Anexar um disco nomeado a uma máquina virtual

Depois de criar um disco nomeado em um VDC, você pode anexá-lo a qualquer máquina virtual implantada no VDC. É possível anexar um disco nomeado compartilhado a várias VMs.

#### Pré-requisitos

Você deve ter uma função de **administrador de organização** ou direitos de proprietário de disco.

#### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Armazenamento**, no painel esquerdo, selecione **Discos Nomeados**.
- 2 Clique no botão de opção ao lado do nome do disco nomeado que você deseja anexar a uma máquina virtual e clique em **Anexar**.
- 3 No menu suspenso, selecione uma máquina virtual à qual anexar o disco nomeado e clique em **Aplicar**.
- 4 Se quiser anexar outra VM a um disco compartilhado, repita [Etapa 2](#) e [Etapa 3](#).

#### Próximo passo

Você pode anexar mais discos nomeados à VM ou desanexá-los conforme necessário.

## Excluir um disco nomeado

Se você não precisa de um disco nomeado, pode excluí-lo.

#### Pré-requisitos

Você deve ter uma função de **administrador de organização** ou direitos de proprietário de disco.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar e, em **Armazenamento**, no painel esquerdo, selecione **Discos Nomeados**.
- 2 Selecione o disco que você deseja excluir e clique em **Excluir**.
- 3 Clique em **OK**.

## Revisar propriedades de políticas de armazenamento

Você pode revisar as políticas de armazenamento e seus detalhes.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar.
- 2 Em **Armazenamento**, clique em **Políticas de Armazenamento**.  
É exibida a lista de políticas de armazenamento disponíveis.
- 3 Para visualizar os detalhes sobre uma política de armazenamento, clique no respectivo nome.
- 4 Revise os detalhes nas guias **Geral** e **Metadados** e clique em **OK**.

Você pode revisar o nome, o limite, as configurações de IOPS e os detalhes de metadados da política de armazenamento.

# Revisando e editando propriedades de centros de dados virtuais

## 7

Como **administrador da organização**, você pode revisar as propriedades do centro de dados virtual. Você também pode controlar o acesso a VDCs de organização por usuários e grupos na sua organização.

Este capítulo inclui os seguintes tópicos:

- [Revisar propriedades do data center virtual](#)
- [Revisar os metadados do data center virtual](#)
- [Limitar o acesso a um VDC de organização a usuários e grupos específicos na sua organização](#)

## Revisar propriedades do data center virtual

Você pode revisar as propriedades dos data centers virtuais que são atribuídos à sua organização.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar.
- 2 Em **Configurações**, clique em **Gerais**.

### Resultados

Você pode revisar as propriedades do data center virtual, como nome, descrição e status. As informações de métricas sobre o data center incluem o modelo de alocação e a vCPU, bem como a CPU e o uso de memória.

## Revisar os metadados do data center virtual

O VMware Cloud Director fornece uma instalação geral para a associação de metadados definidos pelo usuário a um objeto. Se o administrador do sistema tiver criado metadados para o data center virtual da organização, você poderá revisar esses metadados.



### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na tela do painel **Centro de Dados Virtual**, clique no cartão do centro de dados virtual que você deseja explorar.
- 2 Em **Configurações**, clique em **Metadados**.  
A lista dos metadados disponíveis é exibida.

## Limitar o acesso a um VDC de organização a usuários e grupos específicos na sua organização

Como **administrador da organização**, você pode limitar o acesso a cada um dos VDCs de organização na sua organização a usuários e grupos específicos.

Por padrão, VDCs de organização são compartilhados com todos os usuários e grupos que têm uma função com o direito **Permitir Acesso a Todos os VDCs de Organização**.

Se a sua organização tiver vários VDCs de organização e você quiser que eles sejam gerenciados separadamente, poderá criar uma função personalizada que funcionaria como um administrador de VDC de organização e atribuí-la a usuários ou grupos específicos dentro da sua organização, fornecendo a eles acesso somente aos recursos de processamento e rede de um VDC específico.

### Pré-requisitos

- 1 Verifique se você é um **administrador da organização**.
- 2 Crie uma função personalizada para os usuários e grupos aos quais você deseja fornecer acesso a um VDC de organização específico. Essa função deve excluir o direito **Permitir Acesso a Todos os VDCs de Organização**. Consulte [Capítulo 13 Gerenciar usuários, grupos e funções](#).

### Procedimentos

- 1 Na tela do painel **Data Center Virtual**, clique no cartão do centro de dados virtual ao qual você deseja limitar o acesso.
- 2 Em **Configurações**, clique em **Compartilhamento**.  
É exibida a lista de usuários e grupos na organização que têm acesso ao VDC.
- 3 Para alterar as configurações de acesso ao VDC de organização, clique em **Editar**.
- 4 Selecione **Usuários e Grupos Específicos**.
- 5 Na lista **Usuários**, selecione os usuários aos quais você deseja fornecer acesso ao VDC.
- 6 Na lista **Grupos**, selecione os grupos aos quais você deseja fornecer acesso ao VDC.

**7** Para compartilhar o VDC com os usuários e grupos selecionados, clique em **Compartilhar**.

#### **Resultados**

O acesso ao VDC de organização é limitado aos usuários e grupos que você selecionou.

# Como trabalhar com instâncias, endpoints e proxies dedicados do vCenter Server



Você pode acessar um ambiente dedicado do vCenter Server ou componentes do vCenter Server no VMware Cloud Director Tenant Portal.

## Centros de dados dedicados do vSphere

No VMware Cloud Director, um centro de dados definido por software (SDDC) encapsula todo um ambiente dedicado do vCenter Server.

Instâncias dedicadas do vCenter Server no VMware Cloud Director removem a exigência de que a instância do vCenter Server seja publicamente disponível.

O **administrador do sistema** pode publicar uma ou mais instâncias dedicadas do vCenter Server na sua organização. Você pode usar os endpoints para acessar a interface de usuário ou a API dos componentes com ou sem proxy.

## Endpoints

Uma instância dedicada do vCenter Server pode incluir um ou mais endpoints que fornecem acesso a diferentes componentes do ambiente subjacente. Os endpoints podem fornecer um ponto de acesso a um componente do centro de dados, como uma instância do vCenter Server, um host do ESXi, uma instância do NSX Manager ou uma instância do NSX-T Manager.

Os endpoints podem ou não estar conectados a um proxy.

## Proxies

O VMware Cloud Director pode atuar como um servidor proxy HTTPS e fornecer acesso a uma instância dedicada do vCenter Server e a diferentes componentes de instâncias compartilhadas ou dedicadas do vCenter Server que estão fazendo backup do ambiente.

Você pode fazer login na interface do usuário ou na API dos componentes com proxy usando sua conta do VMware Cloud Director.

Para acessar os componentes com proxy, você deve usar o Chrome Browser Extension for VMware Cloud Director ou configurar manualmente o navegador com as Configurações de proxy.

Este capítulo inclui os seguintes tópicos:

- [Usando o Chrome Browser Extension for VMware Cloud Director](#)
- [Configurar o navegador com as configurações de proxy](#)
- [Fazer login na interface de usuário de um componente usando um endpoint](#)

## Usando o Chrome Browser Extension for VMware Cloud Director

Você pode usar o Chrome Browser Extension for VMware Cloud Director para fazer login nos componentes do vSphere em proxy no seu ambiente.

O Chrome Browser Extension for VMware Cloud Director fornece configuração e autenticação de proxy.

O Chrome Browser Extension for VMware Cloud Director oferece suporte a ambientes multissite.

Você pode adicionar a extensão ao seu navegador Chrome na [Chrome Web Store](#).

## Configurar o navegador com as configurações de proxy

Antes de poder acessar a interface de usuário de um componente do vSphere com proxy, você deve configurar os proxies que estão publicados na sua organização.

Para configurar o navegador para usar seus proxies publicados, copie a URL do arquivo de configuração automática de proxy (PAC) no navegador.

---

**Observação** Quando o **administrador do sistema** publica um centro de dados do vSphere dedicado na sua organização, ou adiciona um proxy a um dos seus centros de dados do vSphere dedicados, talvez demore alguns minutos para que o navegador faça uma nova busca na PAC a partir da URL fornecida. Para forçar uma atualização do navegador, você pode repetir esse procedimento.

---

### Pré-requisitos

- Verifique se o **administrador do sistema** publicou pelo menos uma instância dedicada e habilitada do vCenter Server para a sua organização.
- Verifique se o **administrador do sistema** publicou os direitos **SDDC\_VIEW** e **Token: Gerenciar** para a sua organização e se a sua função inclui esses direitos.
- Verifique se o **administrador do sistema** publicou e ativou o plug-in de **Extensão CPOM** para a sua organização. Este plug-in fornece a função para exibir e usar centros de dados do vSphere dedicados no VMware Cloud Director Tenant Portal.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Centro de Dados** e clique em **Centro de Dados Virtual**.

- 2 No painel **Centros de Dados Dedicados do vSphere**, clique em **Clique aqui para exibir o Guia de Configuração do Proxy**.
- 3 Copie a URL da PAC e clique em **Próximo**.
- 4 Siga as instruções para configurar o navegador para apontar para a URL da PAC.
- 5 Se um componente em proxy estiver usando certificados autoassinados, importe os certificados para o seu navegador.
  - a No cartão do centro de dados do vSphere de destino, clique em **Ações** e clique em **Importar Certificado**.
  - b Baixe o certificado e a lista de revogação de certificados (CRL).
  - c Importe o certificado baixado para seu navegador.Consulte as instruções do usuário de seu navegador.

## Fazer login na interface de usuário de um componente usando um endpoint

Você pode usar endpoints para acessar a interface de usuário de componentes com proxy ou sem proxy com sua conta do VMware Cloud Director.

### Pré-requisitos

Se você quiser acessar um componente com proxy, [Configurar o navegador com as configurações de proxy](#) ou [Usando o Chrome Browser Extension for VMware Cloud Director](#) ao Google Chrome.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Centro de Dados** e clique em **Centro de Dados Virtual**.
- 2 Selecione a guia **Centros de Dados Dedicados do vSphere**.
- 3 Abra o endpoint da instância dedicada do vCenter Server.
  - Para abrir o endpoint padrão, clique em **Abrir o vSphere**.
  - Para abrir um endpoint não padrão, siga estas etapas:
    - Clique no menu **Ações** e clique em **Exibir Endpoints**.
    - Clique na URL do endpoint.

Se você estiver acessando um componente com proxy, será aberto um novo cartão com suas credenciais de proxy.

- 4 Se você estiver fazendo login em um componente com proxy, acesse o componente usando suas credenciais.
  - a Copie o nome de usuário e a senha.
  - b Para ativar o proxy, clique em **Abrir**.

Um novo cartão abre e solicita a autenticação no proxy.
  - c Na caixa de texto **Nome do Usuário** , cole o nome de usuário copiado.
  - d Na caixa de texto **Senha**, cole a senha copiada e clique em **OK**.

# Trabalhando com modelos de vApp

## 9

Um modelo vApp é uma imagem de máquina virtual carregada com um sistema operacional, aplicativos e dados. Esses modelos garantem que as máquinas virtuais sejam configuradas de forma consistente em toda a organização. Os modelos do vApp são adicionados aos catálogos.

Este capítulo inclui os seguintes tópicos:

- Visualizar um modelo de vApp
- Criar um modelo de vApp de um arquivo OVF
- Importar uma máquina virtual do vCenter Server como modelo do vApp
- Atribuir uma política de posicionamento de VM e uma política de dimensionamento de VM a um modelo vApp
- Baixar um modelo de vApp
- Excluir um modelo de vApp

## Visualizar um modelo de vApp

Você pode ver a lista de modelos de vApp que estão disponíveis nos catálogos aos quais você tem acesso. Você pode visualizar um modelo de vApp e explorar as máquinas virtuais que ele contém.

Você pode acessar somente os modelos de vApp incluídos em catálogos que foram compartilhados com você. Para obter mais informações sobre como compartilhar catálogos, consulte [Compartilhar um catálogo](#).

### Pré-requisitos


Esta operação requer os direitos incluídos na função predefinida de **autor do vApp** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.

A lista de modelos aparece em uma exibição de grade.


2 (Opcional) Configure a exibição de grade para conter os elementos que você deseja ver.

- a Na exibição de grade, clique no ícone do editor de grade (  ) abaixo da lista de modelos de vApp.
- b Selecione os elementos que você deseja incluir na exibição em grade, como versão, status, catálogo, proprietário e assim por diante.
- c Clique em **OK**.

A grade exibe os elementos selecionados para cada modelo de vApp na lista.

3 Para exibir as máquinas virtuais incluídas em um modelo de vApp, clique no nome do modelo de vApp.

As máquinas virtuais que o modelo de vApp inclui são exibidas em uma grade.

4 (Opcional) Para selecionar os elementos que você deseja ver na exibição em grade, clique no ícone do editor de grade (  ) abaixo da lista de máquinas virtuais.

- a Selecione os elementos que você deseja incluir na exibição em grade.
- b Clique em **OK**.

## Criar um modelo de vApp de um arquivo OVF

Você pode carregar um pacote OVF para criar um modelo vApp em um catálogo.

O VMware Cloud Director oferece suporte às especificações OVF (Open Virtualization Format) e OVA (Open Virtualization Appliance). Se você carregar um arquivo OVF que inclui propriedades OVF para personalizar suas máquinas virtuais, essas propriedades serão preservadas no modelo vApp. Para obter informações sobre como criar pacotes OVF, consulte o *Guia do usuário da ferramenta OVF Tool* e o *Guia do usuário do VMware vCenter Converter*.

### Pré-requisitos

Esta operação requer os direitos incluídos na função predefinida de **autor de catálogo** ou um conjunto equivalente de direitos.

### Procedimentos

1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.

A lista de modelos aparece em uma exibição de grade.

2 Clique em **Novo**.



- 3 Digite um endereço de URL do arquivo OVF ou clique no ícone **Carregar** para navegar até um local acessível do seu computador e selecionar o arquivo de modelo OVF/OVA.

O local pode ser seu disco rígido local, um compartilhamento de rede ou uma unidade de CD/DVD. As extensões de arquivo com suporte incluem `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` e `.strings`. Se você optar por carregar um arquivo OVF, que faz referência a mais arquivos do que você está tentando carregar, por exemplo, um arquivo VMDK, deverá procurar e selecionar todos os arquivos.

- 4 Verifique os detalhes do modelo OVF/OVA que você está prestes a implantar e clique em **Avançar**.
- 5 Insira um nome e, opcionalmente, uma descrição para o modelo de vApp e clique em **Avançar**.
- 6 No menu suspenso **Catálogo**, selecione o catálogo ao qual você deseja adicionar o modelo.
- 7 Revise as configurações do modelo de vApp e clique em **Concluir**.

#### Resultados

O novo modelo de vApp aparece na exibição em grade de modelos.

## Importar uma máquina virtual do vCenter Server como modelo do vApp

Se você tiver direitos de **administrador do sistema**, poderá importar VMs do vCenter Server para o VMware Cloud Director como modelos de vApp em catálogos.

#### Pré-requisitos

Para ver e importar VMs do vCenter Server como modelos de vApp, verifique se você tem direitos de **administrador do sistema**.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.  
A lista de modelos aparece em uma exibição de grade.
- 2 Clique em **Importar do vCenter**.
- 3 No menu suspenso, selecione uma instância do vCenter Server da qual um modelo do vApp é importado.
- 4 Selecione um modelo na lista de máquinas virtuais.
- 5 Insira um nome e, opcionalmente, uma descrição para o modelo do vApp.
- 6 No menu suspenso, selecione um catálogo ao qual o modelo do vApp é adicionado.
- 7 (Opcional) Para excluir a máquina virtual de origem, ative a opção **Mover Máquina Virtual**.

- 8 (Opcional) Marque o modelo do vApp como um modelo preferencial no catálogo.
- 9 Clique em **Importar**.

## Atribuir uma política de posicionamento de VM e uma política de dimensionamento de VM a um modelo vApp

Para associar as VMs de um modelo vApp com posicionamento de VM específico e políticas de dimensionamento de VM, você pode marcar VMs individuais de um modelo vApp com as políticas que deseja atribuir.

A partir do VMware Cloud Director 10.0, você pode permitir que os usuários alterem as políticas predefinidas de posicionamento ou dimensionamento de VM ao editarem uma VM.

---

**Observação** Depois de fazer upgrade para o VMware Cloud Director 10.0 ou posterior, todas as tags de modelo pré-existent se tornam modificáveis. Se quiser proibir as alterações nas políticas predefinidas de posicionamento ou dimensionamento de VM, você deverá desmarcar a caixa de seleção **Modificável** para as políticas que deseja manter intactas.

---

### Pré-requisitos

- Essa operação exige o direito de editar um modelo vApp.
- Verifique se você tem pelo menos um modelo vApp no seu ambiente VMware Cloud Director.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.  
  
A lista de modelos aparece em uma exibição de grade.
- 2 Selecione o botão de opção ao lado do modelo de vApp que você deseja marcar e clique em **Marcar com políticas de processamento**.
- 3 Se quiser atribuir uma política de posicionamento de VM a uma VM no modelo vApp, selecione uma política no menu suspenso **Política de Posicionamento de VM** na linha correspondente à VM.
- 4 Se quiser atribuir uma política de dimensionamento de VM a uma VM no modelo vApp, selecione uma política no menu suspenso **Política de Dimensionamento de VM** na linha correspondente à VM.
- 5 (Opcional) Para permitir que os usuários alterem as políticas de posicionamento ou dimensionamento de VM predefinidas durante a edição de uma VM, marque a caixa de seleção **Modificável** no menu suspenso da política.
- 6 Clique em **Marca**.

## Baixar um modelo de vApp

Você pode baixar um modelo de vApp de um catálogo como um arquivo OVA para sua máquina local.


### Pré-requisitos

Esta operação requer os direitos incluídos na função predefinida de **autor de catálogo** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.

A lista de modelos aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda do modelo de vApp que você deseja baixar e selecione **Baixar**.

---

**Observação** Você pode baixar modelos de vApp dos seus catálogos de organização. Se você for um administrador da organização, poderá baixar modelos de vApp de um catálogo público. Caso contrário, o botão **Baixar** ficará desativado.

---

- 3 (Opcional) Para preservar os UUIDs e os endereços MAC das máquinas virtuais no pacote OVA baixado, marque a caixa de seleção **Preservar informações de identidade**.
- 4 Clique em **OK** e aguarde a conclusão do download.

O arquivo OVA é salvo no local de download padrão do navegador da Web.

## Excluir um modelo de vApp

Você pode excluir um modelo de vApp de um catálogo da organização. Se o catálogo for publicado, o modelo de vApp também será excluído de catálogos públicos.


### Pré-requisitos

Esta operação requer os direitos incluídos na função predefinida de **autor do vApp** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos do vApp**.

A lista de modelos aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda do modelo de vApp que você deseja excluir e selecione **Excluir**.

**3** Confirme a exclusão.

O modelo de vApp excluído é removido da exibição em grade.

# Trabalhando com arquivos de mídia

# 10

O catálogo permite carregar, copiar, mover e editar as propriedades dos arquivos de mídia.

Este capítulo inclui os seguintes tópicos:

- Carregar arquivos de mídia
- Excluir um arquivo de mídia
- Baixar um arquivo de mídia

## Carregar arquivos de mídia

Você pode carregar novos arquivos de mídia ou novas versões de arquivos de mídia existentes em um catálogo. Os usuários com acesso ao catálogo podem abrir os arquivos de mídia com suas máquinas virtuais.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Mídia e Outros**.

A lista de arquivos de mídia aparece em uma exibição de grade.

- 2 Clique em **Adicionar**.

- 3 No menu suspenso **Catálogo**, selecione um catálogo no qual você deseja carregar o arquivo de mídia.

- 4 Insira um nome para o arquivo de mídia.

Se você não inserir um nome, a caixa de texto de nome será preenchida automaticamente após o nome do arquivo de mídia.

- 5 Clique no ícone de carregamento para procurar e selecionar o arquivo de imagem de disco, por exemplo, um arquivo `.iso`.

## 6 Clique em **OK**.

Após o início do carregamento, o arquivo de mídia aparecerá na grade.

### Próximo passo

Dependendo do tamanho do arquivo, a conclusão do carregamento poderá demorar um pouco. Monitore o status do carregamento no modo de exibição de **Tarefas recentes**. Para obter mais informações, consulte [Exibir tarefas](#).

## Excluir um arquivo de mídia

Você pode excluir arquivos de mídia que não deseja mais usar do seu catálogo.


### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Mídia e Outros**.

A lista de arquivos de mídia aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda do arquivo de mídia que você deseja excluir e selecione **Excluir**.

- 3 Confirme a exclusão.

O arquivo de mídia excluído é removido da exibição em grade.

## Baixar um arquivo de mídia

Você pode baixar um arquivo de mídia de um catálogo.


### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Mídia e Outros**.

A lista de arquivos de mídia aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda do arquivo de mídia que você deseja baixar e selecione **Baixar**.

A tarefa de download é iniciada e o arquivo é salvo no local de download padrão do navegador da Web.

#### Próximo passo

Dependendo do tamanho do arquivo, pode levar algum tempo para que o download seja concluído. Você pode monitorar o status do download no painel **Tarefas Recentes**. Para obter mais informações, consulte [Exibir tarefas](#).

# Trabalhando com catálogos

# 11

Um catálogo é um contêiner para modelos do vApp e arquivos de mídia em uma organização. Os administradores de organização e os autores de catálogo podem criar catálogos em uma organização. O conteúdo do catálogo pode ser compartilhado com outros usuários ou organizações na instalação do VMware Cloud Director ou publicado externamente para que organizações fora da instalação do VMware Cloud Director possam acessá-lo.

O VMware Cloud Director contém catálogos privados, catálogos compartilhados e catálogos acessíveis externamente. Os catálogos privados incluem modelos do vApp e arquivos de mídia que podem ser compartilhados com outros usuários na organização. Se um administrador de sistema habilitar o compartilhamento de catálogo para sua organização, você poderá compartilhar o catálogo de uma organização para criar um catálogo acessível a outras organizações na instalação do VMware Cloud Director. Se um administrador de sistema permitir a publicação de catálogo externa para a sua organização, você poderá publicar o catálogo de uma organização para que organizações fora da instalação do VMware Cloud Director possam acessá-lo. Uma organização fora da instalação do VMware Cloud Director deve assinar um catálogo publicado externamente para acessar o conteúdo dele.

Você pode carregar um pacote OVF diretamente em um catálogo, salvar um vApp como um modelo vApp ou importar um modelo vApp do vSphere. Consulte [Criar um modelo de vApp de um arquivo OVF](#) e [Salvar um vApp como um modelo do vApp em um catálogo](#).

Os membros de uma organização podem acessar modelos do vApp e arquivos de mídia que eles possuem ou que são compartilhados com eles. Os administradores de organização e os administradores de sistema podem compartilhar um catálogo com todos de uma organização ou com usuários e grupos específicos em uma organização. Consulte [Compartilhar um catálogo](#).

Este capítulo inclui os seguintes tópicos:

- [Exibir catálogos](#)
- [Criar um catálogo](#)
- [Compartilhar um catálogo](#)
- [Excluir um catálogo](#)
- [Alterar o proprietário de um catálogo](#)
- [Gerenciar metadados para um catálogo](#)
- [Publicar um catálogo](#)



- [Assinar um catálogo externo](#)
- [Atualizar a URL do local e a senha para um catálogo assinado](#)
- [Sincronizar um catálogo assinado](#)

## Exibir catálogos

É possível acessar os catálogos compartilhados com você dentro da sua organização. Você poderá acessar catálogos públicos se um administrador da organização os tiver tornado acessíveis na organização.


O acesso ao catálogo é controlado pelo compartilhamento de catálogo, e não pelos direitos de sua função. É possível acessar somente os catálogos ou itens de catálogo compartilhados com você. Para obter mais informações, consulte [Compartilhar um catálogo](#).

### Procedimentos


- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.

A lista de catálogos aparece em uma exibição de grade.

- 2 (Opcional) Configure a exibição de grade para conter os elementos que você deseja ver.

- a Na exibição de grade, clique no ícone do editor de grade (  ) exibido abaixo da lista de catálogos.
- b Selecione os elementos que você deseja incluir na exibição de grade, como versão, descrição, status e assim por diante.
- c Clique em **OK**.

A grade exibe os elementos selecionados para cada catálogo.

- 3 (Opcional) Na exibição de grade, use a barra de lista (  ) para exibir as ações que podem ser tomadas para cada catálogo.

Por exemplo, você pode compartilhar ou excluir um catálogo.

## Criar um catálogo

Você pode criar novos catálogos e associá-los a uma política de armazenamento.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.  
A lista de catálogos aparece em uma exibição de grade.
- 2 Clique em **Novo** para criar um novo catálogo.
- 3 Insira um nome e, opcionalmente, uma descrição para o catálogo.
- 4 (Opcional) Selecione se deseja atribuir uma política de armazenamento ao catálogo e escolha uma política de armazenamento.
- 5 Clique em **OK**.

## Resultados

O novo catálogo aparece na exibição de grade na guia **Catálogos**.


# Compartilhar um catálogo

É possível compartilhar um catálogo com todos os membros da sua organização ou com membros específicos.

## Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.
- Você deve ser o proprietário do catálogo.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.  
A lista de catálogos aparece em uma exibição de grade.
- 2 Clique na barra de lista (  ) à esquerda do catálogo que você deseja compartilhar e selecione **Compartilhar**.  
A lista de usuários que podem acessar o catálogo aparece na exibição em grade da janela **Compartilhar Catálogo**.
- 3 Clique em **Adicionar** para compartilhar o catálogo com outros usuários.

Opção	Descrição
Compartilhe com todos nesta organização	Conceder acesso a todos os usuários e grupos na organização.
Compartilhe com usuários e grupos específicos	Selecione os usuários ou grupos aos quais deseja conceder acesso ao catálogo e clique em <b>Adicionar</b> .

#### 4 Selecione o nível de acesso.

Opção	Descrição
<b>Somente Leitura</b>	Os usuários com acesso a esse catálogo têm acesso de leitura aos modelos de vApp e aos arquivos ISO desse catálogo.
<b>Leitura/Gravação</b>	Os usuários com acesso a esse catálogo têm acesso de leitura aos modelos de vApp e aos arquivos ISO desse catálogo e podem adicionar modelos de vApp e arquivos ISO a esse catálogo.
<b>Controle Total</b>	Os usuários com acesso a esse catálogo têm controle total sobre o conteúdo e as configurações do catálogo.

#### 5 Clique em **OK**.

Os usuários ou grupos que agora têm acesso ao catálogo aparecem na exibição em grade da caixa de diálogo **Compartilhar Catálogo**.

#### 6 (Opcional) Selecione para compartilhar o acesso somente leitura aos administradores de todas as outras organizações

#### 7 Clique em **Salvar**.

#### Resultados

Na guia **Catálogos**, o status Compartilhado desse catálogo na exibição em grade é alterado.

## Excluir um catálogo

Você pode excluir um catálogo da sua organização.

#### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Autor de catálogo** ou um conjunto equivalente de direitos.

**Observação** O catálogo não deve conter nenhum modelo de vApp ou arquivos de mídia. Você pode mover esses itens para um catálogo diferente ou excluí-los.

#### Procedimentos

#### 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.

A lista de catálogos aparece em uma exibição de grade.

#### 2 Clique na barra de lista ( ) à esquerda do catálogo que você deseja excluir e selecione **Excluir**.

#### 3 Confirme a exclusão.

O item de catálogo excluído é removido da exibição em grade.

## Alterar o proprietário de um catálogo


Um **administrador de organização** pode alterar o proprietário de um catálogo.

Antes de poder excluir um usuário que possui um catálogo, você deve alterar o proprietário ou excluir o catálogo.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.  
A lista de catálogos aparece em uma exibição de grade.
- 2 Use a barra de lista (  ) à esquerda de um catálogo e selecione **Alterar proprietário**.  
A lista de usuários que podem acessar o catálogo aparece na exibição em grade da janela **Alterar Proprietário**.
- 3 Selecione o usuário que você deseja tornar o novo proprietário do catálogo e clique em **OK**.


### Resultados

Na guia **Catálogos**, o nome do proprietário desse catálogo na exibição em grade é alterado.

## Gerenciar metadados para um catálogo

Como **administrador da organização** ou **proprietário de catálogo**, você pode criar ou atualizar os metadados dos catálogos que possui.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.  
A lista de catálogos aparece em uma exibição de grade.
- 2 Use a barra de lista (  ) à esquerda de um catálogo e selecione **Metadados**.  
Os metadados do catálogo selecionado aparecem em uma exibição de grade.
- 3 (Opcional) Para adicionar metadados, clique em **Adicionar**.
  - a Insira o nome dos metadados.  
O nome deve ser diferente dos nomes de metadados anexados a este objeto.
  - b Selecione o tipo de metadados, como **Texto**, **Número**, **Data e Hora** ou **Sim ou Não**.

- c Insira o valor dos metadados.
  - d Clique em **Salvar**.
- 4 (Opcional) Atualize os metadados existentes.
- Você não pode alterar o nome dos metadados.
- a Atualize o tipo de metadados.
  - b Insira o novo valor de metadados.
  - c Clique em **Salvar**.
- 5 (Opcional) Exclua os metadados existentes.
- a Clique no ícone Excluir.
  - b Clique em **Salvar**.


## Publicar um catálogo

Se o **administrador do sistema** tiver concedido acesso ao catálogo, você poderá publicar um catálogo externamente para disponibilizar seus arquivos vApp e arquivos de mídia para assinatura por organizações fora da instalação do VMware Cloud Director.

### Pré-requisitos

Verifique se o **administrador do sistema** habilitou a publicação do catálogo externo para a organização e lhe concedeu acesso ao catálogo.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.  
A lista de catálogos aparece em uma exibição de grade.
- 2 Clique na barra de lista (  ) à esquerda do catálogo que deseja publicar e selecione **Configurações de publicação**.
- 3 Selecione **Habilitar Publicação** e, opcionalmente, insira uma senha para acesso ao catálogo.  
Há suporte apenas para caracteres ASCII.
- 4 Clique em **Salvar**.

## Assinar um catálogo externo

Você pode assinar um catálogo externo e, assim, criar uma cópia somente leitura de um catálogo publicado externamente. Não é possível modificar um catálogo assinado.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- O **administrador de sistema** deve conceder à sua organização permissão para assinar catálogos externos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.

A lista de catálogos aparece em uma exibição de grade.

- 2 Clique em **Novo** para criar um novo catálogo.
- 3 Insira um nome e, opcionalmente, uma descrição para o catálogo.
- 4 Selecione para assinar um catálogo externo e forneça a URL de assinatura.
- 5 Insira a senha opcional para acessar o catálogo.
- 6 Selecione se você deseja baixar automaticamente o conteúdo do catálogo externo.
- 7 Clique em **OK**.

## Atualizar a URL do local e a senha para um catálogo assinado

Depois de criar um catálogo assinado, você poderá atualizar a URL do local e a senha do catálogo.


### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Você precisa ter criado um catálogo assinado.
- O **administrador de sistema** deve conceder à sua organização permissão para assinar catálogos externos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.

A lista de catálogos aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda de um catálogo assinado e selecione **Configurações de assinatura**.

Se o catálogo não for assinado, a opção estará desativada.

- 3 Atualize a URL do local e a senha para este catálogo assinado.

- 4 Selecione se você deseja baixar o conteúdo do catálogo externo automaticamente.
- 5 Clique em **Salvar**.

## Sincronizar um catálogo assinado

Depois de criar um catálogo assinado, você poderá sincronizá-lo com o catálogo original para ver se há alterações. Por exemplo, se os metadados do catálogo original forem alterados, quando você realizar a sincronização, os metadados do catálogo assinado serão atualizados.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Você precisa ter criado um catálogo assinado.
- O **administrador de sistema** deve conceder à sua organização permissão para assinar catálogos externos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Catálogos**.

A lista de catálogos aparece em uma exibição de grade.

- 2 Clique na barra de lista (  ) à esquerda de um catálogo assinado e selecione **Sincronizar**.

Se o catálogo não for assinado, a opção estará desativada.

O catálogo assinado é sincronizado com o original.

# Trabalhando com modelos de data center virtual de organização

# 12

Como administrador de organização ou qualquer função com direitos de visualizar e instanciar modelos de centro de dados virtual da organização, você pode criar centros de dados virtuais da organização adicionais.

Um modelo de centro de dados virtual da organização especifica uma configuração para um centro de dados virtual da organização e, opcionalmente, para um Edge Gateway e uma rede de centros de dados virtuais da organização. Os administradores de sistema podem habilitar administradores de organização a criar esses recursos nas respectivas organizações criando modelos de centro de dados virtuais da organização e compartilhando-os com essas organizações.

Criando e compartilhando modelos de centro de dados virtual, os administradores de sistema podem ativar o provisionamento de autoatendimento dos centros de dados virtuais da organização, enquanto mantêm o controle administrativo sobre a alocação de recursos do sistema como centros de dados virtuais do provedor e redes externas.

Os administradores de sistema criam modelos de centro de dados virtual da organização e oferecem acesso aos modelos a organizações diferentes.

Se a sua organização tiver recebido acesso aos modelos de centro de dados virtual, você poderá usar o VMware Cloud Director Tenant Portal para criar centros de dados virtuais com base nos modelos disponíveis.

Este capítulo inclui os seguintes tópicos:

- [Visualizar modelos de centro de dados virtual disponíveis](#)
- [Instanciar um centro de dados virtual a partir de um modelo](#)

## Visualizar modelos de centro de dados virtual disponíveis

É possível visualizar os modelos de centro de dados virtual da organização que um administrador de sistema criou para você.

Visualize os modelos de centro de dados virtual antes de criar um novo centro de dados virtual da organização baseando-se no modelo centro de dados virtual.



### Pré-requisitos

Essa operação requer os direitos incluídos na função predefinida de **Administrador da organização** ou em uma função que tenha direitos para visualizar e instanciar modelos de data center virtual da organização.

### Procedimentos

- ◆ Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos de VDC de Organização**.

A lista de modelos de centros de dados virtuais aparece em uma exibição de grade.

### Próximo passo

Analise as descrições dos modelos de centro de dados virtual da organização e selecione o modelo com base no qual você deseja criar um novo centro de dados virtual da organização.

## Instanciar um centro de dados virtual a partir de um modelo

Quando um administrador do sistema cria um modelo de centro de dados virtual (VDC) da organização e publica esse modelo na sua organização, você pode criar um VDC da organização com base no modelo.

### Pré-requisitos

Essa operação requer os direitos incluídos na função predefinida de **Administrador da organização** ou em uma função que tenha direitos para visualizar e instanciar modelos de VDC da organização.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, no painel esquerdo, selecione **Modelos de VDC de Organização**.

A lista de modelos de centros de dados virtuais aparece em uma exibição de grade.

- 2 Selecione um modelo e clique em **Novo VDC**.

No VMware Cloud Director 10.2.2, depois de selecionar um modelo, você deve clicar em **Criar Instância do VDC**.

- 3 Insira um nome para o VDC e, opcionalmente, uma descrição.

- 4 Clique em **Criar**.

### Resultados

A criação do novo data center virtual da organização é instanciada e pode levar alguns minutos. Você pode ver o andamento da tarefa no painel **Tarefas Recentes**.

### **Próximo passo**

Você pode gerenciar seu data center virtual de organização criado recentemente criando máquinas virtuais, vApps, gerenciando as configurações de rede e de segurança, etc.

# Gerenciar usuários, grupos e funções

# 13

Você pode adicionar administradores de organizações ao VMware Cloud Director individualmente ou como parte de um grupo LDAP. Você também pode adicionar e modificar as funções que determinam os direitos que um usuário tem na sua organização.

**Importante** Você deve ser um **administrador de organização** para gerenciar os usuários, grupos e funções dentro da sua organização. O **administrador do sistema** pode publicar uma ou mais funções de tenant global no seu tenant e, como um **administrador de organização**, você pode vê-las na lista de funções. Essas funções são, por exemplo, **Autor de catálogo**, **Autor de vApp**, **Usuário de vApp**, **Administrador da organização** e assim por diante. Não é possível modificar as funções de tenant global predefinidas, mas você pode criar e atualizar funções de tenant personalizadas semelhantes e atribuí-las aos usuários dentro do seu tenant.

Este capítulo inclui os seguintes tópicos:

- [Gerenciar usuários](#)
- [Gerenciar grupos](#)
- [Funções e direitos](#)

## Gerenciar usuários

No portal do tenant, você pode criar, editar, importar e excluir usuários. Além disso, também pode desbloquear contas de usuário caso um usuário tenha tentado fazer login com uma senha incorreta e, como resultado, bloqueado sua própria conta de usuário.

## Criar um usuário

Você pode criar um usuário dentro de sua organização do VMware Cloud Director.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.

- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.

A lista de usuários é exibida.

- 3 Clique em **Novo**.

- 4 Insira um nome de usuário e a configuração de senha do usuário.

O comprimento mínimo da senha é de seis caracteres.

- 5 Selecione se deseja ativar o usuário na criação.

- 6 Se quiser definir uma limitação específica sobre os recursos disponíveis para o usuário, ative o botão de alternância **Configurar cota do usuário**.

Se você ativar esse botão de alternância, quando concluir o assistente, o VMware Cloud Director o redirecionará até a página **Cotas**. Você pode adicionar cotas sobre o número de clusters do Tanzu Kubernetes, todas as VMs ou as VMs em execução gerenciadas pelo usuário, bem como consumo de CPU, memória e armazenamento. Selecione **Sem Limites** se quiser que o usuário tenha recursos ilimitados do tipo selecionado.

- 7 Escolha a função que você deseja atribuir ao usuário.

O menu **Funções disponíveis** é composto por uma lista de funções predefinidas e quaisquer funções personalizadas que você ou o administrador do sistema podem ter criado.

Função predefinida	Descrição
<b>Autor do vApp</b>	Os direitos associados à função predefinida <b>Autor de vApp</b> permitem que um usuário use catálogos e crie vApps.
<b>Somente Acesso ao Console</b>	Os direitos associados à função predefinida <b>Somente acesso ao console</b> permitem que um usuário visualize as propriedades e o estado da máquina virtual e use o SO convidado.
<b>Usuário do vApp</b>	Os direitos associados a função predefinida <b>Usuário de vApp</b> permitem que um usuário use vApps existentes.
<b>Administrador da Organização</b>	Um usuário com a função predefinida de <b>Administrador da Organização</b> pode usar o portal do tenant do VMware Cloud Director ou o OpenAPI do Cloud Director para gerenciar usuários e grupos na sua organização e atribuir-lhes funções, incluindo a função predefinida de <b>Administrador da Organização</b> . Um <b>administrador da organização</b> pode usar o OpenAPI do Cloud Director para criar ou atualizar objetos de função locais da organização. As funções criadas ou modificadas por um <b>administrador da organização</b> não são visíveis para outras organizações.
<b>Transferir para Provedor de Identidade</b>	Os direitos associados à função predefinida <b>Transferir para Provedor de Identidade</b> são determinados com base nas informações recebidas do Provedor de identidade OAuth ou SAML do usuário. Para se qualificar para inclusão quando um usuário é atribuído com a função <b>Transferir para Provedor de Identidade</b> , um nome de função fornecido pelo Provedor de identidade deve ser uma correspondência exata com distinção entre maiúsculas e minúsculas para um nome de função definido na sua organização.
<b>Autor do Catálogo</b>	Os direitos associados à função predefinida <b>Autor do Catálogo</b> permitem que um usuário crie e publique catálogos.

- 8 (Opcional) Insira as informações de contato, como nome, endereço de e-mail, número de telefone e ID de mensagens instantâneas.
- 9 Clique em **Salvar**.

#### Próximo passo

Se você tiver ativado a configuração de cotas para o usuário e o VMware Cloud Director o redirecionar para a página **Cotas**, consulte [Gerenciar as cotas de recursos de um usuário](#).

## Importar Usuários

Você pode adicionar usuários às suas organizações, importando um usuário LDAP ou um usuário SAML e atribuindo a ele uma função específica.

#### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Verifique se existe uma conexão válida com um servidor LDAP ou se você [Permitir que sua organização use um provedor de identidade SAML](#).

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.  
A lista de usuários é exibida.
- 3 Clique em **Importar Usuários**.

#### 4 Selecione uma origem da qual você deseja importar os usuários.

Você só visualizará o servidor LDAP de origem ou o servidor SAML que configurou como provedor de identidade.

Origem	Ação
LDAP	<p>Importe usuários de um servidor LDAP.</p> <p>a Insira um nome completo ou parcial na caixa de texto e clique em <b>Pesquisar</b>.</p> <p>b Selecione os usuários que você deseja importar e clique em <b>Adicionar</b>.</p>
SAML	<p>Importe usuários de um servidor SAML. Insira os nomes dos usuários que você deseja importar.</p> <p>Os nomes de usuário devem estar no formato de identificador de nome aceito pelo provedor de identidade SAML configurado para esta organização.</p> <hr/> <p><b>Observação</b> Se você estiver usando vCenter Single Sign-On como provedor de identidade SAML, os nomes de usuários que importar de um domínio do vCenter Single Sign-On deverão estar no formato Nome principal do usuário (UPN), por exemplo, jdoe@mydomain.com.</p> <hr/> <p>Use uma nova linha para cada nome de usuário.</p>

#### 5 Selecione a função que você deseja atribuir aos usuários importados.

#### 6 Clique em **Salvar**.

## Modificar um usuário

Como administrador da organização, você pode modificar a senha, o contato e as configurações de cota da máquina virtual de um usuário existente. Além disso, você também pode alterar a função do usuário.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- Na barra de navegação superior, clique em **Administração**.
- No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.  
A lista de usuários é exibida.
- Clique no botão de opção ao lado do nome da usuário que você deseja editar e clique em **Modificar**.
- Atualize as configurações que você deseja modificar.
  - Altere a senha conforme necessário.
  - Selecione se deseja ativar ou desativar o usuário.

- c Atualize a função do usuário.
- d Atualize as informações de contato, como nome, endereço de e-mail, número de telefone e ID de mensagens instantâneas.
- e Edite a cota da máquina virtual para o usuário.

5 Clique em **Salvar**.

## Desativar ou ativar uma conta de usuário

Você pode desativar uma conta de usuário para impedir que esse usuário faça login no VMware Cloud Director. Para excluir um usuário, você deve primeiro desativar a conta dele.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.  
A lista de usuários é exibida.
- 3 Para desativar uma conta de usuário, clique no botão de opção ao lado do nome de usuário, clique em **Desativar** e confirme.
- 4 Para ativar uma conta de usuário que você já desativou, clique no botão de opção ao lado do nome de usuário e clique em **Ativar**.

## Excluir um usuário

Você pode remover um usuário da organização do VMware Cloud Director excluindo a conta de usuário.

### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Desative a conta que você deseja excluir.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.  
A lista de usuários é exibida.
- 3 Clique no botão de opção ao lado do nome do usuário que você deseja excluir e clique em **Excluir**.

- 4 Para confirmar que você deseja excluir a conta de usuário, clique em **OK**.

## Desbloquear uma conta de usuário bloqueada

Se você tiver habilitado uma política de bloqueio na sua organização do VMware Cloud Director, uma conta de usuário será bloqueada após um determinado número de tentativas de login inválidas. Você pode desbloquear a conta de usuário bloqueada. A boa prática é alterar a senha do usuário e desbloquear a conta.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.  
A lista de usuários é exibida.
- 3 Clique no botão de rádio ao lado do nome do usuário e depois em **Desbloquear**.

## Gerenciar as cotas de recursos de um usuário

Você pode gerenciar o limite geral de consumo de recursos de um usuário. Você pode adicionar, editar e remover cotas do usuário sobre VMs, clusters do Tanzu Kubernetes, CPU, memória ou armazenamento.

Os usuários podem ver as cotas relevantes apenas para o seu tipo de usuário. Os usuários herdam as cotas do grupo ao qual pertencem. Se um usuário herdar uma cota de recursos de seu grupo e tiver uma cota explícita em nível de usuário definida para esse recurso, a cota em nível de usuário terá prioridade sobre a cota em nível de grupo.

Para obter informações sobre como criar ou importar usuários, consulte [Criar um usuário](#) ou [Importar Usuários](#).

### Pré-requisitos

Verifique se você tem os direitos necessários para adicionar, editar e excluir cotas de recursos. Por padrão, **Administradores da organização** podem alterar as cotas dos usuários.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Usuários**.
- 3 Selecione o nome de um usuário e selecione a guia **Cotas**.

Usuários não têm cotas por padrão. Todos os usuários que pertencem a um grupo herdam as cotas desse grupo. Se o usuário pertencer a um grupo que tem uma cota sobre recursos, essa cota aparecerá na lista de cotas do usuário como não editável.



4 Clique em **Editar**.

5 Modifique a cota para o usuário selecionado.

Você pode adicionar, editar ou remover cotas sobre o número de clusters do Tanzu Kubernetes, todas as VMs ou as VMs em execução gerenciadas pelo usuário, bem como consumo de CPU, memória e armazenamento. Selecione **Sem Limites** se quiser que o usuário tenha recursos ilimitados do tipo selecionado.

6 Clique em **Salvar**.

## Gerenciar grupos

Se você tiver uma conexão válida com um servidor LDAP ou tiver habilitado sua organização para usar um provedor de identidade SAML, poderá importar um grupo LDAP ou um grupo SAML. Você também pode editar ou excluir um grupo importado.

### Importar um grupo

Para adicionar um grupo de usuários, você pode importar um grupo LDAP ou um grupo SAML.

#### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Verifique se existe uma conexão válida com um servidor LDAP ou se você [Permitir que sua organização use um provedor de identidade SAML](#).

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Grupos**.  
A lista de grupos de usuários é exibida.
- 3 Clique em **Importar Grupo**.

- 4 Selecione uma origem da qual você deseja importar o grupo de usuários.

Você só pode visualizar o servidor LDAP de origem ou o servidor SAML que configurou como provedor de identidade.

Origem	Ação
LDAP	<p>Importe um grupo de usuários de um servidor LDAP.</p> <ol style="list-style-type: none"> <li>Insira um nome completo ou parcial na caixa de texto e clique em <b>Pesquisar</b>.</li> <li>Selecione os grupos de usuários que você deseja importar e clique em <b>Adicionar</b>.</li> </ol>
SAML	<p>Importe grupos de usuários de um servidor SAML. Insira os nomes dos grupos que você deseja importar.</p> <p>Use uma nova linha para cada nome de grupo.</p>

- 5 Selecione a função que você deseja atribuir ao grupo de usuários importado.

- 6 Clique em **Salvar**.

#### Próximo passo

Se você tiver ativado a configuração de cotas para o grupo e o VMware Cloud Director o redirecionar para a página **Cotas**, consulte [Gerenciar as cotas de recursos de um grupo](#).

## Excluir um grupo

Você pode remover um grupo da sua organização do VMware Cloud Director excluindo seu grupo LDAP.

Quando você exclui um grupo LDAP, os usuários que têm uma conta do VMware Cloud Director com base somente na associação desse grupo são bloqueados e não podem fazer login.

#### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Grupos**.  
A lista de grupos de usuários é exibida.
- 3 Clique no botão de opção ao lado do nome do grupo que você deseja excluir e clique em **Excluir**.
- 4 Para confirmar que você deseja excluir o grupo, clique em **OK**.

## Editar um grupo

Você pode editar um grupo do portal do tenant do VMware Cloud Director.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Grupos**.  
A lista de grupos de usuários é exibida.
- 3 Clique no botão de opção ao lado do nome do grupo que você deseja editar e clique em **Editar**.
- 4 Edite o grupo conforme necessário.
  - a Altere a descrição.
  - b Altere a função dos membros do grupo conforme necessário.
- 5 Clique em **Salvar**.

## Gerenciar as cotas de recursos de um grupo

Ao definir diretamente a cota sobre um grupo, você pode gerenciar o limite geral de consumo de recursos de cada usuário desse grupo. Você pode adicionar, editar e remover cotas do grupo sobre VMs, clusters do Tanzu Kubernetes, CPU, memória ou armazenamento. Cotas do grupo são aplicadas a cada membro do grupo.

Os usuários herdam as cotas do grupo ao qual pertencem. Se um usuário herdar uma cota de recursos de seu grupo e tiver uma cota explícita em nível de usuário definida para esse recurso, a cota em nível de usuário terá prioridade sobre a cota em nível de grupo.

Para obter informações sobre como importar grupos, consulte [Importar um grupo](#).

### Pré-requisitos

Verifique se você tem os direitos necessários para adicionar, editar e excluir cotas de recursos. Por padrão, **Administradores da organização** podem alterar as cotas dos grupos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Grupos**.
- 3 Selecione o nome de um grupo e selecione a guia **Cotas**.  
Grupos não têm cotas por padrão. Todos os usuários que pertencem a um grupo herdam as cotas desse grupo. Se o usuário pertencer a um grupo que tem uma cota sobre recursos, essa cota aparecerá na lista de cotas do usuário como não editável.
- 4 Clique em **Editar**.

## 5 Modifique a cota do grupo selecionado.

Você pode adicionar, editar ou remover cotas sobre o número de clusters do Tanzu Kubernetes, todas as VMs ou as VMs em execução gerenciadas pelo grupo, bem como consumo de CPU, memória e armazenamento. Selecione **Sem Limites** se quiser que o grupo de usuários tenha recursos ilimitados do tipo selecionado.

## 6 Clique em **Salvar**.

# Funções e direitos

O VMware Cloud Director usa funções e direitos para determinar quais ações um usuário pode realizar em uma organização. O VMware Cloud Director inclui várias funções predefinidas com direitos específicos.

**Administradores de sistema** e **administradores de organização** devem atribuir uma função a cada usuário ou grupo. O mesmo usuário pode ter uma função diferente em organizações diferentes. **Administradores de sistema** podem criar funções e modificar as existentes para todo o sistema, enquanto **administradores de organização** podem criar e modificar funções apenas para a organização que eles administram.

O portal do tenant do VMware Cloud Director permite que **administradores de organização** gerenciem as funções em suas organizações. Se um **administrador de sistema** publicar uma ou mais funções de tenant predefinidas na sua organização, como **administrador de organização**, você poderá ver essas funções, mas não poderá modificá-las. No entanto, é possível criar funções de tenant personalizadas com direitos semelhantes e atribuí-las aos usuários dentro da sua organização.

Para obter informações sobre as funções predefinidas e seus direitos, consulte [Funções predefinidas e seus direitos](#).

## Funções predefinidas e seus direitos

Cada função predefinida do VMware Cloud Director contém um conjunto padrão de direitos necessários para realizar as operações incluídas em fluxos de trabalho comuns. Por padrão, todas as funções predefinidas de tenant global são publicadas para todas as organizações do sistema.

### Funções de provedor predefinidas

Por padrão, as funções de provedor que são locais apenas para a organização do provedor são as funções de **Administrador do sistema** e **Sistema multissite**. **Administradores de sistema** pode criar funções de provedor personalizadas adicionais.

#### Administrador do sistema

A função de **Administrador do sistema** existe somente na organização do provedor. A função de **Administrador do sistema** inclui todos os direitos do sistema. Para obter uma lista de direitos disponíveis somente para a função de **administrador do sistema**, consulte *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*. As credenciais

de **Administrador do sistema** são estabelecidas durante a instalação e a configuração. Um **Administrador do sistema** pode criar contas adicionais de usuário e administrador do sistema na organização do provedor.

### Sistema multissite

Usado para executar o processo de heartbeat para implantações multissite. Essa função tem um único direito, **Multissite: Operações do Sistema**, que oferece uma permissão para fazer uma solicitação de OpenAPI do Cloud Director que recupera o status do membro remoto de uma associação de site.

### Funções predefinidas de tenant global

Por padrão, as funções predefinidas de tenant global e os direitos que elas contêm são publicadas para todas as organizações. **Administradores de sistema** podem cancelar a publicação de direitos e funções de tenant global em organizações individuais. **Administradores de sistema** podem editar ou excluir funções predefinidas de tenant global. **Administradores de sistema** podem criar e publicar funções adicionais de tenant global.

### Administrador da organização

Após a criação de uma organização, um **Administrador do sistema** pode atribuir a função de **Administrador da organização** a qualquer usuário da organização. Um usuário com a função predefinida de **Administrador da Organização** pode para gerenciar usuários e grupos na sua organização e atribuir-lhes funções, incluindo a função predefinida de **Administrador da Organização**. As funções criadas ou modificadas por um **Administrador da organização** não são visíveis para outras organizações.

### Autor do catálogo

Os direitos associados à função predefinida **Autor do catálogo** permitem que um usuário crie e publique catálogos.

### Autor de vApp

Os direitos associados à função predefinida **Autor de vApp** permitem que um usuário use catálogos e crie vApps.

### Usuário de vApp

Os direitos associados a função predefinida **Usuário de vApp** permitem que um usuário use vApps existentes.

### Somente acesso ao console

Os direitos associados à função predefinida **Somente acesso ao console** permitem que um usuário visualize as propriedades e o estado da máquina virtual e use o SO convidado.

### Adiar para provedor de identidade

Os direitos associados à função predefinida **Transferir para Provedor de Identidade** são determinados com base nas informações recebidas do Provedor de identidade OAuth ou SAML do usuário. Para se qualificar para inclusão quando um usuário ou grupo é atribuído à função **Adiar para provedor de identidade**, um nome de função ou grupo fornecido pelo Provedor de Identidade deve ser uma correspondência exata com distinção entre maiúsculas e minúsculas para um nome de função ou grupo definido na sua organização.

- Se um provedor de identidade OAuth definir o usuário, ele receberá as funções nomeadas na matriz `roles` do token OAuth do usuário.
- Se um Provedor de Identidade SAML definir o usuário, ele receberá as funções nomeadas no atributo SAML cujo nome aparece no elemento `RoleAttributeName`, que é o elemento `SamlAttributeMapping` no `OrgFederationSettings` da organização.

Se um usuário receber a função **Adiar para o provedor de identidade**, mas nenhuma função ou nome do grupo correspondente estiver disponível na sua organização, ele poderá fazer login na organização, mas não terá direitos. Se um Provedor de Identidade associar um usuário a uma função em nível de sistema, como **Administrador do sistema**, ele poderá fazer login na organização, mas não terá direitos. Você deve atribuir uma função manualmente a esses usuários.

Exceto pela função **Adiar para provedor de identidade**, cada função predefinida inclui um conjunto de direitos padrão. Apenas um **Administrador do sistema** pode modificar os direitos em uma função predefinida. Se um **Administrador do sistema** modificar uma função predefinida, essas modificações se propagarão para todas as instâncias da função no sistema.

## Direitos em funções predefinidas de tenant global

Vários direitos são comuns a várias funções globais predefinidas. Esses direitos são concedidos por padrão a todas as novas organizações e estão disponíveis para uso em outras funções criadas pelo **Administrador da organização**. Para obter uma lista de direitos em funções de tenant predefinidas, consulte [Direitos em funções predefinidas de tenant global](#).

## Direitos em funções predefinidas de tenant global

Vários direitos são comuns a várias funções globais predefinidas. Esses direitos são concedidos por padrão a todas as novas organizações e estão disponíveis para uso em outras funções criadas pelo **Administrador da organização**.

## Direitos incluídos nas funções de tenant global do VMware Cloud Director

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Acessar todos os VDCs de organização	✓				
	Catálogo: Adicionar um vApp da Minha Nuvem	✓	✓	✓		

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Catálogo: Alterar proprietário	✓				
	Catálogo: Publicar e Assinar CLSP	✓	✓			
	Catálogo: Criar/excluir um catálogo	✓	✓			
	Catálogo: Editar Propriedades	✓	✓			
	Catálogo: Publicar	✓	✓			
	Catálogo: Compartilhamento	✓	✓			
	Catálogo: Exibir ACL	✓	✓			
	Catálogo: Exibir Catálogos Particulares e Compartilhados	✓	✓	✓		
	Catálogo: Exibir Catálogos Publicados	✓				
	Entidade personalizada: Exibir todas as instâncias de entidades personalizadas da organização	✓				
	Entidade personalizada: Exibir instância de entidade personalizada	✓				
	Disco: Alterar Proprietário	✓	✓			
	Disco: Criar	✓	✓	✓		
	Disco: Excluir	✓	✓	✓		
	Disco: Editar Propriedades	✓	✓	✓		
	Disco: Exibir Status de Criptografia	✓		✓		
	Disco: Exibir Propriedades	✓	✓	✓	✓	
	Geral: Controle do administrador	✓				
	Geral: Exibição do administrador	✓				
	Geral: Enviar notificação	✓				
	Grupo/usuário: Exibir	✓				
	Operações de Nuvem Híbrida: Adquirir tíquete de controle	✓				
	Operações de Nuvem Híbrida: Adquirir tíquete de túnel proveniente da nuvem	✓				

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Operações de Nuvem Híbrida: Adquirir tíquete de túnel com destino à nuvem	✓				
	Operações de Nuvem Híbrida: Criar túnel proveniente da nuvem	✓				
	Operações de Nuvem Híbrida: Criar túnel com destino à nuvem	✓				
	Operações de Nuvem Híbrida: Excluir túnel proveniente da nuvem	✓				
	Operações de Nuvem Híbrida: Excluir túnel com destino à nuvem	✓				
	Operações de Nuvem Híbrida: Atualizar tag de endpoint de túnel proveniente da nuvem	✓				
	Operações de Nuvem Híbrida: Excluir túnel proveniente da nuvem	✓				
	Operações de Nuvem Híbrida: Exibir túnel com destino à nuvem	✓				
	Rede da Organização: Editar Propriedades	✓				
	Rede da organização: Exibir	✓				
	Política de Processamento do vDC de Organização: Exibir	✓	✓	✓	✓	
	Firewall Distribuído do vDC de Organização: Configurar Regras	✓				
	Firewall Distribuído do vDC de Organização: Exibir Regras	✓				
	Gateway do vDC de Organização: Configurar DHCP	✓				
	Gateway do vDC de Organização: Configurar DNS	✓				
	Gateway do vDC de Organização: Configurar Roteamento ECMP	✓				
	Gateway do vDC de Organização: Configurar Firewall	✓				
	Gateway do vDC de Organização: Configurar VPN IPSec	✓				



Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Gateway do vDC de Organização: Configurar Balanceador de Carga	✓				
	Gateway do vDC de Organização: Configurar NAT	✓				
	Gateway do vDC de Organização: Configurar Roteamento Estático	✓				
	Gateway do vDC de Organização: Configurar Syslog	✓				
	Gateway do vDC de Organização: Converter em Rede Avançada	✓				
	Gateway do vDC de Organização: Exibir	✓				
	Gateway do vDC de Organização: Exibir DHCP	✓				
	Gateway do vDC de Organização: Exibir DNS	✓				
	Gateway do vDC de Organização: Exibir Firewall	✓				
	Gateway do vDC de Organização: Exibir VPN IPsec	✓				
	Gateway do vDC de Organização: Exibir o Balanceador de Carga	✓				
	Gateway do vDC de Organização: Exibir NAT	✓				
	Gateway do vDC de Organização: Exibir Roteamento Estático	✓				
	Rede do vDC de Organização: Editar Propriedades	✓				
	Rede do vDC de Organização: Exibir Propriedades	✓		✓		
	Política de Armazenamento do vDC de Organização: Exibir Recursos	✓				
	Perfil de Armazenamento do vDC de Organização: Definir Padrão	✓				
	vDC de Organização: Editar	✓				
	vDC de Organização: Editar ACL	✓				
	vDC de organização: Gerenciar Firewall	✓				
	vDC de Organização: Exibir	✓	✓			

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	vDC de Organização: Exibir ACL	✓				
	VDC de Organização: Exibir métricas	✓				
	vDC de Organização: Editar Afinidade entre VMs	✓	✓	✓		
	Organização: Editar Configurações de Associação	✓				
	Organização: Editar Configurações de Federação	✓				
	Organização: Editar Configurações SMTP	✓				
	Organização: Editar Política de Concessões	✓				
	Organização: Editar Configurações de OAuth	✓				
	Organização: Editar Política de Senha	✓				
	Organização: Editar Propriedades	✓				
	Organização: Editar Política de Cotas	✓				
	Organização: Editar Configurações SMTP	✓				
	Organização: Importar Usuário/ Grupo do IdP ao Editar ACL do VDC	✓				
	Organização: Exibir	✓	✓	✓		
	Organização: Exibir métricas	✓				
✓	Recursos de Política de Cotas: Exibir	✓				
	Função: Criar, Editar, Excluir ou Copiar	✓				
	Biblioteca de Serviços: Exibir bibliotecas de serviços	✓				
	Plug-ins de UI: Exibir	✓	✓	✓	✓	
	Modelo/Mídia de vApp: Copiar	✓	✓	✓		
	Modelo/Mídia de vApp: Criar/ Carregar	✓	✓			

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Modelo/Mídia de vApp: Editar	✓	✓	✓		
	Modelo/Mídia de vApp: Exibir	✓	✓	✓	✓	
	Modelo de vApp: Alterar Proprietário	✓	✓			
	Modelo de vApp: Fazer Check-out	✓	✓	✓	✓	
	Modelo de vApp: Baixar	✓	✓			
	vApp: Alterar Proprietário	✓				
	vApp: Copiar	✓	✓	✓	✓	
	vApp: Criar/Reconfigurar	✓	✓	✓		
	vApp: Excluir	✓	✓	✓	✓	
	vApp: Baixar	✓	✓	✓		
	vApp: Editar Propriedades	✓	✓	✓	✓	
	vApp: Editar Política de Processamento da VM	✓	✓	✓		
	vApp: Editar CPU da VM	✓	✓	✓		
	vApp: Editar Disco Rígido da VM	✓	✓	✓		
	vApp: Editar Memória da VM	✓	✓	✓		
	vApp: Editar Rede da VM	✓	✓	✓	✓	
	vApp: Editar Propriedades da VM	✓	✓	✓	✓	
	vApp: Gerenciar Configurações de Senha da VM	✓	✓	✓	✓	✓
	vApp: Operações de Energia	✓	✓	✓	✓	
	vApp: Compartilhamento	✓	✓	✓	✓	
	vApp: Operações de Snapshot	✓	✓	✓	✓	
	vApp: Carregar	✓	✓	✓		
	vApp: Usar Console	✓	✓	✓	✓	✓
	vApp: Exibir ACL	✓	✓	✓	✓	
	vApp: Exibir a VM e o Status de Criptografia dos discos da VM	✓		✓		
	vApp: Exibir Métricas de VM	✓		✓	✓	

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	vApp: Opções de Inicialização de VM	✓	✓	✓		
	vApp: Metadados da VM para o vCenter	✓	✓	✓		
✓	Grupo de VDCs: Configurar	✓				
✓	Grupo de VDCs: Exibir	✓				
✓	Grupo de VDCs: Configurar Log	✓				
	Modelo de VDC: Instanciar	✓				
	Modelo de VDC: Exibir	✓				

## Criar uma função de tenant personalizada

Os administradores de organizações podem usar o portal de tenant para criar objetos de função de tenant personalizados nas organizações que administram.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Funções**.  
A lista de funções é exibida.
- 3 Clique em **Adicionar**.
- 4 Insira um nome e, opcionalmente, uma descrição para a função.
- 5 Expanda os direitos da função e selecione os direitos da função.

Os direitos são agrupados em categorias e subcategorias que permitem a visualização ou o gerenciamento de objetos.

Opção	Descrição
<b>Controle de Acesso</b>	Direitos que controlam o acesso à visualização e ao gerenciamento de determinados objetos.
<b>Administração</b>	Direitos de controlar o acesso administrativo.
<b>Calcular</b>	Os direitos que controlam o acesso e o gerenciamento dos data centers virtuais da organização e do provedor, os vApps, os modelos de data centers virtuais de organização, grupos de máquinas virtuais e monitoramento de máquinas virtuais.

Opção	Descrição
<b>Extensões</b>	Direitos que controlam o acesso a quaisquer plug-ins e extensões adicionais do VMware Cloud Director.
<b>Infraestrutura</b>	Direitos que controlam o acesso e o gerenciamento dos objetos de infraestrutura, como datastores, discos, hosts e assim por diante.
<b>Bibliotecas</b>	Direitos de controle de acesso e gerenciamento de quaisquer catálogos e itens de catálogo.
<b>Rede</b>	Direitos de controle de acesso e gerenciamento das configurações de rede.

6 Clique em **Salvar**.

## Editar uma função de tenant personalizada

Os administradores de organizações podem usar o portal do tenant para editar objetos de função de tenant personalizados nas organizações que eles administram. Como administrador da organização, você só pode visualizar as funções de tenant globais que um administrador de sistema publicou na sua organização. Você não pode editar funções de tenant global.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Funções**.  
A lista de funções é exibida.
- 3 Clique no botão de opção ao lado da função que você deseja editar e clique em **Editar**.
- 4 Modifique as configurações da função conforme necessário.
  - a Altere o nome e, opcionalmente, a descrição da função.
  - b Edite os direitos da função.
- 5 Clique em **Salvar**.

## Excluir uma função

Os administradores de organização podem usar o portal do tenant para excluir objetos de função nas organizações que eles administram.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso**, clique em **Funções**.  
A lista de funções é exibida.
- 3 Clique no botão de opção ao lado da função que você deseja excluir e clique em **Excluir**.
- 4 Confirme que você deseja excluir a função clicando em **OK**.

# Configurar provedores de identidade

# 14

Você pode integrar sua nuvem a um provedor de identidade externo e importar usuários e grupos para sua organização.

Você pode habilitar sua organização para usar um provedor de identidade SAML ou pode configurar uma conexão de servidor LDAP.

Este capítulo inclui os seguintes tópicos:

- [Permitir que sua organização use um provedor de identidade SAML](#)
- [Editar configurações LDAP para sua organização](#)
- [Configurar, teste e sincronizar uma conexão LDAP](#)

## Permitir que sua organização use um provedor de identidade SAML

Habilite sua organização para usar um provedor de identidade SAML (Security Assertion Markup Language), também chamado de single sign-on, para importar usuários e grupos de um provedor de identidade SAML e permitir que usuários importados façam login na organização com as credenciais estabelecida no provedor de identidade SAML.

Quando você importa usuários e grupos, o sistema extrai uma lista de atributos do token SAML, se disponível, e os usa para interpretar as partes de informações correspondentes sobre o usuário que está tentando fazer login.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

O atributo de função é configurável.

As informações de grupo serão necessárias se o usuário não for importado diretamente, mas espera-se que ele possa fazer login devido à sua participação em grupos importados. Um usuário pode pertencer a vários grupos e pode ter várias funções durante uma sessão.

Se um usuário ou grupo importado receber a função **Transferir para Provedor de Identidade**, as funções serão atribuídas com base nas informações coletadas do atributo Funções no token. Se um atributo diferente for usado, esse nome de atributo poderá ser configurado usando apenas a API e apenas o atributo Funções será configurável. Se a função **Transferir para Provedor de Identidade** for usada, mas nenhuma informação de função puder ser extraída, o usuário poderá fazer login, mas não terá direito de executar nenhuma atividade.

#### Pré-requisitos

- Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.
- Verifique se você tem acesso a um provedor de identidade em conformidade com o SAML 2.0.
- Verifique se você recebe os metadados necessários do seu provedor de identidade SAML. Você deve importar os metadados para o VMware Cloud Director manualmente ou como um arquivo XML. Os metadados devem incluir as seguintes informações:
  - A localização do serviço single sign-on
  - A localização do serviço de logout único
  - A localização do certificado x.509 do serviço

Para obter informações sobre como configurar e adquirir metadados de um provedor SAML, consulte a documentação do seu provedor de identidade SAML.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 Em **Provedores de Identidade**, clique em **SAML**.
- 3 Clique em **Editar**.
- 4 Na guia **Provedor de Serviços**, insira o ID da Entidade.

O ID da Entidade é o identificador exclusivo da sua organização para o seu provedor de identidade. Você pode usar o nome da sua organização ou qualquer outra cadeia de caracteres que atenda aos requisitos do seu provedor de identidade SAML.

---

**Importante** Depois de especificar um ID de Entidade, não é possível excluí-lo. Para alterar o ID de Entidade, você deverá fazer uma reconfiguração SAML completa para sua organização. Para obter informações sobre IDs de Entidade, consulte [Asserções e protocolos para a SAML \(Security Assertion Markup Language\) 2.0 OASIS](#).

---

- 5 Clique no link de **Metadados** para baixar os metadados SAML para a sua organização.
- Os metadados baixados devem ser fornecidos como estão para o seu provedor de identidade.



- 6 Revise a data de Expiração do Certificado e, opcionalmente, clique em Gerar Novamente para gerar novamente o certificado usado para assinar mensagens de federação.

O certificado está incluído nos metadados SAML e é usado para assinatura e criptografia.

A criptografia e a assinatura, ou ambas, podem ser necessárias, dependendo de como a confiança é estabelecida entre sua organização e seu provedor de identidade SAML.

- 7 Na guia **Provedor de Identidade**, habilite a opção **Usar Provedor de Identidade SAML**.
- 8 Copie e cole os metadados SAML que você recebeu do seu provedor de identidade na caixa de texto ou clique em **Carregar** para procurar e carregar os metadados de um arquivo XML.
- 9 Clique em **Salvar**.

#### Próximo passo

- Configure seu provedor SAML com metadados do VMware Cloud Director. Consulte a documentação do provedor de identidade SAML e *Guia de instalação, configuração e upgrade do VMware Cloud Director*.
- Importe usuários e grupos do seu provedor de identidade SAML. Consulte [Capítulo 13 Gerenciar usuários, grupos e funções](#)

## Editar configurações LDAP para sua organização

Você pode configurar sua organização para usar a conexão LDAP do sistema como uma fonte compartilhada de usuários e grupos. Você pode configurar sua organização para usar uma conexão LDAP separada como uma fonte privada de usuários e grupos.

#### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Provedores de Identidade**, clique em **LDAP**.  
As configurações de LDAP atuais são exibidas.
- 3 Na guia **Configurações de LDAP**, clique em **Editar**.

#### 4 Configure a fonte LDAP de usuários e grupos para sua organização e clique em **Salvar**.

Opção	Descrição
Não usar LDAP	A organização não usa um servidor LDAP como fonte de usuários e grupos da organização.
Serviço LDAP do sistema do VMware Cloud Director	A organização usa a conexão LDAP do sistema VMware Cloud Director configurada pelo seu provedor de serviços. Insira o nome distinto da unidade organizacional.
Serviço LDAP personalizado	A organização usa um servidor LDAP privado como uma fonte de usuários e grupos da organização.

##### Próximo passo

Se você tiver selecionado **Serviço LDAP personalizado**, clique na guia **LDAP Personalizado** para [Configurar, teste e sincronizar uma conexão LDAP](#).

## Configurar, teste e sincronizar uma conexão LDAP

Para configurar uma conexão LDAP, você define os detalhes do seu servidor LDAP. Você pode testar a conexão para verificar se digitou as configurações corretas e se os atributos do usuário e do grupo estão mapeados corretamente. Quando você tem uma conexão LDAP bem-sucedida, pode sincronizar as informações de usuário e grupo com o servidor LDAP a qualquer momento.

##### Pré-requisitos

Se você planeja se conectar a um servidor LDAP por SSL (LDAPS), verifique se o certificado do seu servidor LDAP está em conformidade com a Identificação do Endpoint, introduzida na Atualização 181 do Java 8. O nome comum (CN) ou o nome alternativo da entidade (SAN) do certificado deve corresponder ao FQDN do servidor LDAP. Para obter mais informações, consulte *Alterações na versão do Java 8* em <https://www.java.com>.

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

##### Procedimentos

- 1 Na guia de **Conexão**, insira as informações necessárias para a conexão LDAP.

Informações necessárias	Descrição
Servidor	O nome do host ou o endereço IP do servidor LDAP.
Porta	O número da porta na qual o servidor LDAP está escutando. Para o LDAP, o número da porta padrão é 389. Para o LDAPS, o número da porta padrão é 636.

Informações necessárias	Descrição
Nome distinto de base	<p>O nome distinto de base (DN) é o local no diretório LDAP onde VMware Cloud Director se conecta.</p> <p>Para se conectar a nível da raiz, insira apenas os componentes do domínio, por exemplo, <b>DC=example,DC=com</b>.</p> <p>Para se conectar a um nó na estrutura de árvore do domínio, insira o nome distinto desse nó, por exemplo, <b>OU=ServiceDirector,DC=example,DC=com</b>.</p> <p>Conectar-se a um nó limita o escopo do diretório disponível para o VMware Cloud Director.</p>
Tipo de conector	O tipo de servidor LDAP. Pode ser <b>Active Directory</b> ou <b>OpenLDAP</b> .
Usar SSL	Se o seu servidor for LDAPS, marque essa caixa de seleção.
Aceitar todos os certificados	Se o seu servidor for LDAPS, marque essa caixa de seleção ou carregue o certificado SSL do LDAP.
Truststore Personalizado	Se o seu servidor for LDAPS, clique no botão <b>Carregar</b> e importe um certificado SSL do LDAP ou selecione <b>Aceitar todos os certificados</b> .
Método de autenticação	<p>A autenticação simples consiste em enviar o DN e a senha do usuário para o servidor LDAP. Se você estiver usando o LDAP, a senha do LDAP será enviada pela rede em texto sem formatação.</p> <p>Se você quiser usar o Kerberos, deverá configurar a conexão LDAP usando a API do vCloud.</p>
Nome de usuário	<p>Insira o nome distinto (DN) LDAP completo de uma conta de serviço com direitos de administrador de domínio. O VMware Cloud Director usa essa conta para consultar o diretório LDAP e recuperar as informações do usuário.</p> <p>Se o suporte de leitura anônima estiver habilitado em seu servidor LDAP, você poderá deixar essas caixas de texto em branco.</p>
Senha	<p>A senha da conta de serviço que se conecta ao servidor LDAP.</p> <p>Se o suporte de leitura anônima estiver habilitado em seu servidor LDAP, você poderá deixar essas caixas de texto em branco.</p>

- 2 Clique na guia **Atributos do Usuário**, examine os valores padrão para os atributos do usuário e, se o seu diretório LDAP usar um esquema diferente, modifique os valores.
- 3 Clique na guia **Atributos do Grupo**, examine os valores padrão para os atributos do grupo e, se o seu diretório LDAP usar um esquema diferente, modifique os valores.
- 4 Clique em **Salvar**.
- 5 Se você tiver marcado a caixa de seleção **Usar SSL** e se o certificado do servidor LDAPS ainda não for confiável, na janela **Certificado de Confiança**, confirme se você confia no certificado apresentado pelo endpoint do servidor.

**6** Para testar as configurações de conexão LDAP e os mapeamentos de atributos LDAP:

a Clique em **Testar**

b Insira a senha do usuário do servidor LDAP que você configurou e clique em **Testar**.

Se conectado com êxito, uma marca de seleção verde será exibida.

O usuário recuperado e os valores de atributo do grupo são exibidos em uma tabela. Os valores que são mapeados com êxito para os atributos LDAP estão marcados com marcas de verificação verdes. Os valores que não são atributos LDAP mapeados estão em branco e marcados com pontos de exclamação vermelhos.

c Para sair, clique em **Cancelar**.

**7** Para sincronizar o VMware Cloud Director com o servidor LDAP configurado, clique em **Sincronizar**.

O VMware Cloud Director sincroniza as informações de grupo e usuário com o servidor LDAP regularmente, dependendo do intervalo de sincronização que você definiu nas configurações gerais do sistema.

Aguarde alguns minutos para concluir a sincronização.

**Resultados**

Você pode importar usuários e grupos do servidor LDAP configurado recentemente.

Você pode importar, baixar, editar e excluir certificados do VMware Cloud Director. Você pode copiar os dados PEM do certificado para a área de transferência.

Este capítulo inclui os seguintes tópicos:

- [Importar certificados confiáveis](#)
- [Importar certificados para a biblioteca de certificados](#)

## Importar certificados confiáveis

Você pode importar certificados de servidores com o qual o VMware Cloud Director se comunica, como vCenter Server, NSX Manager e assim por diante.

Ao usar o VMware Cloud Director no modo FIPS, você deve usar chaves privadas compatíveis com FIPS. Você pode usar o pyOpenSSL para gerar chaves privadas no formato PKCS#8 compatível com FIPS. Se você gerar chaves privadas PKCS#8 usando o OpenSSL, elas não serão compatíveis com FIPS. Para obter mais informações sobre o modo FIPS, consulte [Ativar o modo FIPS nas células do grupo de servidores](#) ou [Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director](#).

### Pré-requisitos

Verifique se você está conectado como **administrador do sistema** ou **administrador da organização**.

### Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Gerenciamento de Certificados**, selecione **Certificados Confiáveis** e clique em **Importar**.
- 3 Carregue um arquivo PEM que contenha os certificados que você deseja importar e clique em **Importar**.
- 4 (Opcional) Edite o nome do certificado.
- 5 Clique em **Importar**.

### Próximo passo

- Baixe um certificado.
- Edite o nome de um certificado.
- Exclua um certificado.
- Copie os dados PEM para a área de transferência.

## Importar certificados para a biblioteca de certificados

Na biblioteca de certificados do VMware Cloud Director, você pode importar certificados usados ao criar entidades que devem ser protegidas, como servidores, edge gateways e assim por diante.

A biblioteca de certificados contém informações sobre certificados únicos, cadeias de certificados, chaves privadas, datas de expiração do certificado, as entidades que os certificados protegem e assim por diante.

Ao usar o VMware Cloud Director no modo FIPS, você deve usar certificados autoassinados e chaves privadas compatíveis com FIPS. Você pode gerar certificados não criptografados e chaves privadas autoassinadas usando o pyOpenSSL. Se você gerar certificados autoassinados e chaves privadas usando o OpenSSL, estes não serão compatíveis com FIPS. Para obter mais informações sobre o modo FIPS, consulte [Ativar o modo FIPS nas células do grupo de servidores](#) ou [Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director](#).

### Pré-requisitos

Verifique se você está conectado como **administrador do sistema** ou **administrador da organização**.

### Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Gerenciamento de Certificados**, selecione **Biblioteca de Certificados** e clique em **Importar**.
- 3 Insira um nome e, opcionalmente, uma descrição para este certificado na biblioteca de certificados e clique em **Avançar**.
- 4 Carregue um arquivo PEM que contenha a cadeia de certificados que você deseja importar e clique em **Avançar**.
- 5 (Opcional) Carregue um arquivo de chave privada.  
O seu arquivo de chave privada pode não estar protegido com uma frase-chave.
- 6 Clique em **Importar**.

### Resultados

O certificado importado é exibido na lista de certificados disponíveis durante a criação de entidades que você deve proteger.

### Próximo passo

- Baixe um certificado.
- Edite o nome e a descrição de um certificado.
- Exclua um certificado. Você pode excluir apenas certificados que não protegem nenhuma entidade.
- Copie os dados PEM do certificado para a área de transferência.

# Gerenciar a organização

# 16

Como **administrador da organização**, você pode modificar várias configurações dentro da sua organização. Você pode modificar o nome da organização, as configurações de e-mail, as configurações de domínio, os metadados, as políticas e assim por diante.

Você pode usar a API do VMware Cloud Director para assinar mensagens sobre eventos e tarefas na sua organização por meio do protocolo MQTT. Consulte as informações sobre como assinar eventos e tarefas usando um cliente MQTT no *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Este capítulo inclui os seguintes tópicos:

- [Editar nome e descrição da organização](#)
- [Modificar suas configurações de e-mail](#)
- [Testar configurações de SMTP](#)
- [Modificar configurações de domínio das máquinas virtuais da organização](#)
- [Trabalhando com vários sites](#)
- [Configurar e gerenciar implantações multissite](#)
- [Noções básicas sobre leases](#)
- [Modificar as políticas de lease de modelos de vApp e vApps na sua organização](#)
- [Modificar as políticas de senha e de conta de usuário da organização](#)
- [Criar um painel de avisos](#)

## Editar nome e descrição da organização

Você pode editar o nome completo e a descrição da sua organização.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.



2 Em **Configurações**, clique em **Gerais**.

A lista de configurações gerais, como o nome da organização, a URL padrão, o nome completo e a descrição, é exibida.

3 Para modificar o nome completo e a descrição da organização, clique em **Editar**.

4 Aplique as alterações necessárias e clique em **Salvar**.

## Modificar suas configurações de e-mail

Você pode rever e modificar as configurações de e-mail padrão que foram definidas quando o administrador do sistema criou sua organização

O VMware Cloud Director envia e-mails de alerta quando tem informações importantes para relatar, por exemplo, quando um armazenamento de dados está ficando sem espaço. Por padrão, uma organização envia alertas de e-mail aos administradores do sistema ou a uma lista de endereços de e-mail especificados no nível do sistema usando um servidor SMTP especificado no nível do sistema. Você pode modificar as configurações de e-mail no nível da organização se quiser que o VMware Cloud Director envie alertas dessa organização para um conjunto diferente de endereços de e-mail do que aqueles especificados no nível do sistema ou se quiser que a organização use um servidor SMTP para enviar alertas diferente do que servidor e especificado no nível do sistema.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

1 Na barra de navegação superior, clique em **Administração**.

2 Em **Configurações**, clique em **E-mail**.

São exibidas as configurações de e-mail da sua organização.

3 Clique em **Editar**.

4 Edite as configurações do servidor SMTP na guia **Servidor SMTP**.

- a Selecione se deseja usar um servidor SMTP personalizado ou o padrão.
- b Se você optar por usar um servidor SMTP personalizado, insira o nome do host DNS ou o endereço IP do servidor SMTP na caixa de texto **Nome do servidor SMTP**.
- c (Opcional) Insira a porta do servidor SMTP.
- d (Opcional) Selecione se deseja exigir autenticação e insira um nome de usuário e uma senha.

- 5 Para editar as configurações de notificação, clique na guia **Configurações de notificação**.
  - a Selecione para usar configurações de notificação personalizadas.
  - b Insira o endereço de e-mail que aparece como o remetente dos e-mails da organização.
  - c (Opcional) Insira o texto a ser usado como prefixo de assunto de e-mail.
  - d (Opcional) Selecione se deseja enviar notificações para todos os administradores da organização ou para endereços de e-mail específicos.
  - e (Opcional) Se você optar por enviar notificações para endereços de e-mail específicos, insira esses endereços de e-mail separando-os com uma vírgula.
- 6 Clique em **Salvar**.

## Testar configurações de SMTP

Depois de modificar as configurações de e-mail da sua organização, você poderá testar as configurações de SMTP.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 Em **Configurações**, clique em **E-mail**.

São exibidas as configurações de e-mail da sua organização.
- 3 Clique em **Testar**.
- 4 Insira um endereço de e-mail de destino e a senha do servidor SMTP para testar as configurações de SMTP e clique no botão **Testar**.

## Modificar configurações de domínio das máquinas virtuais da organização

Você pode definir um domínio padrão do Windows no qual as máquinas virtuais criadas na sua organização podem entrar. As máquinas virtuais podem sempre ingressar em um domínio para o qual elas têm credenciais, independentemente de você especificar um domínio padrão ou não.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 Em **Configurações**, clique em **Personalização do Convidado**.
- 3 Selecione para habilitar o ingresso no domínio para as máquinas virtuais na organização.
- 4 Insira o nome do domínio, o nome de usuário e a senha.  
As credenciais que você insere aplicam-se a um usuário de domínio regular, e não a um administrador de domínio.
- 5 (Opcional) Insira uma unidade organizacional da conta.
- 6 Clique em **Salvar**.

## Trabalhando com vários sites

O recurso Multissite do VMware Cloud Director permite que um provedor de serviços ou um tenant de várias instalações distribuídas geograficamente do VMware Cloud Director (grupos de servidor) gerencie e monitore as instalações e suas organizações como entidades únicas.

O portal de tenants do VMware Cloud Director fornece aos **administradores de organização** uma forma de associar organizações em sites associados.

Para obter mais informações sobre associações, consulte o *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

## Configurar e gerenciar implantações multissite

Depois que um **administrador de sistema** tiver associado dois sites, os **administradores de organização** em qualquer site membro poderão começar a associar suas organizações.

Para criar uma associação entre duas organizações (vamos chamá-las de Org-A e Org-B), você deve ser um **administrador de organização** em ambas para poder fazer login em cada uma, recuperar seus dados de associação locais e enviar esses dados recuperados para a outra organização.

---

**Importante** O processo de associar duas organizações pode ser logicamente decomposto em duas operações de emparelhamento complementares. A primeira operação (neste exemplo) emparelha a Org-A no Site-A com a Org-B no Site-B. Em seguida, você deve emparelhar a Org-B no Site-B com a Org-A no Site-A. Até que ambos os pares estejam concluídos, a associação estará incompleta.

---

### Pré-requisitos

- Os sites ocupados pelas organizações devem estar associados.
- Você deve ser um **administrador de sistema** em ambos os sites ou um **administrador de organização** em ambas as organizações.

## Procedimentos

- 1 Faça login no portal do tenant do VMware Cloud Director da Org-A no Site-A para recuperar seus dados de associação locais.

- a Clique em **Administração**.
- b Em **Configurações**, clique em **Multissite**.
- c Para baixar os dados no formato XML, clique em **Exportar dados de associação locais**.

O navegador salva os dados em um arquivo na pasta Downloads.

- 2 Faça login no portal do tenant do VMware Cloud Director da Org-B no Site-B para enviar os dados de associação locais da Org-A no Site-A.

- a Clique em **Administração**.
- b Em **Configurações**, clique em **Multissite**.
- c Clique em **Criar nova associação de organização**.

Envie os dados de associação baixados na [Etapa 1](#) para a Org-B clicando na seta de upload abaixo da caixa de texto **Nova Associação XML** e selecionando os dados de associação locais que você baixou na [Etapa 1](#).

- d Clique em **Avançar** para verificar e enviar os dados.
- e Clique em **Concluir** para exibir a organização associada.
- f Para visualizar os detalhes da organização associada ou excluir a associação, clique no cartão **Nome da Organização**.

- 3 Conclua a associação repetindo as Etapas 1 e 2 para recuperar os dados de associação locais da Org-B e enviá-los para a Org-A.

## Noções básicas sobre leases

A criação de uma organização envolve a especificação de leases. Os leases oferecem um nível de controle sobre o armazenamento de uma organização e recursos de computação, especificando a quantidade máxima de tempo que os vApps podem ser executados e quais modelos de vApps e vApp podem ser armazenados.

O objetivo de um lease de tempo de execução é evitar que os vApps inativos consumam recursos de computação. Por exemplo, se um usuário iniciar um vApp e entrar de férias sem interrompê-lo, o vApp continuará a consumir recursos.

Um lease de tempo de execução começa quando um usuário inicia um vApp. Quando um lease de tempo de execução expira, o VMware Cloud Director interrompe o vApp.

O objetivo de uma locação de armazenamento é evitar que os vApps e os modelos do vApp não utilizados consumam recursos de armazenamento. Uma locação de armazenamento de vApp começa quando um usuário interrompe o vApp. As locações de armazenamento não afetam os vApps em execução. Uma locação de armazenamento de modelo vApp começa quando um usuário adiciona o modelo vApp a um vApp, adiciona o modelo vApp a um espaço de trabalho, baixa, copia ou muda de lugar o modelo vApp.

Quando uma locação de armazenamento expira, o VMware Cloud Director marca o modelo vApp/vApp como expirado ou exclui o modelo vApp/vApp, dependendo da política organizacional definida.

## Modificar as políticas de lease de modelos de vApp e vApps na sua organização

Você pode rever e modificar as políticas padrão que foram definidas pelo administrador do sistema quando sua organização foi criada.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 Em **Configurações**, clique em **Políticas**.

Você pode visualizar as políticas padrão definidas pelo **administrador do sistema**.

- 3 Clique em **Editar**.
- 4 Edite os leases do vApp.

Os leases do vApp fornecem um nível de controle sobre os recursos de processamento e armazenamento da organização, especificando a quantidade máxima de tempo que os vApps podem ser executados e armazenados. Você também pode especificar o que acontece com os vApps quando seu lease de armazenamento expira.

- a Para definir por quanto tempo os vApps podem ser executados antes de serem interrompidos automaticamente, insira o lease máximo de tempo de execução.
- b Selecione uma ação de expiração de tempo de execução, como desligar ou suspender.
- c Para definir por quanto tempo os vApps interrompidos permanecem disponíveis antes de serem limpos automaticamente, insira o lease de armazenamento máximo.
- d Selecione uma ação de limpeza de armazenamento, como excluir permanentemente os vApps ou movê-los para os itens expirados.

5 Edite o lease de modelo de vApp.

Os leases de modelo de vApp fornecem um nível de controle sobre os recursos de computação e armazenamento da organização, especificando a quantidade máxima de tempo que os modelos de vApp podem ser armazenados. Você também pode especificar o que acontece com os modelos de vApp quando seu lease de armazenamento expira.

- a Para definir por quanto tempo os modelos de vApp permanecem disponíveis antes de serem limpos automaticamente, insira o lease de armazenamento máximo.
- b Selecione uma ação de limpeza de armazenamento, como excluir permanentemente os modelos de vApp ou movê-los para os itens expirados.

6 Clique em **OK**.

## Modificar as políticas de senha e de conta de usuário da organização

Você pode revisar e modificar a senha padrão e as políticas de conta de usuário que foram definidas pelo administrador do sistema quando sua organização foi criada.

As políticas de senha e de conta de usuário definem o comportamento do VMware Cloud Director quando um usuário insere uma senha inválida.

### Pré-requisitos

Esta operação exige direitos incluídos na função predefinida de **Administrador da organização** ou um conjunto equivalente de direitos.

### Procedimentos

1 Na barra de navegação superior, clique em **Administração**.

2 Em **Configurações**, clique em **Políticas**.

Você pode visualizar as políticas padrão definidas pelo **administrador do sistema**.

3 Clique em **Editar**.

4 Ative o bloqueio de uma conta de usuário após determinado número de tentativas de login inválido.

5 Digite o número de tentativas de login inválidas antes que a conta seja bloqueada.

6 Insira o intervalo de tempo em minutos no qual o usuário com uma conta bloqueada não pode fazer login novamente.

7 Clique em **OK**.

## Criar um painel de avisos

Você pode criar notificações que são exibidas na parte superior das páginas da interface de usuário no Tenant Portal. As mensagens podem ser exibidas para os usuários em uma organização ou os usuários em todas as organizações.

Não é possível editar avisos depois de criá-los.

### Pré-requisitos

Verifique se você está conectado como **administrador do sistema**.

### Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **Avisos** e clique em **Novo**.
- 3 Na caixa de descrição, adicione o texto da notificação.

Você pode usar a Markdown básica para adicionar links às notificações.

- 4 Selecione a prioridade da mensagem.

Mensagens de prioridade diferentes são exibidas como cores diferentes. As notificações são exibidas na ordem de prioridade. Avisos obrigatórios não podem ser descartados ou adiados.

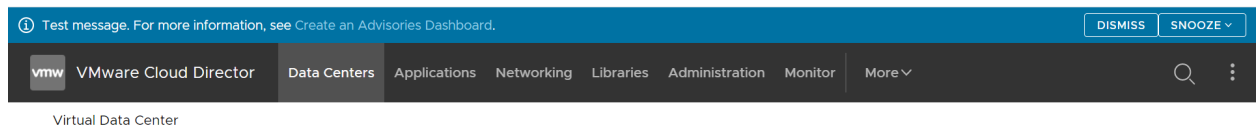
- 5 Selecione o período para o qual você deseja que a notificação seja exibida na interface de usuário.

Você pode exibir todos os avisos na guia **Avisos**. No entanto, eles são exibidos para o grupo de usuários selecionado apenas durante o período selecionado.

- 6 Clique em **OK**.

### Resultados

A notificação é exibida acima da barra de navegação superior do portal selecionado.



### Próximo passo

Exclua a notificação selecionando o botão de opção ao lado dele e clicando em **Excluir**. Os avisos são exibidos na guia **Avisos** mesmo depois de expirarem. Para removê-los da lista, você deve excluí-los.

# Como trabalhar com a biblioteca de serviços

# 17

Os itens da biblioteca de serviços no VMware Cloud Director são fluxos de trabalho do vRealize Orchestrator que ampliam os recursos de gerenciamento de nuvem e possibilitam aos administradores de provedores ou de tenants monitorar e manipular serviços diferentes.

Este capítulo inclui os seguintes tópicos:

- [Procurar um serviço](#)
- [Executar um serviço](#)

## Procurar um serviço

A página **Biblioteca de Serviços** no portal do tenant do VMware Cloud Director lista o conjunto de fluxos de trabalho do vRealize Orchestrator que são importados para o VMware Cloud Director e publicados na sua organização.

### Pré-requisitos

Esta operação requer que os direitos de Biblioteca de serviços sejam incluídos na função de usuário predefinida.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Biblioteca de Serviço**.

A lista de itens de serviço aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada cartão mostra o nome do serviço e uma marca que corresponde à categoria de serviço na qual o vRealize Orchestrator é importado.

- 2 Na caixa de texto **Pesquisar** na parte superior da página, insira a primeira palavra do nome do serviço ou do nome da categoria ao qual o serviço pertence.

a Selecione se você deseja pesquisar entre nomes do serviço ou entre categorias.

Os resultados da pesquisa aparecem em uma exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética.



## Executar um serviço

Você pode executar um serviço na página Biblioteca de Serviços no portal do tenant VMware Cloud Director.

### Pré-requisitos

Esta operação requer que os direitos de Biblioteca de serviços sejam incluídos na função de usuário predefinida.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Biblioteca de Serviço**.

A lista de itens de serviço aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada cartão mostra o nome do serviço e uma marca que corresponde à categoria de serviço na qual o vRealize Orchestrator é importado.

- 2 Procure o serviço que você deseja executar.

- 3 Clique em **Executar** no cartão do serviço.

Uma nova caixa de diálogo é aberta. Você deve inserir valores para os parâmetros de entrada necessários do serviço.

- 4 Clique em **Concluir** para confirmar a execução do serviço.

### Próximo passo

Você pode monitorar o status da execução no modo de exibição de **Tarefas recentes**. Para obter mais informações, consulte [Exibir tarefas](#).

# Gerenciamento de entidades definidas

# 18

A partir do VMware Cloud Director 10.2, os provedores de serviços podem usar a API do VMware Cloud Director para criar extensões que fornecem recursos do VMware Cloud Director adicionais para os tenants. Se um provedor de serviços concedeu a você acesso, você poderá gerenciar entidades definidas e compartilhá-las com outros tenants.

Os provedores de serviços podem criar Runtime Defined Entities (RDEs), permitindo que as extensões armazenem e manipulem as informações específicas da extensão no VMware Cloud Director. Por exemplo, uma extensão do Kubernetes pode armazenar informações sobre os clusters do Kubernetes que ele gerencia nas RDEs. A extensão pode então fornecer APIs de extensão para gerenciar esses clusters usando as informações das RDEs.

## Acesso às entidades definidas

Dois mecanismos complementares controlam o acesso às RDEs.

- **Direitos:** quando um provedor de serviços cria um tipo de RDE, ele cria um pacote de direitos para o tipo. Um provedor de serviços deve atribuir um ou mais dos cinco direitos específicos de tipo: **Exibir: TYPE**, **Editar: TYPE**, **Controle Total: TYPE**, **Exibição do Administrador: TYPE** e **Controle Total do Administrador: TYPE**.

Os direitos **Exibir: TYPE**, **Editar: TYPE** e **Controle Total: TYPE** funcionam apenas em combinação com uma entrada ACL.

- **Lista de controle de acesso (ACL)** - A tabela da ACL contém entradas que definem os usuários de acesso com entidades específicas no sistema. Ela fornece um nível extra de controle sobre as entidades. Por exemplo, enquanto um direito **Editar: TYPE** especifica que um usuário pode modificar entidades às quais eles têm acesso, a tabela de ACL define quais entidades o usuário tem acesso.

Tabela 18-1. Direitos e entradas da ACL para operações da RDE

Operação da entidade	Opção	Descrição
Leitura	Direito <b>Exibição do Administrador: TYPE</b>	Os usuários com esse direito podem ver todas as RDEs desse tipo dentro de uma organização.
	Direito <b>Exibir: TYPE</b> e entrada da ACL <b>&gt;= Exibir</b>	Os usuários com esse direito e uma ACL de nível de leitura podem exibir RDEs desse tipo.
Modificar	Direito <b>Controle Total do Administrador: TYPE</b>	Os usuários com esse direito podem criar, exibir, modificar e excluir RDEs desse tipo em todas as organizações.
	Direito <b>Editar: TYPE</b> e entrada da ACL <b>&gt;= Alterar</b>	Os usuários com esse direito e a ACL de nível de modificação podem criar, exibir e modificar RDEs desse tipo.
Excluir	Direito <b>Controle Total do Administrador: TYPE</b>	Os usuários com esse direito podem criar, exibir, modificar e excluir RDEs desse tipo em todas as organizações.
	Direito <b>Controle Total: TYPE</b> e entrada da ACL <b>= Controle Total</b>	Os usuários com esse direito e a ACL de nível de controle total podem criar, exibir, modificar e excluir RDEs desse tipo.

## Compartilhando as entidades definidas com outro usuário

Se um **administrador do sistema** publicou o pacote de direitos para um tipo de entidade definida e tiver concedido a você acesso `ReadWrite` ou `FullControl`, ou se você for o proprietário da entidade definida, poderá compartilhar o acesso a essas entidades com outros usuários.

- 1 Atribua o direito **Exibir: TYPE**, **Editar: TYPE** ou **Controle Total: TYPE** do pacote para as funções de usuário que você deseja ter o nível específico de acesso à entidade definida.

---

**Observação** Você deve estar conectado como **administrador do sistema** ou **administrador da organização** para atribuir direitos.

---

Por exemplo, se você quiser que os usuários com a função **tkg\_viewer** exibam clusters do Tanzu Kubernetes na organização, deverá adicionar o direito **Exibir: Tanzu Kubernetes Guest Cluster** à função. Se você quiser que os usuários com a função **tkg\_author** criem, exibam e modifiquem os clusters do Tanzu Kubernetes nesta organização, adicione o direito **Editar: Tanzu Kubernetes Guest Cluster** a essa função. Se você quiser que os usuários com a função **tkg\_admin** criem, exibam, modifiquem e excluam os clusters do Tanzu Kubernetes nesta organização, adicione o direito **Controle Total: Tanzu Kubernetes Guest Cluster** à função.

- 2 Conceda ao usuário específico uma Lista de controle de acesso (ACL) fazendo a seguinte chamada de REST API.

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

*Access\_level* deve ser `ReadOnly`, `ReadWrite` ou `FullControl`. *User\_ID* deve ser o ID do usuário ao qual você deseja conceder o acesso à entidade definida.

Você deve ter acesso `ReadWrite` ou `FullControl` a uma entidade para conceder acesso ACL a essa entidade.

Os usuários com a função de **tkg\_viewer**, descritas no exemplo, não podem conceder acesso ACL. Os usuários com a função **tkg\_author** ou **tkg\_admin** podem compartilhar o acesso a uma entidade `VMWARE:TKGCLUSTER` com usuários que têm a função **tkg\_viewer**, **tkg\_author** ou **tkg\_admin** concedendo a eles acesso ACL usando a solicitação de API.

Os usuários com o direito **Controle Total do Administrador: Tanzu Kubernetes Guest Cluster** podem conceder acesso à ACL para qualquer entidade `VMWARE:TKGCLUSTER`.

Você também pode usar chamadas REST API para revogar o acesso ou para exibir quem tem acesso à entidade. Consulte a documentação da REST API do VMware Cloud Director em [code.vmware.com](https://code.vmware.com).

## Alterando o proprietário de uma entidade definida

O proprietário de uma entidade definida ou um usuário com o direito **Controle Total do Administrador: TYPE** pode transferir a propriedade para outro usuário atualizando o modelo de entidade definido e alterando o campo de proprietário com o ID do novo proprietário.

Este capítulo inclui os seguintes tópicos:

- [Como trabalhar com definições de entidades personalizadas](#)

## Como trabalhar com definições de entidades personalizadas

As definições de entidades personalizadas no VMware Cloud Director são tipos de objeto que estão vinculados a tipos de objeto do vRealize Orchestrator. Os usuários dentro de uma organização do VMware Cloud Director podem possuir, gerenciar e alterar esses tipos conforme a necessidade. Executando serviços, os usuários da organização podem instanciar as entidades personalizadas e aplicar ações sobre as instâncias dos objetos.

### Procurar uma entidade personalizada

Você pode procurar as entidades personalizadas que foram publicadas na sua organização.

#### Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

#### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 Na caixa de texto **Pesquisa** no topo da página, insira uma palavra ou um caractere do nome da entidade que você deseja localizar.

Os resultados da pesquisa aparecem em uma exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética.

### Editar uma definição da entidade personalizada

Você pode modificar o nome e a descrição de uma entidade personalizada. Não é possível alterar o tipo de entidade ou o tipo de objeto vRealize Orchestrator ao qual a entidade está vinculada. Essas são as propriedades padrão da entidade personalizada. Se você quiser modificar qualquer uma das propriedades padrão, você deve excluir a definição da entidade personalizada e recriá-la.

#### Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, selecione **Ações > Editar**.

Uma nova caixa de diálogo é aberta.

- 3 Modifique o nome ou a descrição da definição da entidade personalizada.

- 4 Clique em **OK** para confirmar a alteração.

## Adicione uma definição da entidade personalizada

Você pode criar uma entidade personalizada e mapeá-la para um tipo de objeto existente do vRealize Orchestrator.

### Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 Para adicionar uma nova entidade personalizada, clique em **Novo**.

Uma nova caixa de diálogo é aberta.

- 3 Siga as etapas do assistente de **Definição da Entidade Personalizada**.

Etapas	
Nome e Descrição	Insira um nome e, opcionalmente, uma descrição para a nova entidade. Insira um nome para o tipo de entidade, por exemplo, <code>sshHost</code> .
vRO	No menu suspenso, selecione o vRealize Orchestrator que você usará para mapear a definição de entidade personalizada.
<b>Observação</b> Se você tiver mais de um servidor do vRealize Orchestrator, deverá criar uma definição de entidade personalizada para cada um deles separadamente.	

Etapa	
Tipo	<p>Clique no ícone de lista de exibição para navegar pelos tipos de objeto disponíveis do vRealize Orchestrator agrupados por plug-ins. Por exemplo, <b>SSH &gt; Host</b>.</p> <p>Se você souber o nome do tipo, poderá inseri-lo diretamente na caixa de texto. Por exemplo, <code>SSH:Host</code>.</p>
Revisão	Revise os detalhes que você especificou e clique em <b>Concluído</b> para concluir a criação.

## Resultados

A nova definição da entidade personalizada aparece no modo de exibição do cartão.

## Instâncias de Entidades Personalizadas

A execução de um fluxo de trabalho do vRealize Orchestrator com um parâmetro de entrada como um tipo de objeto que já está definido como uma definição de entidade personalizada no VMware Cloud Director mostra o parâmetro de saída como uma instância de uma entidade personalizada.

## Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.


## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, clique em **Instâncias**.

As instâncias disponíveis são exibidas em uma exibição de grade.

- 3 Clique na barra de lista (  ) à esquerda de cada entidade para exibir os fluxos de trabalho associados.

Clicar em um fluxo de trabalho inicia uma execução de fluxo de trabalho que toma a instância da entidade como um parâmetro de entrada.

## Associar uma ação a uma entidade personalizada

Associando uma ação a uma definição de entidade personalizada, você pode executar um conjunto de fluxos de trabalho do vRealize Orchestrator nas instâncias de uma determinada entidade personalizada.

## Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, selecione **Ações > Associar Ação**.

Uma nova caixa de diálogo é aberta.

- 3 Siga as etapas do assistente **Associar a entidade personalizada ao fluxo de trabalho do VRO**.

Etapa	Detalhes
Selecionar Fluxo de Trabalho do VRO	Selecione um dos fluxos de trabalho listados. Esses são os fluxos de trabalho que estão disponíveis na página da <b>Biblioteca de Serviços</b> .
Selecionar Parâmetro de Entrada do Fluxo de Trabalho	Selecione um parâmetro de entrada disponível na lista. Você pode associar o tipo do fluxo de trabalho do vRealize Orchestrator ao tipo de definição da entidade personalizada.
Revisar Associação	Analisar os detalhes que você especificou e clique em <b>Concluído</b> para concluir a associação.

## Exemplo

Por exemplo, se você tiver uma entidade personalizada do tipo `SSH:Host`, poderá associá-la ao fluxo de trabalho do `Add a Root Folder to SSH Host` selecionando o parâmetro de entrada do `sshHost`, que corresponde ao tipo da entidade personalizada.

## Desassociar uma ação de uma definição de entidade personalizada

Você pode remover um fluxo de trabalho do vRealize Orchestrator na lista de ações associadas.

## Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.



## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, selecione **Ações > Desassociar Ação**.

Uma nova caixa de diálogo é aberta.

- 3 Selecione o fluxo de trabalho que você deseja remover e clique em **Desassociar Ação**.

O fluxo de trabalho do vRealize Orchestrator não está mais associado à entidade personalizada.

## Publicar uma entidade personalizada

Você deve publicar uma entidade personalizada para que os usuários de outros tenants ou provedores de serviços possam executar fluxos de trabalho usando as instâncias de entidades personalizadas como parâmetros de entrada.

### Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

## Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, selecione **Ações > Publicar**.

Uma nova caixa de diálogo é aberta.

- 3 Escolha se deseja publicar a definição de entidade personalizada para provedores de serviços, todos os tenants ou somente para tenants selecionados.

- 4 Clique em **Salvar** para confirmar a alteração.

A definição da entidade personalizada fica disponível para os participantes selecionados.

## Excluir uma entidade personalizada

Você pode excluir uma definição de entidade personalizada se a entidade personalizada não estiver mais em uso, se tiver sido configurada incorretamente ou se quiser mapear o tipo do vRealize Orchestrator para uma entidade personalizada diferente.

### Pré-requisitos

Esta operação requer que os direitos de Entidade personalizada sejam incluídos na função de usuário predefinida.

### Procedimentos

- 1 Na barra de navegação superior, clique em **Bibliotecas** e, em **Serviços**, selecione **Definições de Entidade Personalizada**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, classificados por nomes em ordem alfabética. Cada placa mostra o nome da entidade personalizada, o tipo do vRealize Orchestrator ao qual a entidade é mapeada, o tipo de entidade e uma descrição, se disponível.

- 2 No cartão da entidade personalizada selecionada, selecione **Ações > Excluir**.
- 3 Confirme a exclusão.

A entidade personalizada é removida da exibição do cartão.