

Guia do portal de administração do provedor de serviços do VMware Cloud Director

Modificado em 8 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

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

Copyright © 2018-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

- 1 Guia do Portal de Administração do Provedor de Serviços da VMware Cloud Director™ 10**
- 2 Introdução ao VMware Cloud Director Service Provider Admin Portal 11**
 - Visão geral da administração do VMware Cloud Director 11
 - Faça login no VMware Cloud Director Service Provider Admin Portal 15
 - Usar a pesquisa rápida do VMware Cloud Director 15
 - Exibir tarefas 16
 - Parar uma tarefa em andamento 17
 - Exibir eventos 17
 - Definir preferências do usuário 18
 - Limites de tamanho de nomes e descrições 19
- 3 Gerenciamento de recursos do vSphere 21**
 - Como adicionar recursos do NSX e do vCenter Server 22
 - Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager 23
 - Detectando e adotando vApps 27
 - Atribuir a chave de licença do NSX no vCenter Server 28
 - Registrar uma instância do NSX-T Manager 29
 - Gerenciamento do balanceamento de carga avançado do NSX 29
 - Acesso aos componentes do vSphere por meio de endpoints e proxies do VMware Cloud Director 34
 - Criar um endpoint 35
 - Adicionar um proxy para acessar os recursos do vCenter Server subjacentes 36
 - Gerenciar os certificados de proxy e as CRLs 37
 - Adicionar recursos de nuvem 37
 - Centros de dados virtuais do provedor 38
 - Criar um centro de dados virtual do provedor 38
 - Redes Externas 42
 - Pools de Redes 46
 - Exibir as instâncias do vCenter Server 50
 - Modificar configurações do vCenter Server 52
 - Ativar ou desativar uma instância do vCenter Server 52
 - Reconectar uma instância do vCenter Server 53
 - Atualizar uma instância do vCenter Server 53
 - Atualizar as políticas de armazenamento de uma instância do vCenter Server 54
 - Cancelar registro de uma instância do vCenter Server 54
 - Modificar as configurações do NSX Manager 54

Modificar as configurações do NSX-T Manager	55
Excluir uma instância do NSX-T Manager	56
Configurando e gerenciando implantações em multissites	56
Listas de recursos multissites	60

4 Gerenciamento de centros de dados virtuais do provedor 61

Ativar ou desativar um centro de dados virtual do provedor	61
Excluir um data center virtual de provedor	62
Editar as configurações gerais de um data center virtual de provedor	62
Mesclar data centers virtuais de provedor	63
Visualizar os centros de dados virtuais de organização de um centro de dados virtual de provedor	64
Visualizar os datastores em um centro de dados virtual do provedor	64
Visualizar as redes externas em um centro de dados virtual de provedor	65
Usando o Kubernetes com o VMware Cloud Director	66
Criando um cluster do vSphere with VMware Tanzu	70
Criar um cluster do Kubernetes nativo	77
Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition	79
Gerenciamento das políticas de armazenamento de VM em um centro de dados virtual do provedor	80
Habilitando a criptografia da VM em políticas de armazenamento de um centro de dados virtual do provedor	81
Adicionar uma política de armazenamento de VM a um datacenter virtual do provedor	82
Ativar ou desativar uma política de armazenamento de VM em um centro de dados virtual do provedor	83
Excluir uma política de armazenamento de VM de um data center virtual de provedor	84
Modificar os metadados de uma política de armazenamento de VM em um data center virtual de provedor	84
Ativando a configuração de operações de E/S por segundo	85
Editar as configurações de política de armazenamento de VDC de provedor	87
Editar os tipos de entidade aos quais uma política de armazenamento oferece suporte	88
Gerenciamento dos pools de recursos em um centro de dados virtual do provedor	89
Adicionar um pool de recursos a um data center virtual de um provedor	89
Ativar ou desativar um pool de recursos em um centro de dados virtual de provedor	90
Desanexar um pool de recursos de um centro de dados virtual de provedor	91
Modificar os metadados para um centro de dados virtual de provedor	91

5 Gerenciamento de organizações 93

Noções básicas sobre leases	93
Criar uma organização	94
Ativar ou desativar uma organização	94
Excluir uma organização	95
Configurar os catálogos para uma organização	95

Configurar as políticas para uma organização	96
Migrar Armazenamento de Tenant	97
Gerenciar cotas sobre o consumo de recursos de uma organização	99

6 Gerenciamento de centros de dados virtuais da organização 100

Noções básicas sobre modelos de alocação	100
Uso sugerido dos modelos de alocação	102
Modelo de alocação flexível	103
Modelo de alocação do pool de alocação	105
Modelo de alocação Pago pelo Uso	106
Modelo de alocação de pool de reserva	107
Compreendendo políticas de dimensionamento e posicionamento de VM	108
Criar uma política de posicionamento de VM em um VDC do provedor	113
Criar uma política de posicionamento de VM global	114
Editar uma política de posicionamento de VM	115
Adicionar uma política de posicionamento de VM a um VDC de organização	116
Excluir uma política de posicionamento de VM	117
Atributos das políticas de dimensionamento de VM	118
Criar uma política de dimensionamento de VM	119
Adicionar uma política de dimensionamento de VM a um VDC de organização	120
Editar uma política de dimensionamento de VM	121
Excluir uma política de dimensionamento de VM	121
Usando o Kubernetes com o VMware Cloud Director	122
Adicionar uma política do Kubernetes do VDC de Organização	125
Editar uma política do Kubernetes do VDC de organização	127
Criar um cluster do Tanzu Kubernetes	128
Criar um cluster do Kubernetes nativo	130
Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition	132
Criar um centro de dados virtual da organização	133
Ativar ou desativar um centro de dados virtual da organização	136
Excluir um centro de dados virtual da organização	136
Gerenciando modelos de centro de dados virtual	137
Criar um modelo de centro de dados virtual da organização	137
Instanciar um centro de dados virtual a partir de um modelo	141
Editar um modelo de VDC da organização	142
Modificar o nome e a descrição de um centro de dados virtual da organização	146
Modificar as configurações do modelo de alocação de um centro de dados virtual da organização	146
Modificação das configurações de armazenamento de um centro de dados virtual de organização	146
Habilitando a criptografia da VM em políticas de armazenamento de um centro de dados virtual da organização	147

Modificar as configurações de provisionamento da VM de um centro de dados virtual de organização	148
Adicionar uma política de armazenamento de VM a um data center virtual da organização	149
Alterar a política de armazenamento padrão em um centro de dados virtual da organização	149
Editar o limite de uma política de armazenamento em um centro de dados virtual da organização	150
Modificar os metadados de uma política de armazenamento de VM em um centro de dados virtual da organização	150
Ativar ou desativar uma política de armazenamento em um centro de dados virtual da organização	151
Excluir uma política de armazenamento de um centro de dados virtual da organização	152
Editar as configurações da política de armazenamento de VDC de organização	152
Editar as configurações de rede de um data center virtual de organização	153
Configurando a rede do centro de dados virtual cruzada	154
Modificar os metadados de um centro de dados virtual da organização	156
Visualizar os pools de recursos de um centro de dados virtual de organização	156
Gerenciamento do firewall distribuído em um centro de dados virtual da organização	157
Ativar o firewall distribuído em um centro de dados virtual de organização	157
Adicionar uma regra de firewall distribuído	158
Editar uma regra de firewall distribuído	161
Objetos de agrupamento personalizados	162
Trabalhando com grupos de segurança	165
Trabalho com marcas de segurança	169

7 Gerenciando Edge Gateways do NSX Data Center for vSphere 174

Como trabalhar com edge clusters do NSX Data Center for vSphere	175
Adicionar um edge gateway do NSX Data Center for vSphere	176
Configurando serviços do edge gateway do NSX Data Center for vSphere	179
Gerenciando um firewall do edge gateway do NSX Data Center for vSphere	179
Gerenciando o DHCP do edge gateway do NSX Data Center for vSphere	183
Adicionar uma regra de SNAT ou de DNAT	188
Configuração de roteamento avançado	191
Balanceamento de Carga	200
Proteger o acesso usando redes virtuais privadas	215
Gerenciamento de certificados SSL	242
Objetos de agrupamento personalizados	250
Visualizar o uso de redes e as alocações de IP em um edge gateway	253
Edição das propriedades do edge gateway	253
Ativar ou desativar o roteamento distribuído em um edge gateway	254
Modificar as configurações de redes externas e do edge gateway	254
Editar as configurações gerais de um edge gateway	254

Editar o gateway padrão de um edge gateway	255
Editar as configurações de IP de um edge gateway	256
Editar os pools de IPs subalocados em um edge gateway	256
Editar os limites de taxa em um edge gateway	257
Reimplantar um edge gateway	257
Excluir um edge gateway	257
Estatísticas e logs para um edge gateway	258
Visualizar estatísticas	258
Ativar Log	258
Habilitar o acesso pela linha de comando SSH a um edge gateway	260

8 Gerenciando Edge Gateways do NSX-T Data Center 261

Redes externas dedicadas	261
Adicionar um edge gateway do NSX-T Data Center	262
Adicionar um conjunto de IPs a um edge gateway do NSX-T Data Center	263
Adicionar uma regra de firewall do edge gateway do NSX-T Data Center	264
Adicionar uma regra de SNAT ou DNAT a um edge gateway do NSX-T	265
Configurar um serviço de encaminhador de DNS em um edge gateway do NSX-T	268
Editar as alocações de IP de um edge gateway do NSX-T	269
Alocação de IPs rápida	270
Criar perfis de portas de aplicativos personalizados	271
VPN baseada em políticas IPsec para edge gateways do NSX-T Data Center	271
Configurar VPN IPsec baseada em política do NSX-T	272
Personalizar o perfil de segurança de um túnel VPN IPsec	273
Configurar serviços de rede externa dedicada	275
Gerenciar aviso de rota	275
Definir configurações gerais de BGP	276
Criar uma lista de prefixos de IP	277
Adicionar um vizinho BGP	278
Gerenciamento de balanceamento de carga avançado do NSX em um edge gateway do NSX-T Data Center	280
Ativar o balanceador de carga em um Edge Gateway do NSX-T Data Center.	280
Atribuir um grupo de mecanismos de serviço a um edge gateway do NSX-T Data Center	281
Editar as configurações de um grupo de mecanismos de serviço	281
Adicionar um pool de servidores do balanceador de carga	282
Criar um serviço virtual	284

9 Gerenciando instâncias dedicadas do vCenter Server 287

Habilitar o acesso ao tenant de um vCenter Server anexado	290
Publicar um vCenter Server dedicado	290

10 Gerenciamento de funções e administradores do sistema 292

- Gerenciando direitos e funções 292
 - Funções predefinidas e seus direitos 294
 - Direitos de Administrador do Sistema 296
 - Direitos em funções predefinidas de tenant global 310
 - Gerenciamento dos pacotes de direitos 317
 - Gerenciamento das funções do tenant global 320
 - Gerenciamento das funções do provedor 323
- Gerenciamento de grupos e usuários de provedor 326
 - Gerenciamento de usuários do provedor 326
 - Gerenciamento de grupos de provedor 329

11 Gerenciamento de configurações do sistema 331

- Modificar as configurações gerais do sistema 331
- Configurações gerais do sistema 332
- Ativar o modo FIPS nas células do grupo de servidores 334
- Definir as configurações de e-mail do sistema 336
- Alterar a licença do VMware Cloud Director 337
- Definir as configurações de sincronização de catálogo 337
- Criar um painel de avisos 338
- Configurar e monitorar tarefas de bloqueio e notificações 338
 - Configurar um agente AMQP 339
 - Definir as configurações da tarefa de bloqueio 340
 - Monitorar tarefas bloqueadas 341
- Configurar endereços públicos 341
- Gerenciamento de provedores de identidade 343
 - Gerenciamento de conexões LDAP 344
 - Configurar seu sistema para usar um provedor de identidade SAML 347
- Gerenciamento de certificados 349
 - Importar certificados confiáveis 349
 - Importar certificados para a biblioteca de certificados 350
- Gerenciando plug-ins 351
 - Carregar um plug-in 351
 - Ativar ou desativar um plug-in 352
 - Excluir um plug-in 352
 - Publicar ou cancelar a publicação de um plug-in de uma organização 352
- Personalizando os portais do VMware Cloud Director 353
- Configurar a política de senha 355
- Configurar os serviços do vSphere 355

12 Monitorando o VMware Cloud Director 357

[Relatórios de custos e VMware Cloud Director](#) 357

[Visualizar informações de uso para um centro de dados virtual do provedor](#) 358

13 Gerenciamento de serviços 359

[Integração do vRealize Orchestrator ao VMware Cloud Director](#) 359

[Registrar uma instância do vRealize Orchestrator no VMware Cloud Director](#) 360

[Criar uma categoria de serviço](#) 361

[Editar uma categoria de serviço](#) 361

[Importar um serviço](#) 362

[Procurar um serviço](#) 362

[Executar um serviço](#) 363

[Alterar uma categoria de serviço](#) 364

[Cancelar o registro de um serviço](#) 364

[Publicar um serviço](#) 365

14 Gerenciamento de entidades definidas 366

[Compartilhamento de entidades definidas](#) 367

[Gerenciamento de entidades personalizadas](#) 369

[Procurar uma entidade personalizada](#) 369

[Editar uma definição da entidade personalizada](#) 370

[Adicione uma definição da entidade personalizada](#) 370

[Instâncias de Entidades Personalizadas](#) 371

[Associar uma ação a uma entidade personalizada](#) 372

[Desassociar uma ação de uma entidade personalizada](#) 372

[Publicar uma entidade personalizada](#) 373

[Excluir uma entidade personalizada](#) 373

Guia do Portal de Administração do Provedor de Serviços da VMware Cloud Director™

1

O *Guia do VMware Cloud Director Service Provider Admin Portal* fornece informações sobre como usar o Service Provider Admin Portal. Você pode usar o service provider admin portal para gerenciar e monitorar as organizações, os direitos, as funções, os usuários e os grupos na sua nuvem. Você também pode criar e gerenciar as redes de centros de dados virtuais da organização com suporte do NSX-T.

Público-alvo

Este guia destina-se a administradores de provedor de serviços que desejam usar os recursos fornecidos no VMware Cloud Director Service Provider Admin Portal.

Glossário de publicações técnicas da VMware

As publicações técnicas da VMware fornecem um glossário dos termos que você pode não conhecer. Para ver as definições dos termos da forma como são usados na documentação técnica da VMware, acesse <https://docs.vmware.com>.

Introdução ao VMware Cloud Director Service Provider Admin Portal

2

O VMware Cloud Director Service Provider Admin Portal é uma interface dedicada para administradores de provedor de serviços.

Este capítulo inclui os seguintes tópicos:

- Visão geral da administração do VMware Cloud Director
- Faça login no VMware Cloud Director Service Provider Admin Portal
- Usar a pesquisa rápida do VMware Cloud Director
- Exibir tarefas
- Parar uma tarefa em andamento
- Exibir eventos
- Definir preferências do usuário
- Limites de tamanho de nomes e descrições

Visão geral da administração do VMware Cloud Director

Com o VMware VMware Cloud Director, você pode criar nuvens seguras de multiempresa pela criação de pools de recursos de infraestrutura virtual em centros de dados virtuais e expô-las aos usuários por meio de portais da Web e interfaces de programação como serviço baseado em catálogo totalmente automatizado.

O Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director fornece informações sobre o acréscimo de recursos ao sistema, criando e provisionando organizações, gerenciando recursos e organizações e monitorando o sistema.

Recursos do vSphere e NSX

O VMware Cloud Director se baseia nos recursos do vSphere para fornecer a CPU e memória para executar máquinas virtuais. Além disso, datastores do vSphere fornecem armazenamento para arquivos de máquina virtual e outros arquivos necessários para operações de máquina virtual. O VMware Cloud Director também usa switches distribuídos do vSphere, grupos de portas do vSphere e o NSX Data Center for vSphere para oferecer suporte à rede de máquinas virtuais.

O VMware Cloud Director também pode usar recursos do NSX-T Data Center. Para obter informações sobre como registrar uma instância do NSX-T Manager com a nuvem, consulte *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director* ou *Guia de programação da API do VMware Cloud Director*.

Você pode usar os recursos subjacentes do vSphere e NSX para criar recursos de nuvem.

A partir da versão 9.7, o VMware Cloud Director pode atuar como um servidor proxy HTTP, com o qual você pode permitir que as organizações acessem o ambiente do vSphere subjacente.

Recursos de Nuvem

Os recursos de nuvem são uma abstração dos recursos subjacentes do vSphere. Eles fornecem os recursos computacionais e de memória para as máquinas virtuais do VMware Cloud Director e vApps. Um vApp é um sistema virtual que contém uma ou mais máquinas virtuais individuais com parâmetros que definem detalhes operacionais. Os recursos de nuvem também fornecem acesso ao armazenamento e à conectividade de rede.

Os recursos de nuvem incluem centros de dados virtuais de provedor e organização, redes externas, redes de centros de dados virtuais de organização e pools de redes.

Antes de adicionar recursos de nuvem ao VMware Cloud Director, você deve adicionar recursos do vSphere.

Instâncias e proxies dedicados do vCenter Server

Uma instância dedicada do vCenter Server é um recurso de nuvem que encapsula toda a instalação do vCenter Server. Uma instância dedicada do vCenter Server inclui um ou mais proxies que são pontos de acesso para diferentes componentes do ambiente do vSphere subjacente. O provedor pode criar e habilitar proxies e instâncias dedicadas do vCenter Server. O provedor pode publicar uma instância dedicada do vCenter Server em tenants.

Para criar e gerenciar instâncias e proxies dedicados do vCenter Server, você pode usar o Service Provider Admin Portal ou a vCloud OpenAPI. Consulte [Capítulo 9 Gerenciando instâncias dedicadas do vCenter Server](#) e *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

Datacenters virtuais do provedor

Um datacenter virtual do provedor combina os recursos de computação e de memória de um único pool de recursos do vCenter Server com os recursos de armazenamento de um ou mais datastores disponíveis para esse pool de recursos.

Um datacenter virtual do provedor pode usar os recursos de rede de uma instância de NSX Manager que está associada à instância de vCenter Server ou de uma instância de NSX-T Manager que está registrada com a nuvem.

Você pode criar vários datacenters virtuais do provedor para usuários em diferentes locais geográficos ou unidades de negócios ou para usuários com diferentes requisitos de desempenho.

Datacenters virtuais da organização

Um datacenter virtual da organização fornece recursos para uma organização e é particionado de um datacenter virtual do provedor. Os datacenters virtuais da organização fornecem um ambiente onde os sistemas virtuais podem ser armazenados, implantados e operados. Eles também fornecem armazenamento para mídia virtual como disquetes e CD ROMs.

Uma única organização pode ter vários datacenters virtuais da organização.

Rede do VMware Cloud Director

O VMware Cloud Director oferece suporte a três tipos de redes.

- Redes externas
- Redes de datacenters virtuais da organização
- Redes do vApp

Algumas redes de datacenters de organização e todas as redes de vApp têm suporte de pools de redes.

Redes Externas

Uma rede externa é uma rede lógica e diferenciada com base em um grupo de portas do vSphere. As redes do datacenter virtual da organização podem se conectar às redes externas para fornecer conectividade de Internet às máquinas virtuais dentro de um vApp.

Começando com a versão 9.5, o VMware Cloud Director oferece suporte às redes externas IPv6. Uma rede externa IPv6 oferece suporte às sub-redes IPv4 e IPv6, e uma rede externa IPv4 oferece suporte às sub-redes IPv4 e IPv6.

Por padrão, somente **Administradores do Sistema** criam e gerenciam redes externas.

Redes de datacenters virtuais da organização

Uma rede de datacenters virtuais da organização pertence a um datacenter virtual da organização do VMware Cloud Director e está disponível para todos os vApps na organização. Uma rede de datacenters virtuais da organização permite que os vApps em uma organização se comuniquem entre si. Para fornecer conectividade externa, você pode conectar uma rede de datacenters virtuais da organização a uma rede externa. Você também pode criar uma rede isolada de datacenters virtuais da organização que é interna à organização.

O VMware Cloud Director 9.5 oferece suporte a IPv6 para redes de datacenters virtuais da organização diretas e roteadas.

Começando com o VMware Cloud Director 9.5, os **Administradores do Sistema** podem criar redes de datacenters virtuais isoladas com suporte do comutador lógico NSX-T. Os **Administradores da Organização** podem criar redes de datacenters virtuais isoladas com suporte de pools de redes.

O VMware Cloud Director 9.5 também apresenta a rede de datacenters virtuais cruzada, configurando redes estendidas em grupos de datacenters virtuais.

Por padrão, somente **Administradores do Sistema** podem criar redes de datacenters virtuais cruzadas e diretas. **Administradores do Sistema** e **Administradores da Organização** podem gerenciar redes de datacenters virtuais da organização, embora haja alguns limites quanto às ações que os **Administradores da Organização** podem fazer.

Redes do vApp

Uma rede do vApp pertence a um vApp e permite que as máquinas virtuais no vApp se comuniquem entre si. Para ativar um vApp para se comunicar com outros vApps na organização, você pode conectar a rede do vApp a uma rede de datacenters virtuais da organização. Se a rede de datacenters virtuais da organização está conectada a uma rede externa, o vApp pode se comunicar com vApps de outras organizações. Redes do vApp têm suporte de pools de redes.

A maioria dos usuários com acesso a um vApp pode criar e gerenciar suas próprias redes do vApp. Para obter informações sobre como trabalhar com as redes em um vApp, consulte *Guia do Portal de Tenants do VMware Cloud Director*.

Pools de Redes

Um pool de redes é um grupo de redes não diferenciadas que está disponível para uso dentro de um datacenter virtual da organização. Um pool de redes tem o suporte de recursos de rede do vSphere como IDs de VLAN ou grupos de portas. O VMware Cloud Director usa pools de redes para criar redes de datacenters virtuais da organização internas e roteadas para NAT e todas as redes do vApp. O tráfego de rede em cada rede em um pool é isolado na camada 2 de todas as outras redes.

Cada datacenter virtual da organização no VMware Cloud Director pode ter um pool de redes. Vários datacenters virtuais da organização podem compartilhar um pool de redes. O pool de redes para um datacenter virtual da organização fornece as redes criadas para satisfazer a cota de rede em um datacenter virtual da organização.

Somente **Administradores do Sistema** podem criar e gerenciar pools de redes.

Organizações

O VMware Cloud Director oferece suporte ao recurso multiempresa usando as organizações. Uma organização é uma unidade de administração para um conjunto de usuários, grupos e recursos de computação. Os usuários autenticam no nível da organização, fornecendo credenciais estabelecidas pelo administrador da organização quando o usuário foi criado ou importado. Os **Administradores do Sistema** criam e provisionam as organizações, enquanto os **Administradores da Organização** gerenciam catálogos, grupos e usuários da organização. As tarefas de **Administradores da Organização** são descritas no *Guia do Portal de Tenants do VMware Cloud Director*.

Usuários e grupos

Uma organização pode conter um número arbitrário de usuários e grupos. Os **Administradores da Organização** podem criar usuários e importar usuários e grupos a partir de um serviço de diretório como o LDAP. O **Administrador do Sistema** gerencia o conjunto de direitos disponíveis para cada organização. O **Administrador do Sistema** pode criar e publicar funções de tenant global para uma ou mais organizações. O **Administrador da Organização** pode criar funções locais em suas organizações.

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 para criar seus próprios vApps. Um **Administrador do Sistema** pode permitir que uma organização publique um catálogo para torná-lo disponível para outras organizações. Os **Administradores da Organização** podem decidir quais itens de catálogo são fornecidos aos seus usuários.

Faça login no VMware Cloud Director Service Provider Admin Portal

Você pode acessar o VMware Cloud Director Service Provider Admin Portal usando um navegador da Web.

Pré-requisitos

Você deve ter os direitos de administrador do sistema para acessar o VMware Cloud Director Service Provider Admin Portal.

Procedimentos

- 1 Em um navegador, digite a URL do Service Provider Admin Portal do seu site do VMware Cloud Director e pressione Enter.

Por exemplo, digite **https://vcloud.exemplo.com/provedor**.

- 2 Faça login com o nome de usuário do administrador do sistema e a senha.

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 Service Provider Admin Portal, você pode ver as tarefas recentes e seu status.

Você pode usar a exibição de tarefas recentes para monitorar o status das tarefas no seu Service Provider Admin Portal. Essa exibição pode ser uma boa primeira etapa para solucionar problemas no seu ambiente.

Ao lado do botão **Tarefas Recentes**, as tarefas em execução e com falha aparecem em azul e vermelho, respectivamente.

Procedimentos

- 1 No canto inferior esquerdo, clique em **Tarefas Recentes**.
- 2 (Opcional) Modifique e filtre a lista de tarefas recentes.

Resultados

Uma lista de tarefas recentes é exibida, juntamente com o status da tarefa, o tipo, o iniciador e a hora de início e de conclusão.

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**.

Limites de tamanho de nomes e descrições

Siga estas diretrizes ao inserir valores no VMware Cloud Director.

Os valores da cadeia para o atributo `name` e os elementos `Description` e `ComputerName` têm limitações de tamanho que dependem do objeto ao qual eles estão anexados.

Tabela 2-1. Limites de tamanho no objeto Propriedades

Objeto	Propriedade	Tamanho máximo de caracteres
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128
Vdc	Description	256
Vm	name	128

Tabela 2-1. Limites de tamanho no objeto Propriedades (continuação)

Objeto	Propriedade	Tamanho máximo de caracteres
Vm	ComputerName	15 no Windows, 63 em todas as outras plataformas
Vm	Description	256

Gerenciamento de recursos do vSphere

3

O VMware Cloud Director deriva seus recursos de uma infraestrutura virtual subjacente do vSphere. Depois de registrar recursos do vSphere no VMware Cloud Director, você poderá alocar esses recursos para que as organizações dentro da instalação do vSphere os usem.

O VMware Cloud Director usa um ou mais ambientes do vCenter Server para dar suporte aos centros de dados virtuais dele. Desde a versão 9.7, o VMware Cloud Director também pode usar um ambiente do vCenter Server para encapsular um SDDC com um ou mais proxies. Você pode ativar que os tenants usem esses proxies como Access Points para o ambiente subjacente do vSphere a partir do VMware Cloud Director com as contas do VMware Cloud Director deles.

Antes de poder usar uma instância do vCenter Server no VMware Cloud Director, você deve anexar a instância do vCenter Server.

Quando você cria um centro de dados virtual de provedor com o suporte de uma instância conectada do vCenter Server, essa instância do vCenter Server aparece como publicada em um provedor de serviços, ou com escopo definido para o provedor. Para obter informações sobre como criar um centro de dados virtual de provedor, consulte [Criar um centro de dados virtual do provedor](#).

Ao criar um SDDC que encapsula uma instância conectada do vCenter Server, você dedica o vCenter Server a um tenant. Essa instância do vCenter Server aparece como publicada em um tenant, também chamado de escopo do tenant. Para obter informações sobre como criar um SDDC, consulte [Capítulo 9 Gerenciando instâncias dedicadas do vCenter Server](#).

Observação Por padrão, com uma instância conectada do vCenter Server, você pode criar um VDC de provedor ou uma instância dedicada do vCenter Server. Se você tiver criado um VDC de provedor com suporte por uma instância do vCenter Server, não poderá usar essa instância do vCenter Server para criar uma instância dedicada do vCenter Server, e vice-versa.

Gerenciamento de SSL centralizado

A partir da versão 10.1, o VMware Cloud Director está se movendo para uma área de armazenamento centralizada e ciente do tenant para o gerenciamento de certificados. Dessa forma, o VMware Cloud Director centraliza todos os certificados em um local para que os **administradores de sistema** e os **administradores de organização** possam visualizar, auditar e

gerenciar todos os certificados em uso por vários componentes no sistema. Você pode usar a API do VMware Cloud Director para adicionar, atualizar ou remover certificados da nova área de armazenamento com reconhecimento de tenant. Consulte *Referência de esquemas de API do VMware Cloud Director*.

Ao adicionar ou editar uma nova instância do vCenter Server, do NSX Manager ou do NSX-T Manager, a interface de usuário do VMware Cloud Director testa esse endpoint para qualquer certificado que ele esteja apresentando. O VMware Cloud Director adiciona a uma área de armazenamento de certificado centralizada qualquer certificado que você decidir confiar.

Este capítulo inclui os seguintes tópicos:

- [Como adicionar recursos do NSX e do vCenter Server](#)
- [Acesso aos componentes do vSphere por meio de endpoints e proxies do VMware Cloud Director](#)
- [Adicionar recursos de nuvem](#)
- [Exibir as instâncias do vCenter Server](#)
- [Modificar configurações do vCenter Server](#)
- [Ativar ou desativar uma instância do vCenter Server](#)
- [Reconectar uma instância do vCenter Server](#)
- [Atualizar uma instância do vCenter Server](#)
- [Atualizar as políticas de armazenamento de uma instância do vCenter Server](#)
- [Cancelar registro de uma instância do vCenter Server](#)
- [Modificar as configurações do NSX Manager](#)
- [Modificar as configurações do NSX-T Manager](#)
- [Excluir uma instância do NSX-T Manager](#)
- [Configurando e gerenciando implantações em multissites](#)
- [Listas de recursos multissites](#)

Como adicionar recursos do NSX e do vCenter Server

O VMware Cloud Director se baseia nos recursos do vSphere para fornecer CPU, memória e armazenamento para executar máquinas virtuais. Além disso, desde a versão 9.7, o VMware Cloud Director pode atuar como um servidor HTTP entre tenants e o ambiente subjacente do vSphere.

Para obter informações sobre requisitos do sistema do VMware Cloud Director e versões compatíveis do vCenter Server e ESXi, consulte as *Matrizes de interoperabilidade de produtos VMware* em http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager

Você pode anexar uma instância do vCenter Server para que os recursos dela fiquem disponíveis para uso no VMware Cloud Director. Você pode anexar uma instância do vCenter Server junto com sua instância associada do NSX Manager. No caso de instâncias dedicadas do vCenter Server ou daquelas associadas a uma instância do NSX-T Manager, você pode anexar uma instância do vCenter Server isoladamente.

O VMware Cloud Director pode usar uma instância do vCenter Server com sua instância do NSX Manager associada ou com uma instância do NSX-T Manager.

Se você quiser que o VMware Cloud Director use esta instância do vCenter Server com sua instância do NSX Manager associada, deverá anexar as instâncias do vCenter Server e NSX Manager juntas.

Se você quiser que o VMware Cloud Director use esta instância do vCenter Server com uma instância do NSX-T Manager, deverá anexar apenas a instância do vCenter Server. Depois de anexar apenas a instância do vCenter Server, você deve [Registrar uma instância do NSX-T Manager](#).

Observação Depois de anexar apenas uma instância do vCenter Server, você não pode adicionar sua instância do NSX Manager associada em uma etapa posterior. Você pode cancelar o registro e anexar novamente a instância do vCenter Server em conjunto com sua instância do NSX Manager associada.

Você pode anexar uma instância do vCenter Server a qualquer site do seu ambiente VMware Cloud Director.

Você pode anexar uma instância do vCenter Server diretamente acessível ou anexar uma instância do vCenter Server que esteja atrás de um proxy. Usando o OpenAPI do vCloud, você pode usar as configurações no VMware Cloud Director para criar uma conexão com proxy entre uma instância do VMware Cloud Director e a instância do vCenter Server adicionada a ela. Dessa forma, as instâncias do VMware Cloud Director e do vCenter Server podem existir em diferentes locais ou sites.

Para anexar uma instância do vCenter Server que esteja atrás de um proxy, primeiro, você deve declarar uma configuração de proxy. Em seguida, você deve anexar uma instância do vCenter Server e configurar o VMware Cloud Director para usar a configuração do proxy ao acessar a instância do vCenter Server. Você também pode anexar uma solução do NSX Data Center for vSphere por meio de um proxy. O VMware Cloud Director não é compatível com configurações de proxy para o NSX-T Data Center. Você não precisa de configurações SSL adicionais ou de um proxy adicional para o Platform Services Controller e a instância do vCenter Server com que está registrada.

Pré-requisitos

- Se você tiver configurado o VMware Cloud Director para verificar os certificados de SSO do vCenter e vSphere, verifique se carregou os certificados do vCenter Server para o VMware Cloud Director. Para obter informações sobre as configurações gerais do sistema, consulte [Modificar as configurações gerais do sistema](#).
- Se você tiver configurado o VMware Cloud Director para verificar os certificados do NSX Manager, verifique se carregou os certificados do NSX Manager para o VMware Cloud Director. Para obter informações sobre as configurações gerais do sistema, consulte [Modificar as configurações gerais do sistema](#).

Procedimentos

1 Adicionar a instância do vCenter Server

Para adicionar uma instância do vCenter Server, insira os detalhes de acesso do vCenter Server.

2 (Opcional) Adicione a instância de NSX Manager associada

Se deseja que VMware Cloud Director use esta instância do vCenter Server com sua instância do NSX Manager associada, você deve adicionar os detalhes do acesso do NSX Manager.

Adicionar a instância do vCenter Server

Para adicionar uma instância do vCenter Server, insira os detalhes de acesso do vCenter Server.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **Instâncias do vCenter Server** e clique em **Adicionar**.
- 3 Se você tiver uma implantação do VMware Cloud Director multissite, no menu **do Site**, selecione o site ao qual deseja adicionar essa instância do vCenter Server e clique em **Avançar**.
- 4 Insira um nome e, opcionalmente, uma descrição para a instância do vCenter Server no VMware Cloud Director.
- 5 Insira a URL da instância do vCenter Server.

Se a porta padrão for usada, você poderá ignorar o número da porta. Se for usada uma porta personalizada, inclua o número da porta

Por exemplo, `https://FQDN_or_IP_address:<custom_port_number>`.
- 6 Insira o nome de usuário e a senha da conta de **administrador** do vCenter Server.
- 7 (Opcional) Para desativar a instância do vCenter Server após o registro, desative a alternância **Habilitada**.

8 Configure a URL do vCenter Server Web Client.

Opção	Descrição
Usar Serviços do vSphere para fornecer URL	Para usar essa opção, você deve usar a API do vCloud para configurar o VMware Cloud Director para usar o vSphere Lookup Service.
URL do vSphere Web Client	Para usar essa opção, você deve inserir a URL do vSphere Web Client. Por exemplo, https://example.vmware.com/vsphere-client .

9 Clique em **Avançar**.

- 10 Se o endpoint não tiver um certificado confiável, na janela **Certificado de Confiança**, confirme se você confia no endpoint.

Em um ambiente multissite, se você estiver conectado a um site do vCloud Director 10.0 ou tentando registrar uma instância do vCenter Server em um site do vCloud Director 10.0, o VMware Cloud Director não adicionará o endpoint à área de armazenamento de certificados centralizada.

- Para adicionar o endpoint à área de armazenamento de certificados centralizada e continuar, clique em **Confiar**.
- Se você não confiar nesse endpoint, clique em **Cancelar** e repita [Etapa 5](#) para [Etapa 9](#) com um endpoint confiável.

- 11 (Opcional) Pule a adição da instância do NSX Manager que está associada à instância do vCenter Server desligando a opção **Definir Configurações** e clique em **Avançar**.

Se quiser que o VMware Cloud Director use esta instância do vCenter Server com uma instância do NSX-T Manager, você deverá adicionar apenas a instância do vCenter Server.

Observação Não é possível adicionar a instância do NSX Manager associada em um estágio posterior. Você pode cancelar o registro e anexar novamente a instância do vCenter Server em conjunto com sua instância do NSX Manager associada.

- 12 Se você quiser adicionar um vCenter Server dedicado ao tenant que não será usado como um VDC de provedor, ative a opção **Habilitar acesso ao tenant**.

Depois de adicionar a instância do vCenter Server a VMware Cloud Director, as informações relacionadas ao tenant aparecem na exibição de detalhes da instância.

- 13 Se você quiser que o VMware Cloud Director gere proxies padrão para os serviços de instância do vCenter Server e SSO, ative a opção **Gerar proxies**.

Depois de adicionar a instância do vCenter Server a VMware Cloud Director, os proxies aparecem na guia **Proxies** em **Recursos do vSphere**.

- 14 Na página **Pronto para ser Concluído**, revise os detalhes do registro e clique em **Concluir**.

(Opcional) Adicione a instância de NSX Manager associada

Se deseja que VMware Cloud Director use esta instância do vCenter Server com sua instância do NSX Manager associada, você deve adicionar os detalhes do acesso do NSX Manager.

Procedimentos

- 1 Na página **NSX-V Manager**, deixe a opção **Definir Configurações** ativada.

- 2 Insira a URL da instância do NSX Manager.

Se a porta padrão for usada, você poderá ignorar o número da porta. Se for usada uma porta personalizada, inclua o número da porta

Por exemplo, `https://FQDN_or_IP_address:<custom_port_number>`.

- 3 Insira o nome de usuário e a senha da conta do **administrador** do NSX.
- 4 (Opcional) Para habilitar a rede de datacenters virtuais cruzados para os datacenters virtuais apoiados por esta instância do vCenter Server, ative a alternância **de rede entre VDCs** e insira as propriedades de implantação da VM de controle e um nome para o escopo do provedor de rede.

As propriedades de implantação da VM de controle são usadas para implantar um dispositivo na instância do NSX Manager para componentes da rede de datacenters virtuais cruzados, como um roteador universal.

Opção	Descrição
Escopo do provedor de rede	Corresponde ao domínio de falha da rede nas topologias de rede dos grupos de centros de dados. Por exemplo, boston-fault1 . Para obter informações sobre como gerenciar vários grupos de centros de dados virtuais, consulte o <i>Guia do Portal de Tenants do VMware Cloud Director</i> .
Caminho do Pool de Recursos	O caminho hierárquico para um pool de recursos específico na instância do vCenter Server, a partir do cluster, <i>Cluster/Resource_Pool_Parent/Target_Resource</i> . Por exemplo, TestbedCluster1/mgmt-rp . Como alternativa, você pode inserir a ID de referência do objeto gerenciado do pool de recursos. Por exemplo, resgroup-1476 .
Nome do repositório de dados	O nome do repositório de dados para hospedar os arquivos do dispositivo. Por exemplo, shared-disk-1 .
Interface de Gerenciamento	O nome da rede no vCenter Server ou no grupo de portas usado para a interface de gerenciamento do DLR de alta disponibilidade. Por exemplo, TestbedPG1 .

- 5 Clique em **Avançar**.
- 6 Se o endpoint não tiver um certificado confiável, na janela **Certificado de Confiança**, confirme se você confia no endpoint.
 - Para adicionar o endpoint à área de armazenamento de certificados centralizada e continuar, clique em **Confiar**.
 - Se você não confiar nesse endpoint, clique em **Cancelar** e repita [Etapa 2](#) para [Etapa 4](#) com um endpoint confiável.
- 7 Ative ou desative as definições de configuração de acesso.

8 Na página **Pronto para ser Concluído**, revise os detalhes do registro e clique em **Concluir**.

Próximo passo

- [Atribuir a chave de licença do NSX no vCenter Server.](#)
- [Criar um centro de dados virtual do provedor.](#)

Detectando e adotando vApps

Na configuração padrão, um VDC da organização detecta as VMs criadas em qualquer pool de recursos do vCenter Server que faça o backup do VDC. O sistema cria um vApp simplificado, de propriedade do administrador do sistema, para conter cada máquina virtual (VM) detectada. Depois que o administrador do sistema conceder acesso a um vApp detectado, você poderá fazer referência à VM quando compor ou recompor um vApp ou modificar o vApp para adotá-lo e importá-lo.

Os VApps detectados contêm exatamente uma VM e estão sujeitos a várias restrições que não se aplicam a vApps criados no VMware Cloud Director. Quer você os adote ou não, eles podem ser úteis como uma fonte de VMs para usar ao compor ou recompor um vApp.

Cada vApp detectado recebe um nome derivado do nome da VM do vCenter que ele contém e um prefixo especificado pelo administrador da sua organização.

Se você quiser detectar vApps adicionais, um administrador do sistema poderá usar a API do VMware Cloud Director para criar VDCs da organização que adotam pools de recursos especificados disponíveis em um VDC de Provedor. As VMs do vCenter nesses pools de recursos adotados aparecem no novo VDC como vApps detectados e são os candidatos para adoção.

Observação As máquinas virtuais com discos rígidos IDE são detectadas somente se estiverem no estado desligado.

Se uma ou mais VMs do vCenter não forem detectadas pelo VMware Cloud Director, você poderá investigar as possíveis razões depurando a Detecção de VM do vCenter Server. Para obter mais informações, consulte *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Ativando a detecção de VM

A detecção de VM está ativada por padrão. Para desativar a detecção de VM, um administrador de sistema deve desmarcar a caixa de seleção **Detecção de VM ativada** na guia **Configurações do Sistema > Geral**. Um administrador da organização pode usar a API do VMware Cloud Director para desativar a detecção de VMs para VDCs individuais ou para todos os VDCs em uma organização.

Usando uma VM de um vApp detectado

Depois que o administrador do sistema conceder acesso a um vApp detectado, você poderá usar sua VM da mesma maneira que pode usar uma VM que qualquer outro vApp ou modelo vApp contenha. Por exemplo, você pode especificá-lo ao criar um novo vApp. Você também pode clonar um vApp detectado ou modificar seu nome, descrição ou configurações de lease sem acionar o processo de adoção.

Adotando um vApp detectado

Você pode adotar um vApp detectado alterando sua rede vApp ou adicionando uma VM a esse vApp. Depois de um vApp detectado é adotado, o sistema o importa e o trata como se ele tivesse sido criado no VMware Cloud Director. Quando um vApp adotado é recuperado com uma solicitação da API do vCloud, ele inclui um elemento chamado `autoNature`. Esse elemento tem um valor de `false` se o vApp detectado foi adotado ou criado no VMware Cloud Director. Você não pode reverter um vApp adotado para um vApp detectado.

Se você excluir ou mover a VM que um vApp detectado contém, o sistema também removerá o vApp que contém. Esse comportamento não se aplica a vApps adotados.

O vApp criado para conter uma VM detectada do vCenter é semelhante àquele criado quando você importa manualmente uma VM como um vApp, mas é simplificado de maneiras que podem exigir que você o modifique antes de implantá-lo em seu VDC. Por exemplo, você pode ter que editar suas propriedades de rede e armazenamento e fazer outros ajustes específicos para as necessidades da sua organização.

Observação A adoção de uma máquina virtual não mantém as configurações de reserva, limite e compartilhamento de VM configuradas no vCenter Server. As máquinas virtuais importadas obtêm as configurações de alocação de recursos delas do centro de dados virtual da organização em que residem.

Atribuir a chave de licença do NSX no vCenter Server

Depois de anexar uma instância do vCenter Server junto com sua instância do NSX Manager associada, você deverá usar o vSphere Client para atribuir uma chave de licença para a instância do NSX Manager que dá suporte à rede do VMware Cloud Director.

Pré-requisitos

Esta operação está restrita aos administradores de sistema.

Procedimentos

- 1 Em um vSphere Client que está conectado ao sistema do vCenter Server, selecione **Início > Licenciamento**.
- 2 Para exibir o relatório, selecione **Ativo**.
- 3 Clique com botão direito do mouse no ativo do NSX Manager e selecione **Alterar a chave de licença**.

- 4 Selecione **Atribuir uma nova chave de licença** e clique em **Inserir Chave**.
- 5 Insira a chave de licença, insira um rótulo opcional para a chave e clique em **OK**.
Use a chave de licença do NSX Manager que você recebeu quando adquiriu o VMware Cloud Director. Você pode usar essa chave de licença em várias instâncias do vCenter Server.
- 6 Clique em **OK**.

Registrar uma instância do NSX-T Manager

Você pode registrar uma instância do NSX-T Manager no VMware Cloud Director, para que o VMware Cloud Director possa usar seus recursos de rede. Um data center virtual do provedor pode usar recursos de rede do NSX Data Center for vSphere ou do NSX-T Data Center.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **NSX-T Managers** e clique em **Adicionar**.
- 3 Se você tiver uma implantação do VMware Cloud Director multissite, no menu **do Site**, selecione o site ao qual deseja adicionar essa instância do NSX-T Manager e clique em **Avançar**.
- 4 Insira um nome e, opcionalmente, uma descrição para a instância do NSX-T Manager no VMware Cloud Director.
- 5 Insira a URL da instância do NSX-T Manager.
Por exemplo, **`https://FQDN_ou_endereço_IP`**.
- 6 Insira o nome de usuário e a senha da conta de **administrador** do NSX-T Manager.
- 7 Clique em **Salvar**.

Próximo passo

Para obter informações sobre como criar um data center virtual de provedor apoiado pelo NSX-T Data Center, consulte *Guia de programação da API do VMware Cloud Director* em <https://code.vmware.com>.

Gerenciamento do balanceamento de carga avançado do NSX

A partir da versão 10.2, o VMware Cloud Director fornece serviços de balanceamento de carga aproveitando os recursos do VMware NSX Advanced Load Balancer.

Como um **administrador do sistema**, você pode ativar e configurar o acesso aos serviços de balanceamento de carga para os centros de dados virtuais com suporte do NSX-T Data Center.

Os serviços de balanceamento de carga são associados a edge gateways do NSX-T Data Center, que podem ser colocados em escopo para um VDC de organização com suporte do NSX-T Data Center ou para um grupo de centros de dados com tipo de provedor de rede do NSX-T Data Center.

Depois de implantar e configurar o NSX Advanced Load Balancer para usar com a implantação do NSX-T Data Center, você registra os Controladores com o VMware Cloud Director.

Para obter informações sobre como configurar o NSX Advanced Load Balancer com o NSX-T, consulte a [Integração do AVI com o NSX-T](#).

Para obter informações sobre como implantar o NSX Advanced Load Balancer com o VMware Cloud Director, consulte [Implantação do NSX Advanced Load Balancer com o VMware Cloud Director](#).

Para usar a infraestrutura virtual fornecida pelo NSX Advanced Load Balancer, registre suas instâncias do NSX-T Cloud no VMware Cloud Director. Os controladores servem como uma camada de controle central para serviços de balanceamento de carga. Depois de registrar seus controladores, você pode gerenciá-los diretamente do VMware Cloud Director.

A infraestrutura de processamento de balanceamento de carga fornecida pelo NSX Advanced Load Balancer é organizada em grupos de mecanismos de serviço. Você pode atribuir mais de um grupo de mecanismos de serviço a um edge gateway do NSX-T Data Center no VMware Cloud Director. Todos os grupos de mecanismos de serviço que são atribuídos a um único edge gateway usam a mesma rede.

Um grupo de mecanismos de serviço tem um conjunto exclusivo de características de processamento que você define na criação.

Depois que um **administrador do sistema** atribui um grupo de mecanismos de serviço a um edge gateway, um **administrador da organização** pode criar e configurar serviços virtuais que são executados em um grupo de mecanismos de serviço específico.

Registrar uma instância do controlador

Para integrar o VMware Cloud Director com sua implantação do NSX Advanced Load Balancer, registre as instâncias do controlador com sua instância do VMware Cloud Director.

As instâncias do controlador servem como uma camada de controle central para os serviços de balanceamento de carga fornecidos pelo NSX Advanced Load Balancer.

Pré-requisitos

Instale e configure o NSX Advanced Load Balancer com sua instância do NSX-T Data Center.

Para obter informações sobre como configurar o NSX Advanced Load Balancer com o NSX-T, consulte a [Integração do AVI com o NSX-T](#).

Observação O FQDN ou o endereço IP que você usa para registrar o NSX-T Manager com o NSX Advanced Load Balancer deve corresponder ao FQDN ou ao endereço IP da instância do NSX-T Manager que você usou para registrar o NSX-T Data Center com o VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 Clique em **NSX-ALB** e, em seguida, clique em **Controladores**.

- 3 Para adicionar um controlador, clique em **Adicionar**.
- 4 Se você estiver usando uma implantação multissite, no menu suspenso, selecione um site no qual o controlador será registrado.
- 5 Registre a instância do Controlador.
 - a Insira um nome significativo e, opcionalmente, uma descrição para a instância do controlador.
 - b Insira a URL do controlador.
Por exemplo, `https://FQDN-or-IP-address`.
 - c Digite o nome do usuário e a senha para o Controlador.
 - d Clique em **Salvar**.

Resultados

A instância do controlador é exibida na lista como ativada.

Próximo passo

[Registrar uma Nuvem do NSX-T.](#)

Registrar uma Nuvem do NSX-T

Para usar a infraestrutura virtual fornecida pelo NSX Advanced Load Balancer, registre suas instâncias do NSX-T Cloud no VMware Cloud Director.

Uma Nuvem do NSX-T é uma construção no nível do provedor de serviços que consiste em um NSX-T Manager e uma zona de transporte do NSX-T Data Center.

O NSX-T Manager fornece uma exibição do sistema e é o componente de gerenciamento do NSX-T Data Center. Uma zona de transporte do NSX-T Data Center determina quais hosts e máquinas virtuais podem participar do uso de uma determinada rede.

Se houver várias zonas de transporte gerenciadas pelo mesmo NSX-T Manager, uma Nuvem do NSX-T separada encapsulará cada par de instâncias de zona de transporte do NSX-T Manager e do NSX-T Data Center.

Uma Nuvem do NSX-T tem um relacionamento um-para-um com um pool de redes com suporte de uma zona de transporte do NSX-T Data Center.

Pré-requisitos

[Registrar uma instância do controlador.](#)

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 Clique em **NSX-ALB** e, em seguida, clique em **Nuvs do NSX-T**.
- 3 Para adicionar uma Nuvem do NSX-T, clique em **Adicionar**.

- 4 No menu suspenso, selecione uma instância do controlador para a qual deseja criar a Nuvem do NSX-T.
- 5 Insira um nome e, opcionalmente, uma descrição para a Nuvem do NSX-T.
- 6 Selecione uma Nuvem disponível na lista.
- 7 Para importar a nuvem, clique em **Adicionar**.

Resultados

A nuvem importada é exibida na lista de Nuvens do NSX-T disponíveis.

Próximo passo

[Importar um grupo de mecanismos de serviço.](#)

Importar um grupo de mecanismos de serviço

Para fornecer recursos de gerenciamento de serviços virtuais aos seus tenants, importe os grupos de mecanismos de serviço para a sua implantação do VMware Cloud Director.

Um grupo de mecanismos de serviço é um domínio de isolamento que também define as propriedades do mecanismo de serviço compartilhado, como o tamanho, o acesso à rede e o failover.

Os recursos em um grupo de mecanismos de serviço podem ser usados em diferentes serviços virtuais, dependendo das necessidades dos seus tenants. Esses recursos não podem ser compartilhados entre diferentes grupos de mecanismos de serviço.

Você pode gerenciar e atualizar grupos de mecanismos de serviço usando o NSX Advanced Load Balancer. Depois de atualizar um grupo de mecanismos de serviço no NSX Advanced Load Balancer, você deve sincronizá-lo para atualizar suas configurações na UI do VMware Cloud Director.

Somente um grupo de mecanismos de serviço importado pode ser atribuído a um edge gateway.

Para importar um grupo de mecanismos de serviço, associe-o a uma Nuvem do NSX-T que já está registrada com sua instância do VMware Cloud Director.

Pré-requisitos

- [Registrar uma instância do controlador.](#)
- [Registrar uma Nuvem do NSX-T.](#)

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 Clique em **NSX-ALB** e, em seguida, clique em **Grupos de Mecanismos de Serviço**.
- 3 Para importar um grupo de mecanismos de serviço, clique em **Adicionar**.
- 4 No menu suspenso, selecione uma Nuvem do NSX-T.

5 Selecione um modelo de reserva.

- Para atribuir o grupo de mecanismos de serviço a um único edge gateway, selecione **Dedicado**.
- Para compartilhar o grupo de mecanismos de serviço entre vários edge gateways, selecione **Compartilhado**.

6 Insira um nome e, opcionalmente, uma descrição para o grupo de mecanismos de serviço.

7 Selecione uma instância do grupo de mecanismos de serviço.

8 Clique em **Adicionar**.

Próximo passo

Ative o balanceamento de carga no edge gateway e atribua o grupo de mecanismos de serviço ao edge gateway. Consulte [Gerenciamento de balanceamento de carga avançado do NSX em um edge gateway do NSX-T Data Center](#).

Sincronizar um grupo de mecanismos de serviço

Para atualizar as configurações de um grupo de mecanismos de serviço importado, você deve sincronizá-lo com o NSX Advanced Load Balancer.

Você pode gerenciar e atualizar grupos de mecanismos de serviço usando o NSX Advanced Load Balancer. Depois de atualizar um grupo de mecanismos de serviço no NSX Advanced Load Balancer, você deve sincronizá-lo para atualizar suas configurações na UI do VMware Cloud Director.

A sincronização de um grupo de mecanismos de serviço atualiza o registro local do modo de alta disponibilidade do grupo e o número máximo de serviços virtuais compatíveis com o grupo de mecanismos de serviço.

Importante 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

[Importar um grupo de mecanismos de serviço](#).

Procedimentos

1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.

- 2 Selecione **NSX-ALB** e, em seguida, clique em **Grupos de Mecanismos de Serviço**.
- 3 Selecione um grupo de mecanismos de serviço e clique em **Sincronizar**.

Resultados

As configurações do grupo de mecanismos de serviço são atualizadas.

Acesso aos componentes do vSphere por meio de endpoints e proxies do VMware Cloud Director

Você pode usar os endpoints do VMware Cloud Director para acessar o ambiente do vSphere subjacente. Quando os endpoints estão conectados a proxies, o VMware Cloud Director atua como um servidor proxy HTTP.

Endpoints

Um endpoint do VMware Cloud Director é um ponto de acesso a um componente do centro de dados, por exemplo, uma instância do vCenter Server, um host do ESXi ou uma instância do NSX Manager. Os usuários podem fazer login na interface de usuário ou na API dos componentes com ou sem proxy usando suas contas do VMware Cloud Director.

Criar uma instância do vCenter Server dedicada também cria um endpoint padrão para ela. Ao anexar a instância do vCenter Server, você também pode criar um proxy. No entanto, o endpoint padrão não está conectado a nenhum proxy por padrão. Você deve editar o endpoint padrão ou criar um novo para conectá-lo a um proxy.

Você pode criar, editar e excluir endpoints na guia **Endpoints** de uma instância do vCenter Server dedicada. Consulte [Criar um endpoint](#).

Proxies

Os proxies fornecidos pelo VMware Cloud Director são diferentes das configurações de proxy no VMware Cloud Director. Ao contrário dos proxies fornecidos pelo VMware Cloud Director que são delimitados para um tenant, as configurações de proxies do VMware Cloud Director estão no nível do provedor e não há recurso multiempresa.

Ao ativar e desativar um proxy fornecido pelo VMware Cloud Director, você pode permitir e interromper o acesso do tenant por meio desse proxy.

Você pode criar um proxy ao anexar uma instância do vCenter Server ao VMware Cloud Director ou depois. Se você criar um proxy ao anexar um vCenter Server e ativar o acesso do tenant, deverá conectar manualmente o proxy ao endpoint padrão.

Se a instância do vCenter Server usar um Platform Services Controller externo, o VMware Cloud Director também criará um proxy para o Platform Services Controller. Com proxies pai e filho, você pode ocultar determinados proxies dos tenants ou pode ativar e desativar grupos de proxies filho por meio de seus proxies pai. Para obter informações sobre como criar um proxy depois de adicionar uma instância do vCenter Server ao VMware Cloud Director, consulte [Adicionar um proxy para acessar os recursos do vCenter Server subjacentes](#).

Você pode editar, ativar, desativar e excluir proxies da guia **Proxies** em **Recursos de Infraestrutura**.

Observação Ao adicionar um proxy a uma instância do vCenter Server, você deve carregar o certificado e a impressão digital, para que os tenants possam recuperar esse certificado e essa impressão digital se o componente com proxy usar certificados autoassinados.

Para visualizar e gerenciar certificados e listas de certificados revogados (CRLs), consulte [Gerenciar os certificados de proxy e as CRLs](#).

Criar um endpoint

Você pode criar endpoints que os administradores e tenants podem usar para acessar o ambiente subjacente do vSphere.

Os endpoints devem ser anexados a instâncias do vCenter Server dedicadas e são visíveis aos tenants no menu **Ações** das instâncias do vCenter Server dedicadas. Se você ativar o acesso ao tenant quando adicionar uma instância do vCenter Server ao VMware Cloud Director, o VMware Cloud Director criará um endpoint padrão com a URL da instância do vCenter Server como uma URL de destino. Se você criar endpoints adicionais, poderá alterar o padrão.

Os endpoints podem servir como links entre instâncias do vCenter Server dedicadas e proxies. Os endpoints podem ter uma conexão com um proxy ou podem não ter uma conexão de proxy. Se um endpoint estiver conectado a um proxy, o destino do endpoint será a URL de destino, não a URL da interface de usuário do proxy conectado.

Pré-requisitos

Verifique se a instância do vCenter Server para a qual você deseja criar endpoints tem o acesso ao tenant ativado. Consulte [Habilitar o acesso ao tenant de um vCenter Server anexado](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Selecione uma instância do vCenter Server.
- 4 Na página com informações detalhadas do vCenter Server, clique na guia **Endpoints** e clique em **Novo**.
- 5 Insira um nome e uma URL de destino para o endpoint.
- 6 (Opcional) Torne este endpoint o padrão para esta instância do vCenter Server.

7 (Opcional) Faça uma conexão com um proxy.

8 Clique em **Salvar**.

Próximo passo

- Edite as configurações do endpoint.
- Exclua um endpoint. Se você quiser excluir o endpoint padrão, deverá selecionar outro como o padrão.

Adicionar um proxy para acessar os recursos do vCenter Server subjacentes

Se quiser que o VMware Cloud Director atue como servidor proxy HTTP para instâncias do vCenter Server e seus componentes, você poderá criar um proxy. Você pode criar proxies para instâncias do vCenter Server dedicadas e para as instâncias do vCenter Server que não têm um propósito definido.

Se você quiser gerar automaticamente um proxy do vCenter Server com certificados recuperados e impressão digital, poderá fazê-lo na grade das **Instâncias do vCenter Server** ou na exibição de detalhes do vCenter Server. Se o vCenter Server estiver com um Platform Services Controller externo, essa opção também criará um proxy para o endpoint do SSO.

Este procedimento descreve como criar manualmente um proxy para uma instância do vCenter Server ou criar um proxy para um host do ESXi, uma instância do Platform Services Controller externo ou uma instância do NSX Manager.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Selecione uma instância do vCenter Server.
- 4 Na página com informações detalhadas do vCenter Server, clique na guia **Proxies** e clique em **Novo**.
- 5 Insira um nome para o proxy.
- 6 Selecione o tipo do proxy, dependendo do componente que você deseja que VMware Cloud Director seja um proxy.

Não é possível editar essa configuração após a criação do proxy.

Você pode criar apenas um proxy de vCenter Server. Se houver um proxy de vCenter Server existente e você quiser criar um novo proxy, o menu suspenso **Tipo** não inclui uma opção de vCenter Server.

- Se você quiser criar um proxy de vCenter Server, selecione **vCenter** no menu suspenso **Tipo** e continue em [Etapa 10](#).

- Se você quiser criar um proxy para um host do ESXi, NSX Manager ou SSO, faça sua seleção no menu suspenso e continue em [Etapa 7](#).
- 7 Insira um nome, host de destino e a URL do novo proxy.

O host de destino é o nome do host ou o endereço IP do componente do qual você deseja que o VMware Cloud Director seja um proxy. A URL da interface de usuário do novo proxy é a URL para a qual a interface de usuário VMware Cloud Director se direciona quando o tenant abre o proxy.
 - 8 Se quiser que o proxy fique visível para os tenants, ative a opção **Visível para o tenant**.
 - 9 (Opcional) Clique em **Selecionar proxy pai** e selecione um proxy na lista.
 - 10 Clique em **Salvar**.

Próximo passo

[Gerenciar os certificados de proxy e as CRLs](#).

Gerenciar os certificados de proxy e as CRLs

Você pode visualizar, baixar e carregar os certificados de proxy e as listas de certificados de revogação (CRLs).

Pré-requisitos

Verifique se você tem proxies fornecidos pelo VMware Cloud Director em pelo menos uma instância do vCenter Server. Consulte [Acesso aos componentes do vSphere por meio de endpoints e proxies do VMware Cloud Director](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **Proxies** e selecione um proxy.
- 3 Clique em **Gerenciar Certificado**.
- 4 Carregar ou baixar o certificado e a CRL.
- 5 Clique em **Salvar**.

Adicionar recursos de nuvem

Os recursos de nuvem são uma abstração dos recursos subjacentes do vSphere deles e fornecem recursos de processamento e memória para vApps e máquinas virtuais do VMware Cloud Director, além de acesso a armazenamento e conectividade de rede.

Os recursos de nuvem incluem datacenters virtuais do provedor e da organização, redes externas, redes de datacenters virtuais da organização e pools de redes. Antes de adicionar recursos de nuvem ao VMware Cloud Director, você deve adicionar recursos do vSphere.

Para obter informações sobre os centros de dados virtuais da organização, consulte [Capítulo 6 Gerenciamento de centros de dados virtuais da organização](#).

Para obter informações sobre redes de centros de dados virtuais da organização, consulte o capítulo *Gerenciar redes de centros de dados virtuais da organização*, no *Guia do Portal de Tenants do VMware Cloud Director*.

O VMware Cloud Director 9.7 apresenta o SDDC ou instância dedicada do vCenter Server como um recurso de nuvem que encapsula toda a instalação do vCenter Server. O provedor pode criar e habilitar um vCenter Server dedicado, publicá-lo para os tenants e criar e habilitar proxies para diferentes componentes do ambiente vSphere subjacente. Para criar, publicar em tenants e gerenciar instâncias do vCenter Server dedicadas e proxies, você deve usar o Service Provider Admin Portal ou a vCloud OpenAPI. Consulte [Capítulo 9 Gerenciando instâncias dedicadas do vCenter Server](#) ou *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

Centros de dados virtuais do provedor

Um centro de dados virtual (VDC) de provedor combina os recursos de processamento e memória de pools de recursos do vCenter Server com os recursos de armazenamento de uma ou mais políticas de armazenamento de uma única instância do vCenter Server. Para recursos de rede, um VDC de provedor pode usar o NSX Data Center for vSphere ou o NSX-T Data Center.

- Você pode criar e gerenciar um VDC de provedor apoiado por uma instância anexada do vCenter Server e sua instância associada do NSX Manager usando o Service Provider Admin Portal ou a API do vCloud.
- Você pode criar e gerenciar um VDC de provedor com suporte de uma instância conectada do vCenter Server e uma instância do NSX-T Manager usando o Service Provider Admin Portal ou a API do vCloud.

Um típico sistema do VMware Cloud Director inclui vários VDCs de provedor configurados para atender aos diversos requisitos de nível de serviço. Cada VDC de provedor tem um pool de recursos primário. Você pode adicionar e remover pools de recursos não primários da instância de suporte do vCenter Server. Não é possível remover o pool de recursos primário.

Criar um centro de dados virtual do provedor

Para tornar os recursos de processamento, memória e armazenamento do vSphere disponíveis para o VMware Cloud Director, crie um centro de dados virtual (VDC) de provedor.

Antes que uma organização possa começar a implantar VMs ou criar catálogos, o **administrador do sistema** deve criar um VDC de provedor e os VDCs de organização que consomem seus recursos. A relação dos VDCs de provedor com os VDCs de organização é uma decisão administrativa. A decisão pode ser baseada no escopo das ofertas de serviços, na capacidade e na distribuição geográfica de sua infraestrutura de vSphere e considerações semelhantes. Como um VDC de provedor restringe a capacidade e os serviços do vSphere disponíveis para os tenants,

os **administradores do sistema** geralmente criam VDCs de provedor que fornecem classes diferentes de serviço, conforme medido por desempenho, capacidade e recursos. Os tenants podem então ser provisionados com VDCs de organização que fornecem classes específicas de serviço definidas pela configuração do VDC de provedor com backup.

Antes de criar um VDC de provedor, considere o conjunto de recursos do vSphere que você planeja oferecer aos seus tenants. Alguns desses recursos podem ser implementados no pool de recursos primário do VDC de provedor. Outras pessoas podem exigir que você crie pools de recursos adicionais com base em clusters do vSphere especialmente configurados e os adicione ao VDC, conforme descrito em [Adicionar um pool de recursos a um data center virtual de um provedor](#).

O intervalo de versões do ESXi instaladas em hosts no cluster que faz o backup de um pool de recursos determina o conjunto de sistemas operacionais convidados e versões de hardware virtual disponíveis para VMs implantadas em VDCs de organização com backup do VDC de provedor.

Pré-requisitos

- Faça login no Service Provider Admin Portal como um **administrador do sistema**.
- Verifique se você criou o pool de recursos primário de destino com capacidade disponível num cluster configurado para usar o DRS automatizado. Você pode usar um pool de recursos para apenas um VDC de provedor. Para criar um pool de recursos, você pode usar o vSphere Client.

Se planeja adicionar um pool de recursos que faça parte de um cluster que usa o recurso de HA (alta disponibilidade) do vSphere, certifique-se de conhecer como o HA do vSphere calcula o tamanho do slot. Para obter informações sobre tamanhos de slots e como personalizar o comportamento do vSphere de alta disponibilidade, consulte a documentação *Disponibilidade do vSphere*.

- Se quiser usar o vSphere with VMware Tanzu no VMware Cloud Director, verifique se você tem disponível uma instância do vCenter Server 7.0 ou posterior com um Cluster de Supervisor configurado. Consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere.
- Se você usar o NSX Data Center for vSphere para os recursos de rede do VDC de provedor:
 - Verifique se a instância do vCenter Server que contém o pool de recursos primário de destino está anexada e tem uma chave de licença do NSX Data Center for vSphere.
 - Configure a infraestrutura VXLAN no NSX Manager. Consulte o *Guia de Administração do NSX* relevante.

Se quiser usar um pool de redes VXLAN personalizado neste VDC de provedor (em vez do pool de redes VXLAN padrão), crie esse pool de redes agora. Consulte [Criar um pool de redes com suporte de zona de transporte do NSX Data Center for vSphere](#).

- Se você usar o NSX-T Data Center para os recursos de rede do VDC de provedor:
 - [Adicionar uma rede externa com suporte de um gateway de camada 0 do NSX-T Data Center](#)
 - [Criar um pool de redes com suporte de zona de transporte do NSX-T Data Center](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.
- 3 Clique em **Novo**.
- 4 Se você tiver uma implantação do VMware Cloud Director multissite, no menu **Site**, selecione o site ao qual deseja adicionar essa instância de VDC de provedor e clique em **Avançar**.
- 5 Insira um nome e, opcionalmente, uma descrição para o VDC de provedor.

Você pode usar essas caixas de texto para indicar os recursos do vSphere disponíveis para VDCs de organização com backup do VDC de provedor, por exemplo, **vSphere HA** ou **Políticas de armazenamento com suporte para IOPS**.

- 6 (Opcional) Para desativar o VDC de provedor após a criação, desligue o botão de alternância **Estado**.

Você não pode usar os recursos de processamento e armazenamento de um VDC desativado para a criação de VDCs de organização.

- 7 Clique em **Avançar**.
- 8 Para fornecer pools de recursos para o VDC de provedor, selecione uma instância do vCenter Server e clique em **Avançar**.

Esta página lista instâncias do vCenter Server registradas para VMware Cloud Director. Clique numa instância do vCenter Server para exibir seus pools de recursos disponíveis.

Se quiser usar o vSphere with VMware Tanzu no VMware Cloud Director, você deverá selecionar uma instância do vCenter Server 7.0 ou posterior com um Cluster de Supervisor configurado.

- 9 Selecione um pool de recursos para servir como o pool de recursos primário para esse VDC de provedor.

Você pode usar um pool de recursos para um único VDC de provedor. Quando você adiciona um pool de recursos a um VDC de provedor, esse pool de recursos e sua cadeia pai se tornam indisponíveis para seleção por outros VDCs de provedor.

Se quiser usar o vSphere with VMware Tanzu, selecione um Cluster de Supervisor. O VMware Cloud Director exibe um ícone do Kubernetes ao lado dos pools de recursos com o suporte de um Cluster de Supervisor.

- 10 Se você selecionar um pool de recursos ou um cluster com suporte por um Cluster de Supervisor, para estabelecer um relacionamento de confiança com a camada de controle do Kubernetes, você deverá confiar no certificado dela.
- 11 Selecione a versão do hardware virtual mais alta que deseja que o VDC de provedor suporte e clique em **Próximo**.

O sistema determina a versão de hardware virtual mais alta suportada por todos os hosts no cluster que faz o backup do pool de recursos e o oferece como padrão no menu suspenso **Versão de hardware mais alta com suporte**. Você pode usar esse padrão ou selecionar uma versão de hardware inferior no menu. A versão que você especifica se torna a mais alta versão de hardware virtual disponível para uma VM implantada em um VDC de organização com backup desse VDC de provedor. Se você selecionar uma versão de hardware virtual mais baixa, alguns sistemas operacionais convidados podem não ser suportados para uso por essas VMs. Depois de criar o VDC de provedor com a versão de hardware selecionada, você só poderá fazer upgrade, e não downgrade, dessa versão.

Observação A versão de hardware disponível para o VDC de provedor depende da versão mais alta disponível do host ESXi no cluster de destino. Se a versão de hardware com suporte mais alta do host ESXi não estiver disponível para seleção, verifique no vSphere Client se a compatibilidade padrão para a criação da máquina virtual no centro de dados está definida como **Usar configuração e versão do host do centro de dados**. Você também pode definir a configuração de compatibilidade padrão como a versão de hardware mais alta que deseja usar para o cluster.

O VMware Cloud Director 9.7 e versões posteriores oferecem suporte à versão de hardware mais alta compatível com a infraestrutura do vSphere. A partir do VMware Cloud Director 10.2.2, você pode definir a versão do hardware sem configurar manualmente a versão de hardware padrão na instância do vCenter Server.

-
- 12 Selecione uma ou mais políticas de armazenamento para o VDC de provedor e clique em **Próximo**.

Todas as políticas de armazenamento do vSphere compatíveis com o pool de recursos selecionado são listadas.

13 Configure o pool de redes para esse VDC de provedor.

Cada VDC de provedor deve ter um pool de redes. Você pode fazer com que o sistema crie um para você com um escopo padrão ou pode usar um VXLAN personalizado com base em um NSX Data Center for vSphere específico ou um pool Geneve com base em uma zona de transporte do NSX-T Data Center.

Observação Se quiser usar o vSphere with VMware Tanzu no VMware Cloud Director, você deverá selecionar a opção **NSX-T Manager e pool de Redes Geneve**.

Opção	Descrição
Criar um pool de redes padrão do VXLAN	O sistema cria um pool VXLAN para este VDC de provedor.
Selecione Pool de Redes VXLAN na lista	Selecione um pool de redes numa lista para usar um pool do VXLAN personalizado com base numa zona de transporte do NSX específica.
Selecionar o pool de redes NSX-T Manager e Geneve	Selecione um pool de redes em uma lista para usar um pool VXLAN personalizado com suporte por uma zona de transporte do NSX-T Data Center.

14 Revise suas escolhas e clique em **Concluir** para criar o VDC de provedor.**Próximo passo**

É possível adicionar um ou mais pools de recursos secundários que permitem ao VDC de provedor fornecer recursos especializados, como Edge Clusters, grupos de afinidades e hosts com configurações especiais que podem ser exigidas por algumas organizações. Consulte [Adicionar um pool de recursos a um data center virtual de um provedor](#).

Redes Externas

Uma rede externa do VMware Cloud Director fornece uma interface de uplink que conecta redes e máquinas virtuais no sistema a uma rede fora do sistema, como uma VPN, uma intranet corporativa ou a Internet pública. Apenas um **administrador do sistema** pode criar uma rede externa.

Se você tiver mais de uma instância do vCenter Server registrada no sistema, poderá criar várias redes externas, cada uma com suporte de uma rede do vSphere ou de um roteador lógico de camada 0.

O VMware Cloud Director oferece suporte às redes externas IPv4 e IPv6.

Observação O intervalo de endereços IP que você define ao criar a rede externa é alocado a um edge gateway ou às máquinas virtuais que estão diretamente conectadas a essa rede. Por causa disso, os endereços IP não devem ser usados fora do VMware Cloud Director.

Redes externas com suporte de redes do vSphere

As redes externas podem ter suporte de uma única rede do vSphere ou por várias redes do vSphere.

- Redes externas com suporte de uma instância única do vSphere.

Para fornecer a cada consumidor da rede externa um conjunto de endereços IP sem sobreposição na rede do vSphere, o **administrador do sistema** deve configurar os intervalos de IPs na VLAN subjacente manualmente.

- Redes externas com suporte de várias redes do vSphere.

Uma rede externa pode ter suporte de várias redes do vSphere. Essa abordagem pode simplificar o gerenciamento de endereços IP no VMware Cloud Director. Você pode modificar as propriedades de uma rede externa para alterar o suporte de sua rede.

Redes externas com o suporte de várias redes vSphere apresentam várias restrições.

- Uma rede pode ter no máximo uma rede vSphere de suporte em cada instância do VMware Cloud Director registrada no sistema.
- Todos os comutadores de rede de suporte devem ser do mesmo tipo: comutador padrão ou Comutador Distribuído do vSphere.

Redes externas com suporte de um roteador lógico de camada 0

Uma rede externa pode ter suporte de um roteador lógico de camada 0 do NSX-T Data Center.

Você também pode criar uma rede externa com o suporte de um gateway de camada 0 VRF-lite no NSX-T Data Center.

Um gateway de roteamento e encaminhamento virtual (VRF) é criado a partir de um gateway de camada 0 principal. Ele tem suas próprias tabelas de roteamento.

Vários gateways de VRF podem existir no mesmo gateway de camada 0 ao mesmo tempo. Por causa disso, a criação de uma rede externa com suporte para VRF permite a criação de uma topologia de rede totalmente roteada em um VDC por meio do dimensionamento de um gateway de camada 0 no NSX-T Data Center.

Para obter informações sobre gateways de VRF, consulte *Guia de administração do NSX-T Data Center*.

Adicionar uma rede externa com o suporte por recursos do vSphere

Ao adicionar uma rede externa, você pode registrar recursos de rede do vSphere para o VMware Cloud Director usar. Você pode criar redes VDC de organização que se conectam a uma rede externa.

Você pode adicionar uma rede externa IPv4 ou IPv6. Uma rede externa IPv6 oferece suporte às sub-redes IPv4 e IPv6, e uma rede externa IPv4 oferece suporte às sub-redes IPv4 e IPv6.

Pré-requisitos

Verifique se um grupo de portas do vSphere está disponível com ou sem entroncamento de VLAN. Os grupos de portas elásticos com vinculação de porta estática garantem um desempenho ideal.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Redes Externas** e em **Novo**.
- 3 Selecione **Recursos do vSphere**, selecione o tipo de grupos de portas para fazer backup da rede e clique em **Avançar**.
- 4 Digite um nome e, opcionalmente, uma descrição para a nova rede externa.
- 5 Selecione os grupos de portas para fazer backup da rede externa e clique em **Avançar**.
- 6 Configure pelo menos uma sub-rede e clique em **Avançar**.
 - a Para adicionar uma sub-rede, clique em **Adicionar**.
 - b Insira as configurações de roteamento entre domínios sem classe (CIDR) da rede.
Use o formato *network_gateway_IP_address/subnet_prefix_length*, por exemplo, **192.167.1.1/24**.
 - c (Opcional) Insira as configurações de DNS.
 - d Configure um pool de IPs estáticos adicionando pelo menos um intervalo de endereços IP ou um endereço IP.
 - e Clique em **OK**.
 - f (Opcional) Para adicionar outra sub-rede, repita esta etapa.
- 7 Analise as configurações de rede e clique em **Concluir**.

Próximo passo

Você pode criar uma rede de VDC de organização que se conecta à rede externa.

Adicionar uma rede externa com suporte de um gateway de camada 0 do NSX-T Data Center

Para registrar os recursos de rede do NSX-T Data Center para o VMware Cloud Director usar, adicione uma rede externa com suporte de um gateway de camada 0.

Pré-requisitos

Para criar uma rede externa com suporte de um gateway de camada 0 do NSX-T Data Center, primeiro você deve criar um gateway de camada 0. Você pode criar o gateway de camada 0 na interface de usuário do NSX-T Manager ou usando a API de Política do NSX.

Se você quiser criar uma rede externa com suporte de um gateway VRF no NSX-T Data Center, também deverá criar um gateway VRF que esteja vinculado ao gateway de camada 0.

- Crie um gateway de camada 0 na interface de usuário do NSX-T Manager.
 - a Faça login com privilégios de administrador na instância do NSX-T Manager.
 - b Clique em **Rede**, em **Gateways de Camada 0** e em **Adicionar Gateway > Camada 0**.
 - c Digite um nome para o roteador de camada 0.
 - d Selecione um modo de Alta Disponibilidade.

Observação Por padrão, o modo ativo-ativo é usado. No modo ativo-ativo, o tráfego tem balanceamento de carga em todos os membros. No modo ativo-de espera, um membro ativo eleito processa o tráfego. Se o membro ativo falhar, um novo membro ficará ativo.

- e Selecione um Edge Cluster do NSX-T existente no menu suspenso para voltar a este roteador lógico de camada 0 e clique em **Salvar**.
- Se você quiser criar uma rede externa com suporte de um gateway VRF no NSX-T Data Center, crie um gateway VRF que esteja vinculado ao gateway de camada 0.
 - a Faça login com privilégios de administrador na instância do NSX-T Manager.
 - b Clique em **Rede**, em **Gateways de Camada 0** e em **Adicionar Gateway > VRF**.
 - c Insira um nome para o gateway VRF.
 - d Selecione o gateway de camada 0 ao qual conectar o gateway VRF.
 - e Clique em **Salvar**.

Procedimentos

- 1 Faça login no VMware Cloud Director Service Provider Admin Portal.
- 2 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 3 No painel esquerdo, clique em **Redes Externas** e em **Novo**.
- 4 Selecione um site no qual deseja registrar a nova rede externa e clique em **Avançar**.
- 5 Na página **Tipo de suporte**, selecione **Recursos do NSX-T (Roteador de Camada 0)**, selecione um NSX-T Manager registrado para suportar a rede e clique em **Avançar**.
- 6 Digite um nome e, opcionalmente, uma descrição para a nova rede externa.
- 7 Selecione um gateway de camada 0 ou um gateway VRF para conectar à rede externa e clique em **Avançar**.
- 8 Configure pelo menos uma sub-rede e clique em **Avançar**.
 - a Para adicionar uma sub-rede, clique em **Adicionar**.
 - b Insira as configurações de roteamento entre domínios sem classe (CIDR) da rede.
 - c (Opcional) Insira as configurações de DNS.

- d Configure um pool de IPs estáticos adicionando pelo menos um intervalo de endereços IP ou um endereço IP.
- e Clique em **OK**.
- f (Opcional) Para adicionar outra sub-rede, repita as etapas de 8.a a 8.e.

9 Analise as configurações de rede e clique em **Concluir**.

Próximo passo

Use o gateway de camada 0 para criar um uplink para a rede externa.

Pools de Redes

Um pool de redes é um grupo de redes não diferenciadas que está disponível para uso em um VDC de organização para criar redes do vApp e determinados tipos de redes de VDC de organização.

Um pool de redes tem o suporte de recursos de rede do vSphere como IDs de VLAN ou grupos de portas, de recursos do NSX Data Center for vSphere ou de recursos do NSX-T Data Center.

O VMware Cloud Director usa pools de redes para criar redes de VDC de organização internas e roteadas para NAT e todas as redes do vApp. O tráfego de rede em cada rede em um pool é isolado na camada 2 de todas as outras redes.

Cada VDC de organização no VMware Cloud Director pode ter um pool de redes. Vários VDCs de organização podem compartilhar um pool de redes. O pool de redes para um VDC de organização fornece as redes criadas para satisfazer a cota de rede em um VDC de organização.

Pools de rede VXLAN

Cada VDC de provedor com suporte do NSX Data Center for vSphere inclui um pool de redes VXLAN.

Quando você cria um VDC de provedor com suporte do NSX Data Center for vSphere, é possível associar esse VDC de provedor a um pool de redes VXLAN existente, ou você pode criar um pool de redes VXLAN para o VDC de provedor.

Um pool de redes VXLAN recém-criado recebe um nome derivado do nome do VDC de provedor que o contém e anexado a ele na criação. Não é possível excluir ou modificar esse pool de redes. Se você renomear um VDC de provedor, o pool de redes VXLAN será renomeado automaticamente.

Observação Para garantir um desempenho de rede ideal em toda a sua infraestrutura, crie um pool de redes VXLAN e associe-o a todos os seus VDCs de provedor na criação.

Redes VXLAN do VMware Cloud Director são baseadas no padrão VXLAN IETF e fornecem vários benefícios.

- Redes lógicas estendendo-se pelos limites da camada 3
- Redes lógicas estendendo-se por vários racks em uma única camada 2

- Contenção da difusão
- Desempenho superior
- Maior escala (até 16 milhões endereços de rede)

Para obter mais informações sobre redes VXLAN em um ambiente VMware Cloud Director, consulte o *Guia de administração do NSX*.

Criar um pool de redes com suporte de zona de transporte do NSX Data Center for vSphere

Para registrar uma zona de transporte do NSX Data Center for vSphere para o VMware Cloud Director usar, adicione um pool de redes com suporte a VXLAN.

Pré-requisitos

Crie uma zona de transporte do NSX Data Center for vSphere em qualquer vCenter Server registrado no VMware Cloud Director. Consulte o *Guia de Administração do NSX*.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Pools de Redes** e clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo pool de redes e clique em **Avançar**.
- 4 Selecione **Com suporte do VXLAN** e clique em **Avançar**.
- 5 Selecione uma instância do vCenter Server para especificar a zona de transporte VXLAN a ser usada por esse pool de redes e clique em **Avançar**.
- 6 Selecione uma zona de transporte do NSX Data Center for vSphere para fazer suportar o novo pool de redes e clique em **Avançar**.

Observação Para criar um pool de redes universal para rede entre centro de dados virtuais, selecione uma zona de transporte do tipo UNIVERSAL_VXLAN.

- 7 Analise as configurações do pool de redes e clique em **Concluir**.

Próximo passo

Crie uma rede de VDC de organização com suporte do pool de redes ou associe o pool de redes a um VDC de organização e crie redes do vApp.

Pools de redes Geneve

Cada VDC de provedor com suporte do NSX-T Data Center inclui um pool de redes Geneve.

Geneve é o padrão de virtualização de rede que fornece o recurso de sobreposição no NSX-T Data Center.

Quando você cria um VDC de provedor com suporte do NSX-T Data Center, é possível associar esse VDC de provedor a um pool de redes Geneve existente, ou você pode criar um pool de redes Geneve para o VDC de provedor.

Observação O VMware Cloud Director oferece suporte a pools de rede do NSX-T Data Center com o suporte de zonas de transporte VLAN.

As redes Geneve do VMware Cloud Director oferecem uma série de benefícios.

- Redes lógicas estendendo-se pelos limites da camada 3
- Redes lógicas estendendo-se por vários racks em uma única camada 2
- Contenção da difusão
- Desempenho superior
- Maior escala (até 16 milhões endereços de rede)

Criar um pool de redes com suporte de zona de transporte do NSX-T Data Center

Para registrar uma zona de transporte do NSX-T Data Center para o VMware Cloud Director usar, crie um pool de redes com suporte de Geneve.

Pré-requisitos

Crie uma zona de transporte do NSX-T Data Center com suporte de sobreposição.

Observação O VMware Cloud Director oferece suporte a pools de rede do NSX-T Data Center com o suporte de zonas de transporte VLAN.

Para obter mais informações sobre a criação de zonas de transporte e o processo de Encapsulamento de Virtualização de Rede Genérico, chamado de Geneve Overlay, consulte a *Documentação do produto NSX-T Data Center*.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Pools de Redes** e clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo pool de redes e clique em **Avançar**.
- 4 Selecione **Com suporte de Geneve** e clique em **Avançar**.
- 5 Selecione uma instância do NSX-T Manager para fornecer a zona de transporte para esse pool de redes e clique em **Avançar**.
- 6 Selecione uma zona de transporte do NSX-T e clique em **Avançar**.
- 7 Analise as configurações do pool de redes e clique em **Concluir**.

Próximo passo

Crie uma rede de VDC de organização com suporte do pool de redes ou associe o pool de redes a um VDC de organização e crie redes do vApp.

Criar um pool de redes com suporte de IDs de VLAN

Para registrar IDs de VLAN do vSphere para o VMware Cloud Director usar, adicione um pool de redes com suporte a VLAN. Um pool de redes com suporte a VLAN fornece segurança, dimensionamento e desempenho para as redes de VDC da organização.

Pré-requisitos

Verifique se um intervalo de IDs de VLAN e um switch distribuído do vSphere estão disponíveis no vSphere. As IDs de VLAN devem ser IDs válidas que são configuradas no comutador físico ao qual os servidores do ESXi são conectados.

Cuidado As VLANs devem ser isoladas no nível da camada 2. Não isolar adequadamente as VLANs pode causar uma interrupção na rede.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Pools de Redes** e clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo pool de redes e clique em **Avançar**.
- 4 Selecione **Com suporte de VLAN** e clique em **Avançar**.
- 5 Selecione uma instância do vCenter Server para especificar o switch virtual distribuído a ser usado por esse pool de redes e clique em **Avançar**.
- 6 Insira um intervalo de IDs de VLAN e clique em **Avançar**.
- 7 Selecione um switch distribuído para o pool de redes e clique em **Avançar**.
- 8 Analise as configurações do pool de redes e clique em **Concluir**.

Próximo passo

Crie uma rede de VDC de organização com suporte do pool de redes ou associe o pool de redes a um VDC de organização e crie redes do vApp.

Criar um pool de redes com suporte de grupos de portas do vSphere

Para registrar grupos de portas do vSphere para o VMware Cloud Director usar, adicione um pool de redes com suporte de grupos de portas. Ao contrário de outros tipos de pools de rede, um

pool de redes com suporte do grupo de portas não requer um switch distribuído do vSphere e pode oferecer suporte a grupos de portas associados a switches distribuídos de terceiros.

Cuidado Os grupos de portas devem ser isolados de todos os outros grupos de portas na camada 2. Os grupos de portas devem ser isolados fisicamente ou devem ser isolados usando tags de VLAN. A falha em isolar adequadamente os grupos de portas pode causar uma interrupção na rede.

Pré-requisitos

Verifique se um ou mais grupos de portas estão disponíveis no ambiente do vSphere. Os grupos de portas devem estar disponíveis em cada host ESXi no cluster, e cada grupo de portas deve usar apenas uma única VLAN. Há suporte para grupos de portas com ou sem entroncamento de VLAN.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Pools de Redes** e clique em **Novo**.
- 3 Insira um nome e, opcionalmente, uma descrição para o novo pool de redes e clique em **Avançar**.
- 4 Selecione **Com suporte por grupo de portas** e clique em **Avançar**.
- 5 Selecione uma instância do vCenter Server para fornecer grupos de portas a serem usados por esse pool de redes e clique em **Avançar**.
- 6 Selecione um ou mais grupos de portas e clique em **Avançar**.
Você pode criar uma rede para cada grupo de portas.
- 7 Analise as configurações do pool de redes e clique em **Concluir**.

Próximo passo

Crie uma rede de VDC de organização com suporte do pool de redes ou associe o pool de redes a um VDC de organização e crie redes do vApp.

Exibir as instâncias do vCenter Server

Você pode ver uma lista das instâncias do vCenter Server em todos os sites na sua instalação do VMware Cloud Director. Você pode ver como o VMware Cloud Director usa cada instância do vCenter Server.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.

Resultados

Uma lista de todas as instâncias do vCenter Server anexadas é exibida. A lista contém as seguintes informações para cada instância do vCenter Server.

	Descrição
Nome	O nome da instância do vCenter Server no VMware Cloud Director.
Status	O status do vCenter Server pode ser normal, aviso e crítico.
Estado	Ativado ou desativado. Consulte Ativar ou desativar uma instância do vCenter Server .
Conexão	Conectado ou não ao VMware Cloud Director. Consulte Reconectar uma instância do vCenter Server .
Host do VC	FQDN da instância do vCenter Server.
Versão	A versão do vCenter Server.
Uso	As instâncias dedicadas do vCenter Server têm o acesso do tenant ativado. O provedor pode usar pools de recursos diferentes da instância compartilhada do vCenter Server em vários VDCs de provedor e, em seguida, alocar esses pools de recursos para diferentes tenants. Consulte Capítulo 9 Gerenciando instâncias dedicadas do vCenter Server .
Integridade do cluster	Agregação da integridade de todos os clusters na instância do vCenter Server. Ao agregar a integridade do cluster, a integridade do cluster menos íntegro é exibida.
Clusters	Número de clusters na instância do vCenter Server.
VMs	Número de VMs na instância do vCenter Server.
VMs em execução	Número de VMs em execução na instância do vCenter Server.
CPU	Quantidade de CPU virtual usada ativamente como uma porcentagem do total disponível da CPU do vCenter Server.
Memória	Quantidade de memória virtual usada ativamente como uma porcentagem do total disponível da memória do vCenter Server.
Armazenamento	Quantidade de armazenamento virtual usada ativamente como uma porcentagem do armazenamento total disponível do vCenter Server.

Modificar configurações do vCenter Server

Se as informações de conexão para uma instância anexada do vCenter Server forem alteradas ou se você quiser alterar seu nome e a descrição no VMware Cloud Director, ou seu escopo de provedor de processamento, poderá modificar suas configurações.

Você pode modificar as configurações que definiu ao adicionar a instância do vCenter Server. Consulte [Adicionar a instância do vCenter Server](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **Instâncias do vCenter Server** e clique no nome da instância do vCenter Server que você deseja modificar.
- 3 No canto superior direito da seção **Informações do vCenter Server**, clique em **Editar**.
- 4 (Opcional) Edite o nome e a descrição da instância.
- 5 (Opcional) Editar o escopo do provedor de computação para o vCenter Server
O escopo do provedor de processamento representa domínios de falha de processamento ou zonas de disponibilidade que são visíveis para tenants e onde as cargas de trabalho residem. Por padrão, o escopo do provedor de processamento de um centro de dados virtual de provedor é herdado da instância do vCenter Server de apoio. Você 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 definir o vCenter Server com **Alemanha** como escopo de provedor de processamento e definir o VDC de provedor com **Munique** como escopo.
- 6 (Opcional) Edite a URL da instância do vCenter Server.
- 7 (Opcional) Edite o nome de usuário e a senha da conta do **administrador** do vCenter Server.
- 8 (Opcional) Ative ou desative o botão de alternância **Habilitado**.
- 9 (Opcional) Configure a URL do cliente Web do vCenter Server.
- 10 Clique em **Salvar**.

Próximo passo

Se você tiver modificado as informações de conexão, deverá [Reconectar uma instância do vCenter Server](#).

Ativar ou desativar uma instância do vCenter Server

Antes de realizar uma manutenção ou cancelar o registro de uma instância do vCenter Server, você deve desativar a instância de destino do vCenter Server. Para fornecer seus recursos aos centros de dados virtuais no VMware Cloud Director, você deve ativar a instância do vCenter Server.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Clique no botão de opção ao lado do nome da instância de destino do vCenter Server e clique em **Habilitar** ou **Desabilitar**.
- 4 Para confirmar, clique em **OK**.

Reconectar uma instância do vCenter Server

Se uma instância do vCenter Server aparecer como desconectada ou se você tiver modificado as configurações de conexão, poderá tentar redefinir a conexão.

Observação Durante o estabelecimento da nova conexão, a instância do vCenter Server não está disponível para operações.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Clique no botão de opção ao lado do nome da instância de destino do vCenter Server e clique em **Reconectar**.
- 4 Para confirmar, clique em **OK**.

Atualizar uma instância do vCenter Server

Para atualizar as informações no banco de dados do VMware Cloud Director sobre os recursos do vCenter Server subjacentes, você deve atualizar a instância do vCenter Server.

Começando com o VMware Cloud Director 10.2.2, se você estiver usando o Kubernetes, quando atualizar uma instância do vCenter Server, isso resultará na restauração das políticas de firewall e das regras de NAT padrão que bloqueiam o acesso ao cluster Tanzu Kubernetes por redes fora do centro de dados virtual da organização.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Clique no botão de opção ao lado do nome da instância de destino do vCenter Server e clique em **Atualizar**.
- 4 Para confirmar, clique em **OK**.

Atualizar as políticas de armazenamento de uma instância do vCenter Server

Para atualizar as informações no banco de dados do VMware Cloud Director sobre as políticas de armazenamento de VM no ambiente vSphere subjacente, você deve atualizar as políticas de armazenamento da instância do vCenter Server.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Clique no botão de opção ao lado do nome da instância de destino do vCenter Server e clique em **Atualizar Políticas**.
- 4 Para confirmar, clique em **OK**.

Cancelar registro de uma instância do vCenter Server

Para parar de usar os recursos de uma instância do vCenter Server, você pode remover essa instância do vCenter Server da sua instalação do VMware Cloud Director.

Pré-requisitos

- Desative a instância do vCenter Server Consulte [Ativar ou desativar uma instância do vCenter Server](#).
- Exclua todos os centros de dados virtuais do provedor que usem pools de recursos dessa instância do vCenter Server. Consulte [Excluir um data center virtual de provedor](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Clique no botão de seleção ao lado do nome da instância de destino do vCenter Server e clique em **Cancelar registro**.
- 4 Para confirmar, clique em **OK**.

Modificar as configurações do NSX Manager

Se as informações de conexão para uma instância registrada do NSX Manager forem alteradas ou se você quiser alterar seu nome e a descrição no VMware Cloud Director, poderá modificar suas configurações.

Você pode modificar as configurações que definiu ao adicionar a instância do NSX Manager. Consulte [\(Opcional\) Adicione a instância de NSX Manager associada](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **vCenters** e clique no nome da instância do vCenter Server associada à instância do NSX Manager de destino.
- 3 No canto superior direito da seção **Informações do NSX-V Manager**, clique em **Editar**.
- 4 Modifique o nome de host e as credenciais de administrador do NSX Manager e clique em **Salvar**.
- 5 (Opcional) Para habilitar a rede de centros de dados virtuais cruzados para os centros de dados virtuais com suporte por esta instância do vCenter Server, ative a alternância e insira as propriedades da VM de controle e um nome para o escopo do provedor de rede.

As propriedades da VM de controle são usadas para implantar um dispositivo na instância do NSX Manager para componentes de rede do centro de dados virtual cruzado, como um roteador universal.

Parâmetro	Descrição
Caminho do Pool de Recursos	O caminho hierárquico para um pool de recursos específico na instância do vCenter Server, a partir do cluster, <i>Cluster/Resource_Pool_Parent/Target_Resource</i> . Por exemplo, TestbedCluster1/mgmt-rp . Como alternativa, você pode inserir a ID de referência do objeto gerenciado do pool de recursos. Por exemplo, resgroup-1476 .
Nome do repositório de dados	O nome do repositório de dados para hospedar os arquivos do dispositivo. Por exemplo, shared-disk-1 .
Interface de Gerenciamento	O nome da rede no vCenter Server ou no grupo de portas usado para a interface de gerenciamento do DLR de alta disponibilidade. Por exemplo, TestbedPG1 .
Escopo do provedor de rede	Corresponde ao domínio de falha da rede nas topologias de rede dos grupos de centros de dados. Por exemplo, boston-fault1 . Para obter informações sobre como gerenciar vários grupos de centros de dados virtuais, consulte o <i>Guia do Portal de Tenants do VMware Cloud Director</i> .

Modificar as configurações do NSX-T Manager

Se as informações de conexão para uma instância registrada do NSX-T Manager forem alteradas ou se você quiser alterar seu nome e a descrição no VMware Cloud Director, poderá modificar suas configurações.

Você pode modificar as configurações que definiu ao adicionar a instância do vCenter Server. Consulte [Registrar uma instância do NSX-T Manager](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.

- 2 No painel esquerdo, clique em **NSX-T Managers** e clique no nome da instância do NSX-T Manager que você deseja modificar.
- 3 No canto superior direito da guia **Geral**, clique em **Editar**.
- 4 Edite as configurações do NSX-T Manager e clique em **Salvar**.

Excluir uma instância do NSX-T Manager

Para parar de usar os recursos de uma instância do NSX-T Manager, você pode remover essa instância do vCenter Server da sua instalação do VMware Cloud Director.

Pré-requisitos

Exclua todos os data centers virtuais de provedor que usam recursos dessa instância do NSX-T Manager. Consulte [Excluir um data center virtual de provedor](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, clique em **NSX-T Managers**.
- 3 Clique no botão de opção ao lado do nome da instância do NSX-T Manager que você deseja remover e clique em **Excluir**.
- 4 Para confirmar, clique em **Excluir**.

Configurando e gerenciando implantações em multissites

Para gerenciar e monitorar várias instalações do VMware Cloud Director geograficamente distribuídas ou grupos de servidores e suas organizações como entidades individuais, os provedores de serviços e os tenants podem usar o recurso multissite do VMware Cloud Director.

Implementação efetiva de um multissite

Ao associar dois sites do VMware Cloud Director, você ativa a administração dos sites como uma entidade única. Você também permite que as organizações nesses sites formem associações entre si. Quando uma organização é um membro de uma associação, os usuários da organização podem usar o do VMware Cloud Director Tenant Portal para acessar os ativos da organização em qualquer site membro, embora cada organização membro e seus recursos sejam locais para o site que ela ocupa.

Observação Para associar sites, você deve usar a API do VMware Cloud Director. Os sites devem ter a mesma versão da API do VMware Cloud Director ou uma versão principal separada. Por exemplo, você pode associar um site do VMware Cloud Director 10.1 (API versão 34.0) com um site do VMware Cloud Director versão 10.0, 10.1, 10.2 ou 10.2.2, respectivamente, as versões de API 33.0, 34.0, 35.0 ou 35.2.

Depois de associar dois sites, você poderá usar a API do VMware Cloud Director ou o VMware Cloud Director Tenant Portal para associar organizações que ocupam esses sites. Consulte o *Guia de programação da API do VMware Cloud Director* ou o tópico [Configurar e gerenciar implantações multissite](#) no *Guia do Portal de Tenants do VMware Cloud Director*.

Um site ou organização pode formar um número ilimitado de associações com um par, mas cada associação inclui exatamente dois membros. Cada site ou organização deve ter sua própria chave privada. Os membros da associação estabelecem uma relação de confiança trocando chaves públicas, que são usadas para verificar solicitações assinadas de um membro para outro.

Cada site em uma associação é definida pelo escopo de um grupo de servidores do VMware Cloud Director (um grupo de servidores que compartilham um banco de dados do VMware Cloud Director). Cada organização em uma associação ocupa um único site. O administrador da organização controla o acesso por usuários e grupos da organização aos recursos em cada site membro.

Objetos e Associações de Site

O processo de instalação ou atualização cria um objeto do `site` que representa o grupo local de servidores do VMware Cloud Director. Um administrador de sistema cuja autoridade estende a mais de um grupo de servidores do VMware Cloud Director pode configurar esses grupos de servidores como uma associação de sites do VMware Cloud Director.

Associações de Organizações

Após a conclusão da associação de sites, os **administradores da organização** em qualquer site de membro podem começar a associação de suas organizações.

Observação Você não pode associar uma organização do `System` a uma organização de `tenant`. A organização do `System` em qualquer site pode ser associada somente à organização do `System` em outro site.

Identidades de Usuário e Grupo

As associações de sites e organizações devem concordar em usar o mesmo provedor de identidade (IDP). As identidades de usuário e grupo para todas as organizações na associação devem ser gerenciadas por meio desse IDP.

Exceto para a organização do sistema, que deve usar o IDP integrado do VMware Cloud Director, as associações são livres para escolher o IDP que funciona melhor para elas.

Controle de Acesso do Site para Usuários e Grupos da Organização

Os **administradores de organização** podem configurar seu IDP para gerar tokens de acesso de usuários ou grupos que sejam válidos em todos os sites de membro ou válidos apenas em um subconjunto de sites de membro. Embora as identidades de usuário e grupo devam ser as mesmas em todas as organizações membros, os direitos de usuário e grupo são limitados pelas funções a que esses usuários e grupos são atribuídos em cada organização membro. A atribuição de uma função a um usuário ou grupo é local para uma organização membro, assim como qualquer função personalizada criada por você.

Requisitos do Balanceador de Carga

A implementação efetiva de uma implantação multissite exige a configuração de um balanceador de carga que distribui solicitações que chegam a um endpoint institucional, como `https://vcloud.exemplo.com` para os endpoints para cada membro da associação do site (por exemplo, `https://us.vcloud.exemplo.com` e `https://uk.vcloud.exemplo.com`). Se um site tiver mais de uma célula, você também deverá configurar um balanceador de carga que distribua as solicitações de entrada em todas as células, de modo que uma solicitação para `https://us.vcloud.exemplo.com` possa ser tratada por `https://cell1.us.vcloud.exemplo.com`, `https://cell2.us.vcloud.exemplo.com` e assim por diante.

Observação Você deve usar o balanceador de carga global, neste caso `https://vcloud.exemplo.com`, apenas para acesso à interface do usuário. Se você desenvolve seus próprios scripts ou programas que usam a REST API, essas chamadas deverão ser destinadas a um site específico.

Requisitos de conectividade de rede

Se você quiser usar o recurso multissite, cada célula em cada site deverá ser capaz de fazer solicitações de REST API aos endpoints de REST API de todos os sites. Se você usar os exemplos da seção Requisitos do Balanceador de Carga, `cell1.us.vcloud.exemplo.com` e `cell2.us.vcloud.exemplo.com` deverão ser capazes de acessar o endpoint de REST API para `uk.exemplo.com`. O contrário é válido para todas as células em `uk.exemplo.com`. Isso significa que uma célula também deve ser capaz de fazer chamadas de REST API para seu próprio endpoint de REST API, ou seja, `cell1.us.vcloud.exemplo.com` deve ser capaz de fazer uma chamada de REST API para `https://us.vcloud.exemplo.com`.

Fazer solicitações de REST API para os endpoints de REST API de todos os sites é necessário para o fan-out da REST API. Por exemplo, se a UI ou um cliente de API fizer uma solicitação multissite para obter uma página de organizações de todos os sites e `cell1.us.vcloud.exemplo.com` lidar com a solicitação. A célula `cell1` deve fazer uma chamada de REST API para obter uma página de organizações de cada site usando o endpoint de REST API configurado para esse site. Quando todos os sites retornarem sua página de organizações, `cell1` agrupará os resultados e retornará uma única página de resultados que contém os dados de todos os outros sites.

Sites e certificados

Quando um site estiver associado a outros sites, se você atualizar o certificado dele, poderá ser preciso permitir que os outros sites saibam sobre essa alteração. Se você não permitir que os outros sites saibam sobre a alteração do certificado, o fan-out do multissite poderá ser afetado.

Se estiver substituindo um certificado em um site por um certificado válido e assinado, não será necessário informar os outros sites. Como o certificado é válido e está bem assinado, as células em outros sites podem continuar se conectando a ele de maneira segura, sem interrupção.

Se estiver substituindo um certificado em um site por um certificado autoassinado ou se houver algum outro problema com o certificado que impeça a confiança automática, outros sites precisarão saber sobre isso. Por exemplo, se o certificado expirar, você deverá informar os outros sites. Em cada um dos outros sites, você deve carregar o certificado em **Certificados Confiáveis** no Service Provider Admin Portal. Consulte [Importar certificados confiáveis](#). Quando você importa o certificado, o site para o qual ele é carregado pode confiar no site para obter o novo certificado.

Observação Você pode importar esses certificados para os Certificados Confiáveis dos outros sites antes de instalá-los no site remoto. Isso não garante interrupções na comunicação, pois o certificado antigo e o novo estão no pool de Certificados Confiáveis. Você não precisa reassociar os sites.

Status do Membro de Associação

Depois de criar uma associação de sites ou organizações, o sistema local recupera periodicamente o status de cada membro da associação remota e atualiza esse status no banco de dados do VMware Cloud Director do site local. O status do membro está visível no elemento do `Status` de um `SiteAssociationMember` ou `OrgAssociationMember`. Este elemento pode ter um dos três valores:

ACTIVE

A associação foi estabelecida por ambas as partes, e a comunicação com a parte remota foi bem-sucedida.

ASYMMETRIC

A associação foi estabelecida no local, mas o local remoto ainda não retribuiu.

UNREACHABLE

Uma associação foi criada por ambas as partes, mas o site remoto não está atualmente acessível na rede.

O processo de "heartbeat" de status de membro é executado com a identidade do usuário do sistema multissite, uma conta de usuário local do VMware Cloud Director criada na organização do Sistema durante a instalação do VMware Cloud Director. Embora essa conta seja membro da organização do Sistema, ela não possui direitos de administrador do sistema. Ele tem apenas um único direito, `Multisite: System Operations`, que concede permissão para fazer uma solicitação da API do VMware Cloud Director que recupera o status do membro remoto de uma associação de site.

Listas de recursos multissites

Se você estiver trabalhando com implantações do VMware Cloud Director em vários locais, poderá visualizar as listas de recursos que incluem informações sobre objetos de todos os sites conectados.

Para facilitar a navegação por meio do vSphere e recursos de nuvem do Service Provider Admin Portal, começando com a versão 9.7, o VMware Cloud Director introduz listas de recursos multissites. A partir da versão 10.0, o VMware Cloud Director oferece suporte a listas de recursos multissites que incluem organizações.

Você pode acessar as listas de recursos por meio dos menus **Recursos do vSphere** e **Recursos de Nuvem**.

Você pode acessar informações detalhadas sobre objetos dos diferentes sites e também criar objetos no site local e em sites remotos.

As listas de recursos multissites do vSphere têm suporte para instâncias do vCenter Server, instâncias do NSX-T Manager, pools de recursos, repositórios de dados, hosts, switches distribuídos, grupos de portas, itens bloqueados e políticas de armazenamento.

As listas de recursos de nuvem multissite têm suporte para organizações, VDCs de organização, modelos de VDC de organização, VDCs de provedor, células de nuvem, edge gateways, redes externas, pools de rede e políticas de dimensionamento de VM.

Gerenciamento de centros de dados virtuais do provedor

4

Depois de criar um centro de dados virtual do provedor, você pode modificar suas propriedades, desativá-lo ou excluí-lo e gerenciar suas políticas de armazenamento e pools de recursos.

Para criar um centro de dados virtual de provedor, você deve usar o Service Provider Admin Portal ou a API do vCloud. Para obter informações sobre como usar o Service Provider Admin Portal, consulte [Criar um centro de dados virtual do provedor](#). Para obter informações sobre como usar a API do vCloud, consulte *Guia de programação da API do VMware Cloud Director*.

Este capítulo inclui os seguintes tópicos:

- [Ativar ou desativar um centro de dados virtual do provedor](#)
- [Excluir um data center virtual de provedor](#)
- [Editar as configurações gerais de um data center virtual de provedor](#)
- [Mesclar data centers virtuais de provedor](#)
- [Visualizar os centros de dados virtuais de organização de um centro de dados virtual de provedor](#)
- [Visualizar os datastores em um centro de dados virtual do provedor](#)
- [Visualizar as redes externas em um centro de dados virtual de provedor](#)
- [Usando o Kubernetes com o VMware Cloud Director](#)
- [Gerenciamento das políticas de armazenamento de VM em um centro de dados virtual do provedor](#)
- [Gerenciamento dos pools de recursos em um centro de dados virtual do provedor](#)
- [Modificar os metadados para um centro de dados virtual de provedor](#)

Ativar ou desativar um centro de dados virtual do provedor

Para desativar todos os centros de dados virtuais (VDCs) de organização existentes que usam os recursos de um VDC de provedor, você pode desativar esse VDC de provedor. Não é possível criar VDCs de organização que usem os recursos de um VDC de provedor desativado.

vApps em execução e máquinas virtuais ligadas continuam ativas nos VDCs de organização existentes suportados pelo VDC desse provedor, mas você não pode criar ou iniciar vApps ou máquinas virtuais adicionais.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.
- 3 Clique no botão de opção ao lado do nome do VDC de provedor de destino e clique em **Ativar** ou **Desativar**.
- 4 Para confirmar, clique em **OK**.

Excluir um data center virtual de provedor

Para remover os recursos de um data center virtual de provedor do VMware Cloud Director, você pode excluir esse data center virtual de provedor.

Os recursos subjacentes no vSphere permanecem inalterados.

Pré-requisitos

- Desative o centro de dados virtual do provedor de destino. Consulte [Ativar ou desativar um centro de dados virtual do provedor](#).
- Exclua todos os data centers virtuais de organização que usam recursos desse data center virtual de provedor. Consulte [Excluir um centro de dados virtual da organização](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.
- 3 Clique no botão de opção ao lado do nome do data center virtual de provedor que você deseja remover e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Editar as configurações gerais de um data center virtual de provedor

Você pode alterar o nome e a descrição de um data center virtual de provedor. Se o pool de recursos de apoio suportar uma versão de hardware virtual superior, você poderá atualizar o maior hardware virtual compatível com um centro de dados virtual de provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

- 2 No painel esquerdo, clique em **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor que você deseja modificar.
- 3 Na guia **Configurar > General**, no canto superior direito, clique em **Editar**.
- 4 (Opcional) Modifique o nome e a descrição do data center virtual de provedor.
- 5 (Opcional) Insira um escopo de provedor de processamento para o centro de dados virtual de provedor.

O escopo do provedor de processamento representa domínios de falha de processamento ou zonas de disponibilidade que são visíveis para tenants e onde as cargas de trabalho residem. Por padrão, o escopo do provedor de processamento de um centro de dados virtual de provedor é herdado da instância do vCenter Server de apoio. Você 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 definir o vCenter Server com **Alemanha** como escopo de provedor de processamento e definir o VDC de provedor com **Munique** como escopo.

- 6 (Opcional) No menu suspenso, selecione a versão de hardware mais alta suportada pelo centro de dados virtual desse provedor e clique em **Salvar**.

A versão mais alta que você pode selecionar depende dos hosts do ESXi no pool de recursos que faz backup do centro de dados virtual de provedor.

Observação Você só pode atualizar a versão de hardware compatível com um data center virtual de provedor. Não é possível fazer downgrade da versão do hardware. A versão mais alta do hardware da máquina virtual com suporte no VMware Cloud Director 10.2 é a versão 17. A versão de hardware 17 está disponível quando você a habilita na instância do vCenter Server no nível do cluster ou do centro de dados.

- 7 Clique em **Salvar**.

Mesclar data centers virtuais de provedor

Para combinar os recursos de dois data centers virtuais de provedor, você pode mesclar esses data centers em um único data center virtual de provedor.

Pré-requisitos

- Os centros de dados virtuais de provedor de destino devem pertencer ao mesmo centro de dados do vCenter Server.
- Os centros de dados virtuais de provedor de destino devem conter apenas centros de dados virtuais de organização elásticos.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.

- 3 Clique no botão de opção ao lado do nome do data center virtual de provedor que você deseja mesclar e clique em **Mesclar**.
- 4 Clique no botão de opção ao lado do nome do data center virtual de provedor com o qual mesclar os recursos e clique em **Mesclar**.

Visualizar os centros de dados virtuais de organização de um centro de dados virtual de provedor

Você pode visualizar uma lista dos centros de dados virtuais de organização que estão usando recursos de um centro de dados virtual de provedor.


Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **VDCs de Organização**.

Resultados

A lista dos centros de dados virtuais de organização que estão consumindo os recursos desse centro de dados virtual de provedor é exibida. Para cada VDC de organização, a lista inclui informações sobre o status, o estado, o modelo de alocação, a organização, a instância do vCenter Server, o número de redes, o número de vApps, o número de políticas de armazenamento e o número de pools de recursos.

Próximo passo

- Você pode ir até a exibição do centro de dados virtual de organização no VMware Cloud Director Tenant Portal clicando no ícone **pop-out**  ao lado do nome do centro de dados virtual de organização de destino.
- Clicando no botão de opção ao lado do nome de um centro de dados virtual de organização, você pode realizar operações de gerenciamento semelhantes às operações descritas em [Capítulo 6 Gerenciamento de centros de dados virtuais da organização](#).

Visualizar os datastores em um centro de dados virtual do provedor

Você pode visualizar detalhes sobre os datastores que fornecem a capacidade de armazenamento a um centro de dados virtual do provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **Repositórios de dados**.

Uma lista de todos os datastores no centro de dados virtual de provedor é exibida. A lista contém as seguintes informações para cada datastore.

Título	Descrição
Nome	O nome do datastore
Estado	Ativado ou desativado
Tipo	O tipo de sistema de arquivos usado pelo datastore: VMFS (sistema de arquivos da máquina virtual) ou NFS (Network File System)
Em uso	O espaço do repositório de dados ocupado pelos arquivos da máquina virtual, incluindo arquivos de log, snapshots e discos virtuais. Quando uma máquina virtual é ligada, o espaço de armazenamento utilizado também inclui arquivos de log.
Provisionado	O espaço do repositório de dados garantido para máquinas virtuais. Se qualquer máquina virtual estiver usando o provisionamento dinâmico, uma parte do espaço provisionado talvez não esteja em uso e outras máquinas virtuais poderão ocupar o espaço não utilizado. Esse valor pode ser maior que a capacidade real do repositório de dados se o provisionamento dinâmico for usado.
Armazenamento Solicitado	<p>Armazenamento provisionado em uso somente com objetos do VMware Cloud Director no datastore, incluindo:</p> <ul style="list-style-type: none"> ■ Máquinas virtuais provisionadas no VMware Cloud Director ■ Itens de catálogo (mídia e modelos) ■ NSX Edges ■ Requisitos de permuta de memória usados e não usados para máquinas virtuais <p>Esse valor não inclui o armazenamento solicitado por VMs de sombra ou discos intermediários em uma árvore de clone vinculado.</p>
vCenter Server	A instância do vCenter Server associada ao datastore.

Visualizar as redes externas em um centro de dados virtual de provedor

Você pode visualizar uma lista das redes externas que são acessíveis a um centro de dados virtual de provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **Redes externas**.

Resultados

Você pode visualizar uma lista das redes externas disponíveis com informações sobre suas configurações de CIDR de gateway e o uso do pool de IPs.

Usando o Kubernetes com o VMware Cloud Director

Ao usar o Kubernetes com o VMware Cloud Director, você pode fornecer um serviço Kubernetes de vários tenants para seus tenants.

Container Service Extension

Kubernetes Container Clusters são o plug-in do Container Service Extension para o VMware Cloud Director. Provedores de serviços e tenants devem usar o plug-in Kubernetes Container Clusters para criar clusters do Kubernetes. A partir do VMware Cloud Director 10.2, não é necessário baixar manualmente o plug-in e carregá-lo no VMware Cloud Director Service Provider Admin Portal. O plug-in está disponível no VMware Cloud Director por padrão. No entanto, você deve publicá-lo nos tenants para permitir que eles criem clusters do Kubernetes.

Tanto provedores de serviços quanto tenants devem usar o Container Service Extension versão 3.0 para criar clusters nativos e VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). Você deve concluir a configuração do Container Service Extension 3.0 do servidor e publicar uma política de posicionamento nativa do Container Service Extension para um ou mais VDCs de organização.

vSphere with VMware Tanzu no VMware Cloud Director

Você pode usar o vSphere with VMware Tanzu no VMware Cloud Director para criar centros de dados virtuais (VDCs) de provedor com o suporte de Clusters de Supervisor. Um cluster de host com o vSphere with VMware Tanzu ativado é chamado de Cluster de Supervisor. Você pode definir restrições sobre os usos dos recursos e limitar os recursos disponíveis, incluindo o número de clusters do Kubernetes por organização, usuário ou grupo. Para obter mais informações, consulte [Gerenciar cotas sobre o consumo de recursos de uma organização](#).

Para usar o vSphere with VMware Tanzu no VMware Cloud Director, primeiro você deve ativar a funcionalidade do vSphere with VMware Tanzu em um cluster do vSphere 7.0 ou posterior e configurar esse cluster como um Cluster de Supervisor. Consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere. A instância do vCenter Server que você deseja usar pode ter clusters de hosts e Clusters de Supervisor.

Para criar clusters do Tanzu Kubernetes, você deve publicar uma política do Kubernetes do VDC de provedor em uma organização e aplicar a política do Kubernetes do VDC de organização durante a criação. Clusters nativos e TKGI não usam as políticas do Kubernetes do VDC de provedor e organização.

Tipos de cluster do Kubernetes

- 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. Para a implantação do cluster do Kubernetes nativo, você deve configurar um servidor do Container Service Extension. Consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- Clusters do Tanzu Kubernetes - Você pode usar o vSphere com a opção de tempo de execução do Tanzu para criar clusters do Tanzu Kubernetes gerenciados pelo vSphere with VMware Tanzu. 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 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, recuperação automática e atualizações contínuas para clusters do Kubernetes. Para obter mais informações sobre clusters TKGI, consulte a documentação do *VMware Tanzu Kubernetes Grid Integrated Edition*.

Fluxo de trabalho para criação de clusters do Tanzu Kubernetes

- 1 Adicione uma instância do vCenter Server 7.0 ou posterior com uma funcionalidade do vSphere with VMware Tanzu ativada ao VMware Cloud Director. Consulte [Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager](#).

- 2 Verifique as configurações de rede em cada Cluster de Supervisor para ativá-las para executar cargas de trabalho do Kubernetes.

Importante Os intervalos de endereços IP para os parâmetros `Ingress CIDRs` e `Services CIDR` não devem se sobrepor aos endereços IP 10.96.0.0/12 e 192.168.0.0/16 que são os valores de vSphere padrão para os parâmetros `services` e `Pods`. Consulte os parâmetros de configuração para informações de clusters do Tanzu Kubernetes no guia *Gerenciamento e configuração do vSphere with Kubernetes*.

Observação No VMware Cloud Director 10.2.2, se você modificar as configurações de rede do cluster supervisor após a configuração inicial, deverá atualizar a instância do vCenter Server para ajustar as políticas de firewall e regras NAT automáticas que bloqueiam o acesso ao cluster do Tanzu Kubernetes de fora do centro de dados virtual da organização no qual esse cluster é criado.

- 3 Crie um VDC de provedor com o suporte de um Cluster de Supervisor. Consulte [Criar um centro de dados virtual do provedor](#).

Como alternativa, você pode adicionar um Cluster de Supervisor a um VDC de provedor existente. Se você tiver um ambiente do vSphere 6.7 ou anterior, também poderá atualizar esse ambiente para a versão 7.0 e ativar o vSphere with VMware Tanzu em um cluster existente.

VDCs de provedor com o suporte de um Cluster de Supervisor aparecem com um ícone do Kubernetes ao lado do seu nome na grade que lista todos os VDCs de provedor.

- 4 (Opcional) O VMware Cloud Director gera automaticamente uma política do Kubernetes de VDC de provedor padrão para VDCs de provedor com o suporte de um Cluster de Supervisor. Você pode criar políticas do Kubernetes do VDC de provedor adicionais para clusters do Tanzu Kubernetes. Consulte [Criar uma política do Kubernetes do VDC de provedor](#).
- 5 [Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização](#) na guia **VDCs de Provedor** ou [Adicionar uma política do Kubernetes do VDC de Organização](#) na guia **VDCs de Organização**.
- 6 Publique o plug-in Kubernetes Container Clusters para provedores de serviços. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#). Se quiser permitir que os tenants criem clusters do Kubernetes, você deverá publicar o plug-in Kubernetes Container Clusters para essas organizações. Para obter mais informações sobre como gerenciar plug-ins do VMware Cloud Director, consulte [Gerenciando plug-ins](#).
- 7 Se quiser conceder aos tenants os direitos para criar e gerenciar clusters do Tanzu Kubernetes, você deverá publicar o pacote de direitos **vmware:tkgcluster Entitlement** a todas as organizações que você deseja trabalhar com clusters. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit: Tanzu Kubernetes Guest Cluster** às funções que deseja criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control: Tanzu Kubernetes Guest Cluster** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja

que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).

- 8 Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).
- 9 [Criar um cluster do Tanzu Kubernetes](#)

Fluxo de trabalho para a criação de clusters nativos e TKGI

- 1 Publique o plug-in Kubernetes Container Clusters para provedores de serviços. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#). Se quiser permitir que os tenants criem clusters do Kubernetes, você deverá publicar o plug-in Kubernetes Container Clusters para essas organizações. Para obter mais informações sobre como gerenciar plug-ins do VMware Cloud Director, consulte [Gerenciando plug-ins](#).
- 2 Configure um servidor Container Service Extension e publique a política de posicionamento nativa do Container Service Extension ou os metadados de ativação do TKGI para o VDC de organização. Para obter mais informações sobre como configurar o servidor CSE, consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- 3 Se quiser conceder aos tenants os direitos para criar e gerenciar clusters nativos, você deverá publicar o pacote de direitos **cse:nativeCluster Entitlement** a todas as organizações que você deseja trabalhar com clusters nativos. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit CSE:NATIVECLUSTER** às funções que deseja criar e modificar clusters nativos. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control CSE:NATIVECLUSTER** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que exibam todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- 4 Se você deseja conceder aos tenants os direitos de criar e gerenciar clusters do TKGI, deverá publicar **{cse}:PKS DEPLOY RIGHT** para as organizações específicas e adicionar o direito **{cse}:PKS DEPLOY RIGHT** às funções que você deseja que criem e gerenciem clusters do TKGI. O direito **{cse}:PKS DEPLOY RIGHT** é criado durante a instalação do servidor Container Service Extension.
- 5 Para clusters nativos, conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).
- 6 [Criar um cluster do Kubernetes nativo](#) ou [Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition](#).

Criando um cluster do vSphere with VMware Tanzu

Você pode usar as políticas do Kubernetes do VDC de provedor e do VDC de organização para criar clusters do vSphere with VMware Tanzu.

vSphere with VMware Tanzu no VMware Cloud Director

Quando ativado em um cluster do vSphere, o vSphere with VMware Tanzu fornece a capacidade de executar cargas de trabalho do Kubernetes diretamente em hosts ESXi e de criar clusters do Kubernetes 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.

Você pode usar o vSphere with VMware Tanzu no VMware Cloud Director para criar centros de dados virtuais (VDCs) de provedor com o suporte de Clusters de Supervisor. Um cluster de host com o vSphere with VMware Tanzu ativado é chamado de Cluster de Supervisor. Você pode definir restrições sobre os usos dos recursos e limitar os recursos disponíveis, incluindo o número de clusters do Kubernetes por organização, usuário ou grupo. Para obter mais informações, consulte [Gerenciar cotas sobre o consumo de recursos de uma organização](#).

Para usar o vSphere with VMware Tanzu no VMware Cloud Director, primeiro você deve ativar a funcionalidade do vSphere with VMware Tanzu em um cluster do vSphere 7.0 ou posterior e configurar esse cluster como um Cluster de Supervisor. Consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere. A instância do vCenter Server que você deseja usar pode ter clusters de hosts e Clusters de Supervisor.

Os tenants podem criar clusters do Tanzu Kubernetes aplicando uma das políticas do Kubernetes do VDC de organização. Os administradores do sistema podem editar e excluir as políticas do Kubernetes do VDC de organização usando o Service Provider Admin Portal ou o VMware Cloud Director Tenant Portal. Clusters nativos e TKGI não usam as políticas do Kubernetes do VDC de provedor e organização.

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*.

Fluxo de trabalho

- 1 Adicione uma instância do vCenter Server 7.0 ou posterior com uma funcionalidade do vSphere with VMware Tanzu ativada ao VMware Cloud Director. Consulte [Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager](#).
- 2 Crie um VDC de provedor com o suporte de um Cluster de Supervisor. Consulte [Criar um centro de dados virtual do provedor](#).

Como alternativa, você pode adicionar um Cluster de Supervisor a um VDC de provedor existente. Se você tiver um ambiente do vSphere 6.7 ou anterior, também poderá atualizar esse ambiente para a versão 7.0 e ativar o vSphere with VMware Tanzu em um cluster existente.

VDCs de provedor com o suporte de um Cluster de Supervisor aparecem com um ícone do Kubernetes ao lado do seu nome na grade que lista todos os VDCs de provedor.

- 3 (Opcional) O VMware Cloud Director gera automaticamente uma política do Kubernetes de VDC de provedor padrão para VDCs de provedor com o suporte de um Cluster de Supervisor. Você pode criar políticas do Kubernetes do VDC de provedor adicionais para clusters do Tanzu Kubernetes. Consulte [Criar uma política do Kubernetes do VDC de provedor](#).
- 4 [Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização](#) na guia **VDCs de Provedor** ou [Adicionar uma política do Kubernetes do VDC de Organização](#) na guia **VDCs de Organização**.
- 5 Publique o plug-in Kubernetes Container Clusters para provedores de serviços. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#). Se quiser permitir que os tenants criem clusters do Kubernetes, você deverá publicar o plug-in Kubernetes Container Clusters para essas organizações. Para obter mais informações sobre como gerenciar plug-ins do VMware Cloud Director, consulte [Gerenciando plug-ins](#).
- 6 Publique o pacote de direitos **vmware:tkgcluster Entitlement** em todas as organizações que você deseja trabalhar com clusters do Tanzu Kubernetes.
- 7 Adicione o direito **Edit: Tanzu Kubernetes Guest Cluster** às funções que você deseja criar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control: Tanzu Kubernetes Guest Cluster** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- 8 Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).
- 9 [Criar um cluster do Tanzu Kubernetes](#)

Criar uma política do Kubernetes do VDC de provedor

O VMware Cloud Director gera automaticamente uma política do Kubernetes do VDC de provedor padrão para VDCs de provedor com o suporte de um Cluster de Supervisor. Você pode criar políticas do Kubernetes do VDC de provedor adicionais para clusters do Tanzu Kubernetes.

Políticas do Kubernetes do VDC de provedor e de VDC de organização serão necessárias apenas se você quiser criar ou permitir que os tenants criem clusters do Tanzu Kubernetes. Clusters nativos e TKGI não usam essas políticas do Kubernetes.

Pré-requisitos

Certifique-se de ter pelo menos um VDC de provedor com o suporte de um Cluster de Supervisor ou adicione um Cluster de Supervisor a um VDC de provedor existente. Consulte [Usando o Kubernetes com o VMware Cloud Director](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Provedor** e clique no nome de um VDC de provedor.
- 3 Em Políticas, selecione **Kubernetes** e clique em **Novo**.

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

- 4 Insira um nome e uma descrição para a política do Kubernetes do VDC de provedor e clique em **Avançar**.
- 5 Selecione um pool de recursos com o suporte de Cluster de Supervisor com capacidade para Kubernetes.
- 6 Escolha se deseja reservar a CPU e a memória para os nós de cluster do Kubernetes criados nessa política.

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.

- 7 Selecione limites de CPU e Memória para os clusters do Kubernetes criados de acordo com essa política.

Quando você publicar a política em um VDC de organização, os limites selecionados atuarão como máximos para a política do Kubernetes do VDC de organização recém-criada.

- 8 Clique em **Avançar**.
- 9 Na página **Classes de máquinas** do assistente, selecione um ou mais tipos de classe de VM disponíveis para essa política e clique em **Avançar**.

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

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

Próximo passo

[Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização](#)

Editar uma política do Kubernetes do vSphere

Você pode editar as configurações de políticas do Kubernetes de VDC de provedor usadas para a criação de políticas do Kubernetes de VDC de organização e clusters do Tanzu Kubernetes.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Provedor** e clique no nome de um VDC de provedor.
- 3 (Opcional) Em Políticas, selecione **Kubernetes**, selecione a política que você deseja publicar e clique em **Editar**.

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

- 4 (Opcional) Edite o nome e a descrição da política do Kubernetes do VDC de provedor e clique em **Avançar**.
- 5 (Opcional) Altere os limites de CPU e memória para os clusters do Kubernetes criados de acordo com essa política e clique em **Avançar**.

Quando você publicar a política em um VDC de organização, os limites selecionados atuarão como máximos para a política do Kubernetes do VDC de organização recém-criada.

- 6 (Opcional) Na página **Classes de máquinas** do assistente, adicione um ou mais tipos de classe de VM disponíveis para essa política e clique em **Avançar**.

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

- 7 (Opcional) Adicione uma ou mais políticas de armazenamento.
- 8 Revise suas escolhas e clique em **Salvar**.

Próximo passo

[Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização](#)

Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização

Para disponibilizar uma política do Kubernetes do VDC de provedor para os tenants, você pode publicá-la em um VDC de organização flexível. Ao publicar uma política do Kubernetes do VDC de provedor, você cria uma política do Kubernetes do VDC de organização que os tenants podem usar para criar clusters do Kubernetes.

Ao adicionar ou publicar uma política do Kubernetes do VDC de provedor a um VDC de organização, você torna essa política disponível para os tenants. Os tenants podem usar as políticas do Kubernetes do VDC de organização disponíveis para aproveitar a capacidade do Kubernetes ao criar clusters do 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.

Você pode publicar várias políticas do Kubernetes do VDC de provedor para um único VDC de organização. Você pode publicar uma única política do Kubernetes do VDC de provedor várias vezes para um 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

- Crie um VDC de provedor com o suporte de um Cluster de Supervisor ou adicione um Cluster de Supervisor a um VDC de provedor existente. Consulte [Usando o Kubernetes com o VMware Cloud Director](#).
- Verifique se você tem pelo menos um VDC de organização flexível no seu ambiente. Consulte [Criar um centro de dados virtual da organização](#).
- 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Provedor** e clique no nome de um VDC de provedor.
- 3 Em Políticas, selecione **Kubernetes**, selecione a política que você deseja publicar e clique em **Publicar**.

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 o VDC de organização flexível para o qual você deseja publicar a política e clique em **Avançar**.
- 6 Selecione limites de CPU e Memória para os clusters do Kubernetes criados de acordo com essa política.

Os limites máximos dependem das alocações de Memória e CPU do VDC de organização. Quando você publicar 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 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 publica a política em um 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 seção Políticas do VDC de organização flexível. 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 Kubernetes. O VMware Cloud Director coloca cada cluster do 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 Kubernetes criados pelo tenant no Namespace de Supervisor competem pelos recursos dentro desses limites.

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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

- Publique o plug-in Kubernetes Container Clusters em qualquer organização que você deseja gerenciar clusters do Tanzu Kubernetes.
- 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](#).
- Você deve publicar o pacote de direitos **vmware:tkgcluster Entitlement** para todas as organizações que você deseja trabalhar com clusters. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit: Tanzu Kubernetes Guest Cluster** às funções que deseja criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control: Tanzu Kubernetes Guest Cluster** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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**.
- Para ativar o VDC de organização para implantação de cluster do Kubernetes nativo, configure o servidor Container Service Extension. Consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- Publique a política nativa de CSE criada durante a configuração do servidor CSE em um VDC de organização. Para usar a interface de usuário, consulte [Adicionar uma política de posicionamento de VM a um VDC de organização](#). Como alternativa, você pode usar o CSE 3.0 CLI para publicar a política executando o comando `vcd cse ovdc enable Organization_VDC_Name --org Organization_Name --native`.
- Você deve publicar o pacote de direitos **cse:nativeCluster Entitlement** para qualquer organização que queira trabalhar com clusters nativos. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit CSE:NATIVECLUSTER** às funções que deseja para criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control CSE:NATIVECLUSTER** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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

Ao usar os metadados de ativação do TKGI, você pode fornecer acesso aos tenants para criar clusters do TKGI e acessar o VDC de organização ativado para TKGI. Se você deseja limitar a capacidade dos tenants de criar clusters do TKGI, poderá fornecer acesso apenas ao VDC de organização. Nesse caso, os tenants podem gerenciar clusters do TKGI existentes, mas não podem criar novos.

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**.

- Para ativar o VDC de organização para implantação de cluster do Kubernetes TKGI, configure o servidor Container Service Extension. Para obter informações sobre como usar a CSE CLI para ativar um VDC de organização para o TKGI, consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- Se você deseja fornecer acesso de tenant à criação e ao gerenciamento de TKGI, deverá publicar **{cse}:PKS DEPLOY RIGHT** para as organizações específicas e adicionar o direito **{cse}:PKS DEPLOY RIGHT** às funções que você deseja criar e gerenciar clusters do TKGI. O direito **{cse}:PKS DEPLOY RIGHT** é criado durante a instalação do servidor Container Service Extension.

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.

Gerenciamento das políticas de armazenamento de VM em um centro de dados virtual do provedor

Você pode adicionar, ativar, desativar e remover políticas de armazenamento de VM de um centro de dados virtual do provedor (VDC). Você pode adicionar, editar e excluir metadados para uma política de armazenamento de VM em um centro de dados virtual de provedor.

No VMware Cloud Director 10.2.2, você pode limitar as entidades permitidas em uma política de armazenamento. Consulte [Editar os tipos de entidade aos quais uma política de armazenamento oferece suporte](#).

Habilitando a criptografia da VM em políticas de armazenamento de um centro de dados virtual do provedor

Você pode adicionar uma política de armazenamento habilitada para criptografia a um VDC de provedor. Você pode criptografar VMs e discos associando uma VM ou um disco a uma política de armazenamento que tenha o recurso de criptografia de VM.

A partir do VMware Cloud Director 10.1, você pode melhorar a segurança dos seus dados usando a criptografia da 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.

Habilitando a detecção de VM

Para criptografar VMs no VMware Cloud Director, você deve configurar pelo menos um servidor de gerenciamento de chaves (KMS) em sua instância do vCenter Server e associar as VMs e discos a uma política de armazenamento que tenha o recurso de criptografia de VM.

- 1 No vCenter Server, adicione um cluster KMS. Uma instância do vCenter Server pode ter vários clusters KMS. Para obter informações sobre como configurar um cluster de servidor de gerenciamento de chaves, consulte o tópico [Configurar o cluster do servidor de gerenciamento de chaves](#) no *vSphere Guia de segurança*.
- 2 No vCenter Server, habilite a criptografia em uma política de armazenamento. Consulte o tópico [Criar uma política de armazenamento de criptografia](#) no *vSphere Guia de segurança*.
- 3 No VMware Cloud Director Service Provider Admin Portal, adicione a política habilitada para criptografia a um VDC de provedor. Consulte [Adicionar uma política de armazenamento de VM a um datacenter virtual do provedor](#).
- 4 No VMware Cloud Director Service Provider Admin Portal, adicione a política habilitada para criptografia a um VDC de organização. Consulte [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#).
- 5 No VMware Cloud Director Tenant Portal, os tenants podem associar a VM ou o disco a uma política de armazenamento com criptografia de VM habilitada.
- 6 Para descriptografar uma VM ou um disco, os tenants podem associar 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 suportadas no 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 VMs e discos. Para obter mais informações sobre funções e direitos, consulte [Funções predefinidas e seus direitos](#).

Você pode ver todos os recursos de armazenamento na coluna **Recursos** em **Recursos > Recursos do vSphere > Políticas de Armazenamento**. Essa coluna exibe a criptografia da VM, a associação baseada em tags, o vSAN e o IOPS limitando os recursos de armazenamento. Para visualizar a lista completa de recursos de armazenamento, expanda a linha clicando na seta à esquerda do nome da política de armazenamento.

Você também pode visualizar as informações de recurso de armazenamento na guia **Políticas de Armazenamento** de um VDC de provedor.

Adicionar uma política de armazenamento de VM a um datacenter virtual do provedor

Você pode adicionar uma política de armazenamento de VM a um datacenter virtual do provedor, o que lhe permite configurar os datacenters virtuais da organização suportados por esse datacenter virtual do provedor para dar suporte à política de armazenamento adicionada.

Pré-requisitos

- O administrador do vSphere criou a política de armazenamento de VM de destino. Para obter informações sobre o Gerenciamento baseado em política de armazenamento (SPBM), consulte a documentação de *Armazenamento do vSphere*.
- [Atualizar as políticas de armazenamento de uma instância do vCenter Server](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento** e clique em **Adicionar**.
- 4 Selecione uma ou mais políticas de armazenamento que deseja adicionar e clique em **Adicionar**.

Se você selecionar * **(Qualquer)**, o VMware Cloud Director adicionará e removerá dinamicamente os datastores à medida que são adicionados ou removidos dos clusters de datastore do centro de dados virtual do provedor.

Próximo passo

Configure os datacenters virtuais da organização com suporte do datacenter virtual do provedor para dar suporte à política de armazenamento. Consulte [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#).

Ativar ou desativar uma política de armazenamento de VM em um centro de dados virtual do provedor

Depois de desativar uma política de armazenamento de VM em um centro de dados virtual de provedor, seus centros de dados virtuais de organização não poderão mais usar essa política de armazenamento de VM.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de VM de destino e clique em **Habilitar** ou **Desabilitar**.
- 5 Para confirmar, clique em **OK**.

Excluir uma política de armazenamento de VM de um data center virtual de provedor

Você pode excluir uma política de armazenamento de VM de um data center virtual de provedor.

Pré-requisitos

Desative a política de armazenamento de VM de destino. Consulte [Ativar ou desativar uma política de armazenamento de VM em um centro de dados virtual do provedor](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de VM de destino e clique em **Remover**.
- 5 Para confirmar, clique em **Remover**.

Modificar os metadados de uma política de armazenamento de VM em um data center virtual de provedor

Você pode adicionar, editar e excluir metadados para uma política de armazenamento em um data center virtual de provedor.

Usando os metadados do objeto, você pode associar pares de *nome=valor* definidos pelo usuário com uma política de armazenamento num centro de dados virtual de provedor. Você pode usar os metadados do objeto nas expressões de filtro de consulta da API do vCloud.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de VM de destino e clique em **Metadados**.
- 5 Clique em **Editar**.
- 6 (Opcional) Para adicionar um par chave-valor, clique em **Adicionar**, insira um nome e um valor e selecione um tipo para o novo par chave-valor.
- 7 (Opcional) Para editar um par de chave-valor, insira um novo nome e um valor e selecione um novo tipo para o par chave-valor.

- 8 (Opcional) Para remover um par de chave/valor, na extremidade direita da linha, clique no ícone **Excluir**.
- 9 Clique em **Salvar** e em **OK**.

Ativando a configuração de operações de E/S por segundo

Você pode ativar a configuração de operações de E/S por segundo (IOPS) para uma política de armazenamento para que os tenants possam definir os limites de IOPS por disco.

O desempenho de leitura/gravação gerenciado em dispositivos de armazenamento físico e discos virtuais é definido em unidades chamadas IOPS, que medem as operações de leitura/gravação por segundo. Para limitar o desempenho de E/S, uma política de armazenamento de VDC de provedor que inclui dispositivos de armazenamento com alocação de IOPS habilitada deve voltar a uma política de armazenamento de VDC de organização. Posteriormente, um tenant pode configurar discos que o usam para solicitar um nível especificado de desempenho de E/S. Um perfil de armazenamento configurado com suporte a IOPS entrega seu valor padrão de IOPS para todos os discos que o usam. Isso inclui discos que não estão configurados para solicitar um valor de IOPS específico. Um disco rígido configurado para solicitar um valor de IOPS específico não pode usar uma política de armazenamento cujo valor de IOPS máximo seja inferior ao valor solicitado ou uma política de armazenamento que não está configurada com suporte a IOPS.

Observação A taxa de transferência real de E/S que as máquinas virtuais veem é uma combinação de tamanho e IOPS de bloco. Se as VMs estiverem usando diferentes tamanhos de bloco, sua taxa de transferência será diferente, mesmo se o IOPS estiver limitado ao mesmo número. Para obter mais informações sobre como gerenciar recursos de E/S de armazenamento, consulte o guia *Gerenciamento de recursos do vSphere*.

Política de armazenamento de IOPS do VMware Cloud Director

Com essa opção, há configurações de IOPS padrão que podem ser editadas. Você pode definir limites de IOPS por disco ou IOPS por política de armazenamento. É possível definir limites de IOPS por disco com base no tamanho do disco em GB, para que você conceda mais IOPS para discos maiores. Os tenants podem definir configurações de IOPS personalizadas em um disco dentro desses limites. Você pode usar a limitação de IOPS com ou sem as considerações de capacidade de IOPS para posicionamento.

Não é possível ativar o IOPS em uma política de armazenamento com suporte de um cluster do DRS de Armazenamento.

- 1 Se você deseja que o VMware Cloud Director considere o IOPS ao colocar discos em repositórios de dados, no vCenter Server, adicione capacidades de IOPS a todos os repositórios de dados associados à política de armazenamento que você deseja modificar.
- 2 Se você deseja que o VMware Cloud Director considere o IOPS ao colocar discos em repositórios de dados, no vCenter Server, crie uma política de armazenamento que use os repositórios de dados com capacidades de IOPS adicionadas.

- 3 Usando o VMware Cloud Director Service Provider Admin Portal ou a API do VMware Cloud Director, adicione a política de armazenamento a um ou mais VDCs de provedor.
- 4 Ao usar o Service Provider Admin Portal ou a API do VMware Cloud Director, publique a política de armazenamento em um ou mais VDCs de organização. Os VDCs de organização nos quais você publicar a política de armazenamento herdarão as configurações de IOPS da política.
- 5 Se quiser editar as configurações de IOPS da política de armazenamento herdada, use o Service Provider Admin Portal ou a API do VMware Cloud Director para atualizar a política de armazenamento de VDC de organização.

Esse tipo de política é exibido como uma capacidade de `VCD/IOPS` da política de armazenamento.

Política de armazenamento de IOPS do vCenter Server

Essa opção tem uma configuração de IOPS para todos os discos que usam essa política. Não é possível editar essa configuração no VMware Cloud Director. Os tenants não podem definir configurações de IOPS personalizadas nos discos usando essas políticas. Essa opção não fornece dimensionamento de IOPS, dependendo dos tamanhos dos discos ou do balanceamento de carga entre repositórios de dados.

- 1 No vCenter Server, crie uma política de armazenamento habilitada para VC-IOPS com reserva, limite e compartilhamentos personalizados.
- 2 No vCenter Server ou VMware Cloud Director Service Provider Admin Portal, atribua o disco à política de armazenamento.

Esse tipo de política é exibido como uma capacidade de `vSphere/IOPS` da política de armazenamento. Quando a VM de origem ou de destino tem o recurso `vSphere/IOPS`, não é possível criar VMs de provisionamento rápido.

Configurando IOPS em um disco no vCenter Server

Para alterar a configuração de IOPS, no vCenter Server, atualize manualmente o IOPS no disco. Não é possível editar essas configurações de IOPS no VMware Cloud Director.

Ativando a limitação de IOPS em uma política de armazenamento existente

Observação Não é possível ativar a limitação de IOPS do VMware Cloud Director em uma política que já tenha o recurso `vSphere/IOPS` nela.

- Ative a limitação de IOPS em uma política de armazenamento de `VCD/IOPS`:
 - a Se você deseja que o VMware Cloud Director considere as capacidades de IOPS ao colocar discos em repositórios de dados, no vCenter Server, adicione capacidades de IOPS a todos os repositórios de dados associados à política de armazenamento que você deseja modificar.

- b Se você deseja que o VMware Cloud Director considere as capacidades de IOPS ao colocar discos em repositórios de dados, usando a API do VMware Cloud Director Service Provider Admin Portal ou do VMware Cloud Director, certifique-se de que a política de armazenamento de VDC de provedor correspondente relate a capacidade de IOPS como diferente de zero.
 - c Usando o VMware Cloud Director Service Provider Admin Portal ou a API do VMware Cloud Director, atualize a política de armazenamento de VDC de organização para ativar a capacidade de VCD/IOPS e para definir o valor máximo de IOPS, o valor padrão de IOPS e assim por diante.
- Ative a limitação de IOPS em uma política de armazenamento de vSphere/IOPS no vCenter Server.

Quando você ativa a limitação de IOPS para uma política de armazenamento de VDC de organização, os tenants podem usar o VMware Cloud Director Tenant Portal para definir limites de IOPS por disco.

Editar as configurações de política de armazenamento de VDC de provedor

É possível alterar as configurações de operações de E/S por segundo (IOPS) de uma política de armazenamento de VDC de provedor. Por padrão, os VDCs de organização aos quais a política é publicada herdam as configurações de política de armazenamento de VDC de provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de destino e clique em **Editar Configurações**.
- 5 Se quiser limitar as operações de E/S por segundo, ative o botão de alternância **Limitação de IOPS**.
- 6 Se quiser que as operações de IOPS sejam consideradas durante o posicionamento, ative o botão de alternância **Afetar Posicionamento**.

Se o botão de alternância de **Afetar Posicionamento** estiver ativado, o VMware Cloud Director fornecerá balanceamento de carga de IOPS entre os repositórios de dados. Quando você define as configurações de IOPS para um disco, o VMware Cloud Director considera os repositórios de dados com capacidade de IOPS suficiente para o disco selecionado. Se o botão de alternância de **Afetar Posicionamento** estiver desativado, você não precisará definir as capacidades de IOPS por repositório de dados e poderá usar os clusters de DRS de Armazenamento.

7 Defina as configurações máximas e padrão para IOPS e clique em **Salvar**.

Resultados

As novas configurações de política de armazenamento aplicam-se a todos os VDCs de organização aos quais essa política é publicada.

Editar os tipos de entidade aos quais uma política de armazenamento oferece suporte

No VMware Cloud Director 10.2.2, se você não quiser que uma política de armazenamento de VDC do provedor ofereça suporte a certos tipos de entidades do VMware Cloud Director, será possível editar e limitar a lista de entidades associadas à política.

Quando você cria uma política de armazenamento de VDC do provedor, por padrão, ela oferece suporte a todos os tipos de entidade disponíveis. Os tipos de entidade padrão são:

- Máquinas virtuais
- Discos nomeados
- Mídia de catálogo
- Modelos de vApp e VM
- Clusters Tanzu Kubernetes
- Edge gateways

É possível limitar os tipos de entidade para os quais uma política de armazenamento oferece suporte a um ou mais tipos nessa lista. Quando você cria uma entidade, apenas as políticas de armazenamento que oferecem suporte ao seu tipo ficam disponíveis. Por exemplo, se você quiser criar um catálogo, as únicas políticas de armazenamento que aparecem serão as que oferecem suporte para mídias de catálogo, modelos de vApp ou ambas. Se uma entidade usar uma política de armazenamento e você remover o tipo de entidade da lista de tipos de entidades com suporte, essa entidade continuará a usar a política de armazenamento, mas você não poderá fazer alterações nela sem selecionar uma nova política de armazenamento.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de destino e clique em **Editar Tipos com Suporte**.
- 5 No menu **Oferece Suporte a Tipos de Entidade**, escolha **Selecionar Entidades Específicas**.
- 6 Selecione as entidades para as quais você deseja que a política de armazenamento ofereça suporte e clique em **Salvar**.

Próximo passo

- [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#)
- Os usuários com o direito **Tipo de Entidade de Armazenamento com Suporte: Gerenciar** podem usar a OpenAPI do VMware Cloud Director para adicionar ou remover tipos de entidade da lista de tipos disponíveis para todas as políticas de armazenamento. Por exemplo, você pode adicionar entidades definidas de tempo de execução (RDEs) à lista ou removê-las da lista. Para obter mais informações sobre como criar extensões que fornecem recursos adicionais do VMware Cloud Director aos tenants, consulte a [Capítulo 14 Gerenciamento de entidades definidas](#).

O VMware Cloud Director aplica automaticamente as alterações às políticas de armazenamento que oferecem suporte a todas as entidades. Não é possível remover entidades selecionadas especificamente em uma ou mais políticas de armazenamento.

Gerenciamento dos pools de recursos em um centro de dados virtual do provedor

Você pode adicionar, ativar, desativar e desanexar pools de recursos secundários de um centro de dados virtual de provedor. Não é possível desativar ou desanexar o pool de recursos primários em um centro de dados virtual do provedor.

Adicionar um pool de recursos a um data center virtual de um provedor

Você pode adicionar um ou mais pools de recursos secundários a um data center virtual do provedor, para que seus data centers virtuais da organização com pagamento por consumo e pool de alocações possam ser expandidos.

Quando os recursos de processamento têm o suporte de vários pools de recursos, eles podem se expandir para acomodar mais máquinas virtuais.

Você pode adicionar pools de recursos que tenham suporte de clusters do vSphere, que estão configurados para hospedar NSX Edges com uplinks de VLAN. O VMware Cloud Director pode usar metadados para indicar que o sistema deve colocar Edge Gateways do VDC da organização em pools de recursos que tenham suporte desses clusters. Para obter mais informações, consulte o artigo da Base de Conhecimento da VMware <https://kb.vmware.com/kb/2151398>

Pré-requisitos

O administrador do vSphere criou o pool de recursos secundários de destino na instância do vCenter Server, que faz backup do pool de recursos primários do data center virtual do provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.

- 3 Na guia **Pools de recursos**, clique em **Adicionar**.
- 4 Selecione o pool de recursos que você deseja adicionar e clique em **Adicionar**.

Se quiser usar o vSphere with VMware Tanzu, selecione um Cluster de Supervisor. O VMware Cloud Director exibe um ícone do Kubernetes ao lado dos pools de recursos com o suporte de um Cluster de Supervisor.
- 5 Se você selecionar um pool de recursos ou um cluster com suporte por um Cluster de Supervisor, para estabelecer um relacionamento de confiança com a camada de controle do Kubernetes, você deverá confiar no certificado dela.
- 6 Se quiser adicionar mais um pool de recursos, repita de [Etapa 1](#) a [Etapa 5](#).

Resultados

O VMware Cloud Director adiciona um pool de recursos para o data center virtual do provedor usar, tornando elásticos todos os data centers virtuais da organização com pagamento por consumo e pools de alocações com suporte do data center virtual do provedor.

O VMware Cloud Director também adiciona um pool de recursos do VDC de Sistema sob o novo pool de recursos. Esse pool de recursos é usado para a criação de recursos do sistema, como VMs do NSX Edge e VMs que servem como um modelo para os clones vinculados.

Importante Não edite nem exclua o pool de recursos do VDC de Sistema.

Ativar ou desativar um pool de recursos em um centro de dados virtual de provedor

Quando você desativa um pool de recursos, os recursos de memória e computação desse pool não ficam mais disponíveis para o centro de dados virtual de provedor.

Os processos que já estão em andamento não param de usar recursos do pool de recursos desativado.

Observação Não é possível desativar o pool de recursos primário em um centro de dados virtual do provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **Pools de Recursos**.
- 4 Clique no botão de opção ao lado do pool de recursos de destino e clique em **Habilitar** ou **Desabilitar**.
- 5 Para confirmar, clique em **OK**.

Desanexar um pool de recursos de um centro de dados virtual de provedor

Se um centro de dados virtual do provedor tiver mais de um pool de recursos, você poderá desanexar um pool de recursos secundário do centro de dados virtual do provedor. Não é possível desanexar o pool de recursos primário do centro de dados virtual do provedor.

Pré-requisitos

- Desative o pool de recursos de destino no centro de dados virtual do provedor. Consulte [Ativar ou desativar um pool de recursos em um centro de dados virtual de provedor](#).
- Reimplante todas as redes afetadas pelo pool de recursos desativado.
- Reimplante todos os edge gateways afetados pelo pool de recursos desativado.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **Pools de Recursos**.
- 4 Clique no botão de opção ao lado do pool de recursos de destino e clique em **Desanexar**.
- 5 Para confirmar, clique em **OK**.

Modificar os metadados para um centro de dados virtual de provedor

Você pode adicionar, editar e excluir metadados para um centro de dados virtual de provedor.

Ao usar os metadados do objeto, você pode associar os pares *nome=valor* definidos pelo usuário com um centro de dados virtual de provedor. Você pode usar os metadados do objeto nas expressões de filtro de consulta da API do vCloud.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Na guia **Configurar > Metadados**, no canto superior direito, clique em **Editar**.
- 4 (Opcional) Para adicionar um par chave-valor, clique em **Adicionar**, insira um nome e um valor e selecione um tipo para o novo par chave-valor.
- 5 (Opcional) Para editar um par de chave-valor, insira um novo nome e um valor e selecione um novo tipo para o par chave-valor.

- 6 (Opcional) Para remover um par de chave/valor, na extremidade direita da linha, clique no ícone **Excluir**.
- 7 Clique em **Salvar** e em **OK**.

Gerenciamento de organizações

5

O VMware Cloud Director Service Provider Admin Portal permite criar, configurar e gerenciar as organizações do VMware Cloud Director.

Use o VMware Cloud Director Service Provider Admin Portal para gerenciar as organizações, defina as políticas para determinar como os usuários consomem os recursos alocados para uma organização e gerenciam a publicação e o compartilhamento de catálogos.

Este capítulo inclui os seguintes tópicos:

- [Noções básicas sobre leases](#)
- [Criar uma organização](#)
- [Ativar ou desativar uma organização](#)
- [Excluir uma organização](#)
- [Configurar os catálogos para uma organização](#)
- [Configurar as políticas para uma organização](#)
- [Migrar Armazenamento de Tenant](#)
- [Gerenciar cotas sobre o consumo de recursos de uma organização](#)

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 sair de férias sem pará-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.

Criar uma organização

Você pode criar uma nova organização partindo do VMware Cloud Director Service Provider Admin Portal.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
 - a No painel esquerdo, selecione **Organizações**.

A lista de organizações existentes é exibida em um modo de exibição de grade.

- 2 Clique em **Novo**.

Abre a caixa de diálogo **Nova Organização**.

- 3 Insira os seguintes valores.

Opção	Descrição
Nome da organização	O identificador exclusivo que forma a URL de acesso ao Portal do Tenant da organização.
Nome completo da organização	Nome completo da organização.
Descrição	Uma descrição opcional para a organização.

- 4 Clique no botão **Criar** para concluir a criação.

Ativar ou desativar uma organização

Desativar uma organização impede que os usuários efetuem login na organização e terminem as sessões dos usuários que estão conectados no momento. Os vApps em execução na organização continuam a ser executados.

Como **administrador do sistema**, você pode alocar recursos, adicionar redes e assim por diante, mesmo depois de desativar uma organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
 - a No painel esquerdo, selecione **Organizações**.A lista de organizações existentes é exibida em um modo de exibição de grade.
- 2 Clique no botão de opção ao lado do nome da organização e clique em **Habilitar** ou **Desabilitar**.

Excluir uma organização

Exclua uma organização para removê-la permanentemente do VMware Cloud Director.

Pré-requisitos

Antes de excluir uma organização, você deve desativá-la e excluir todos os centros de dados virtuais, modelos, arquivos de mídia e vApps da organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
 - a No painel esquerdo, selecione **Organizações**.A lista de organizações existentes é exibida em um modo de exibição de grade.
- 2 Clique no botão de seleção ao lado do nome da organização e clique em **Excluir**.
- 3 Para confirmar, clique em **Sim**.

Configurar os catálogos para uma organização

Você pode configurar como uma organização compartilha seus catálogos de serviços.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
 - a No painel esquerdo, selecione **Organizações**.A lista de organizações existentes é exibida em um modo de exibição de grade.
- 2 Selecione uma organização e, na guia **Configurar**, selecione **Catálogo**.

- 3 Para alterar as configurações de compartilhamento e publicação, clique em **Editar**.

Opção	Descrição
Compartilhando	Permite que os administradores da organização compartilhem os catálogos dessa organização com outras organizações nesta instância do VMware Cloud Director. Se você não selecionar essa opção, os administradores da organização ainda poderão compartilhar catálogos dentro da organização.
Permitir publicação em catálogos externos	Permite que os administradores da organização publiquem catálogos em organizações fora dessa instância do VMware Cloud Director.
Permitir assinatura de catálogos externos	Permite que os administradores da organização assinem catálogos fora dessa instância do VMware Cloud Director.

Configurar as políticas para uma organização

Lease, cotas e limites restringem a capacidade de usuários da organização em consumir recursos de processamento e armazenamento. Você pode modificar essas configurações para impedir que os usuários esgotem ou monopolizem os recursos da organização.

Pré-requisitos

Consulte [Noções básicas sobre leases](#).

Procedimentos

- Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
 - No painel esquerdo, selecione **Organizações**.
A lista de organizações existentes é exibida em um modo de exibição de grade.
- Selecione uma organização e selecione a guia **Políticas**.
- Clique em **Editar** para editar as concessões, as cotas, os limites de recursos e as políticas de senha para a organização.
- Configure as concessões do vApp com as seguintes configurações.

Opção	Descrição
Lease máximo de tempo de execução	Por quanto tempo os vApps podem ser executados antes de serem automaticamente parados.
Ação de expiração de tempo de execução	Como os vApps de execução expirados são processados. Suspender um vApp suspende todas as suas máquinas virtuais e preserva seu estado atual gravando a memória no disco. Desligar interrompe imediatamente todas as suas máquinas virtuais e vApps herdeiros.
Locação máxima de armazenamento	Por quanto tempo os vApps parados estarão disponíveis antes de serem automaticamente limpos.
Limpeza de armazenamento	Como os vApps são processados depois de serem interrompidos e limpos.

5 Configure as concessões de modelos do vApp com as seguintes configurações.

Opção	Descrição
Locação máxima de armazenamento	Por quanto tempo os modelos do vApp estarão disponíveis antes de serem automaticamente limpos.
Limpeza de armazenamento	Como modelos expirados do vApp são processados depois de serem limpos.

6 Configure as cotas do vApp com as seguintes configurações.

Opção	Descrição
Cota de todas as VMs	Número total de VMs disponíveis que um usuário pode armazenar nessa organização.
Executando cota de VMs	Número total de VMs que um usuário pode ativar nesta organização.

7 Configure os limites com as seguintes configurações.

Opção	Descrição
Número de operações com uso excessivo de recursos por usuário	Digite o número máximo de operações simultâneas com uso excessivo de recursos por usuário ou selecione Herdar limite do sistema .
Número de operações com uso excessivo de recursos para serem colocadas em fila por usuário	Digite o número máximo de operações em fila com uso excessivo de recursos por usuário ou selecione Herdar limite do sistema .
Número de operações com uso excessivo de recursos por organização	Digite o número máximo de operações simultâneas com uso excessivo de recursos por organização ou selecione Herdar limite do sistema .
Número de operações com uso excessivo de recursos para serem colocadas em fila por organização	Digite o número máximo de operações em fila com uso excessivo de recursos por organização ou selecione Herdar limite do sistema .
Número de conexões simultâneas por VM	Digite o número máximo de conexões de console simultâneas por máquina virtual ou selecione Herdar limite do sistema .
Número de datacenters virtuais por organização	Digite o número máximo de datacenters virtuais da organização por organização ou selecione Herdar cota do sistema .

8 Configure as políticas de senha com as seguintes configurações.

Opção	Descrição
Bloqueio de conta ativada	Ative o bloqueio de conta de usuário após várias tentativas de login inválidas.
Logins inválidos antes do bloqueio	Número de tentativas de login inválidas antes que a conta do usuário seja bloqueada.
Intervalo de bloqueio de conta	Período durante o qual uma conta de usuário bloqueada não pode fazer login.

Migrar Armazenamento de Tenant

Você pode migrar todos os vApps, discos independentes e itens de catálogo de uma ou mais organizações de um ou mais datastores para diferentes datastores.

Antes de desativar um datastore, você deve migrar todos os itens armazenados nesse datastore para um novo datastore. Você também pode querer migrar uma organização para um novo datastore com mais capacidade de armazenamento ou que usa uma tecnologia de armazenamento mais recente, como o VMware vSAN.

Importante A migração de armazenamento tenant é uma operação de uso intensivo de recursos que pode ser executada por um longo período, especialmente quando há a migração de muitos ativos. Para obter mais informações sobre como migrar o armazenamento de tenant, consulte <https://kb.vmware.com/kb/2151086>.

Pré-requisitos

- Determine as políticas de armazenamento usadas pelos VDCs de organizações de destino. Consulte [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#).
- Para cada política de armazenamento que contém um datastore de origem que você deseja migrar, verifique se há pelo menos um datastore de destino para o qual migrar. Você pode criar datastores de destino ou usar datastores existentes. Para obter mais informações sobre como determinar os datastores nas políticas de armazenamento usadas pelas organizações de destino, consulte a documentação do *Armazenamento do vSphere*.

Procedimentos

- 1 Faça login no VMware Cloud Director Service Provider Admin Portal como um **administrador do sistema** ou com uma função que tenha o direito **Organização: Migrar Armazenamento de Tenant**.
- 2 Inicie o assistente para **Migrar Armazenamento de Tenant**.
 - Em **Recursos de Nuvem**, selecione **Organizações** e clique em **Migrar Armazenamento de Tenant**.
 - Em **Recursos do vSphere**, selecione **Datastores** e clique em **Migrar Armazenamento de Tenant**.
- 3 Selecione uma ou mais organizações com itens de armazenamento que você deseja migrar e clique em **Avançar**.
- 4 Selecione um ou mais datastores a serem migrados e clique em **Avançar**.

O assistente lista todos os datastores no sistema.
- 5 Selecione um ou mais datastores de destino e clique em **Avançar**.
- 6 Revise a página **Pronto para ser Concluído** e clique em **Concluir** para iniciar a migração.

Gerenciar cotas sobre o consumo de recursos de uma organização

É possível gerenciar o limite geral de consumo de recursos de uma organização. Você pode adicionar, editar e remover cotas da organização sobre VMs, clusters do Tanzu Kubernetes, CPU, memória ou armazenamento.

Para obter informações sobre como limitar os recursos disponíveis para usuários ou grupos, consulte [Gerenciar as cotas de recursos de um usuário](#) ou [Gerenciar as cotas de recursos de um grupo](#).

Pré-requisitos

[Criar uma organização](#)

Procedimentos

1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

2 No painel esquerdo, selecione **Organizações**.

3 Selecione o nome da organização para a qual você deseja impor uma cota.

4 Na seção **Configurar**, selecione **Cotas**.

Organizações não têm cotas por padrão.

5 Clique em **Editar**.

6 Modifique a cota da organização selecionada.

Você pode adicionar, editar ou remover cotas sobre o número de clusters do Tanzu Kubernetes, todas as VMs ou as VMs em execução na organização, bem como consumo de CPU, memória e armazenamento. Selecione **Sem Limites** se quiser que a organização tenha recursos ilimitados do tipo selecionado.

7 Clique em **Salvar**.

Gerenciamento de centros de dados virtuais da organização

6

Para fornecer recursos para uma organização, crie um ou mais centros de dados virtuais (VDCs) de organização para esta organização. Depois de criar um VDC de organização, você pode modificar suas propriedades, desativá-la ou excluí-la e gerenciar seu modelo de alocação, armazenamento e configurações de rede.

Este capítulo inclui os seguintes tópicos:

- [Noções básicas sobre modelos de alocação](#)
- [Compreendendo políticas de dimensionamento e posicionamento de VM](#)
- [Usando o Kubernetes com o VMware Cloud Director](#)
- [Criar um centro de dados virtual da organização](#)
- [Ativar ou desativar um centro de dados virtual da organização](#)
- [Excluir um centro de dados virtual da organização](#)
- [Gerenciando modelos de centro de dados virtual](#)
- [Modificar o nome e a descrição de um centro de dados virtual da organização](#)
- [Modificar as configurações do modelo de alocação de um centro de dados virtual da organização](#)
- [Modificação das configurações de armazenamento de um centro de dados virtual de organização](#)
- [Editar as configurações de rede de um data center virtual de organização](#)
- [Configurando a rede do centro de dados virtual cruzada](#)
- [Modificar os metadados de um centro de dados virtual da organização](#)
- [Visualizar os pools de recursos de um centro de dados virtual de organização](#)
- [Gerenciamento do firewall distribuído em um centro de dados virtual da organização](#)

Noções básicas sobre modelos de alocação

Um modelo de alocação determina como e quando os recursos alocados de processamento e memória do centro de dados virtual (VDC) de provedor são comprometidos ao VDC de organização.

A tabela a seguir mostra as configurações de distribuição de recursos do vSphere na VM ou no nível do pool de recursos com base no modelo de alocação do VDC de organização.

	Modelo de alocação flexível	Modelo de pool de alocações elástico	Modelo de pool de alocações não elástico	Modelo pago pelo uso	Modelo de pool de reservas
Elástico	Com base na configuração do VDC de organização.	Sim	Não	Sim	Não
Velocidade da vCPU	Se um limite de CPUs de VM não estiver definido em uma política de dimensionamento de VM, a velocidade da vCPU poderá afetar o limite de CPUs de VM no VDC.	Afeta o número de vCPUs em execução no VDC de organização.	Não aplicável	Afeta o limite de CPUs de VM	Não aplicável
Limite de CPUs do pool de recursos	Limite de CPUs do VDC de organização distribuído com base no número de VMs no pool de recursos.	Alocação de CPUs do VDC de organização	Alocação de CPUs do VDC de organização	Ilimitado	Alocação de CPUs do VDC de organização
Reserva de CPUs do pool de recursos	A reserva de CPU do VDC de organização é distribuída com base no número de vCPUs no pool de recursos. A reserva de CPUs do VDC de organização é igual à alocação de CPUs do VDC de organização vezes a garantia de CPUs.	Soma de VMs ativadas e igual à garantia de CPUs vezes a velocidade de vCPU, vezes o número de vCPUs.	Alocação de CPUs do VDC de organização vezes garantia de CPUs	Nenhum, expansível	Alocação de CPUs do VDC de organização
Limite de memória do pool de recursos	O limite de memória do VDC de organização é distribuído com base no número de VMs no pool de recursos.	Ilimitado	Alocação de RAM do VDC de organização	Ilimitado	Alocação de RAM do VDC de organização
Reserva de memória do pool de recursos	A reserva de RAM do VDC de organização é distribuída com base no número de VMs no pool de recursos. A reserva de RAM do VDC de organização é igual à alocação de RAM do VDC de organização vezes a garantia de RAM.	Soma da garantia de RAM vezes a vRAM de todas as VMs ligadas no pool de recursos. A reserva de RAM do pool de recursos é expansível.	Alocação de RAM do VDC de organização vezes garantia de RAM	Nenhum, expansível	Alocação de RAM do VDC de organização
Limite de CPUs da VM	Com base na política de dimensionamento de VM da VM.	Ilimitado	Ilimitado	Velocidade da vCPU vezes número de vCPUs	Personalizado

	Modelo de alocação flexível	Modelo de pool de alocações elástico	Modelo de pool de alocações não elástico	Modelo pago pelo uso	Modelo de pool de reservas
Reserva de CPUs de VM	Com base na política de dimensionamento de VM da VM.	0	0	Igual à velocidade da CPU vezes a velocidade da vCPU, vezes o número de vCPUs.	Personalizado
Limite de RAM da VM	Com base na política de dimensionamento de VM da VM.	Ilimitado	Ilimitado	vRAM	Personalizado
Reserva de RAM da VM	Com base na política de dimensionamento de VM da VM.	0	É igual a vRAM vezes a garantia de RAM mais a sobrecarga de RAM.	É igual a vRAM vezes a garantia de RAM mais a sobrecarga de RAM.	Personalizado

Convertendo um modelo de alocação de VDC herdado em um modelo de alocação flexível

Você adiciona uma política de posicionamento de VM e uma política de dimensionamento de VM a um VDC com um modelo de pool de alocações elástico, um modelo de pool de alocações não elástico, um modelo de pagamento conforme o uso ou um modelo de pool de reservas. Se a política de posicionamento ou dimensionamento de VM não for compatível com o modelo de alocação de VDC existente, você poderá optar por converter o VDC em um VDC de organização flexível.

Conformidade de políticas de VM

A conversão do VDC herdado não causa falta de conformidade com a VM. Se um administrador alterar os valores de processamento de VM ou a associação de grupo de VMs de uma VM diretamente na instância do vCenter Server, uma VM poderá se tornar não compatível com a política de posicionamento ou dimensionamento de VM atribuída. Uma VM também poderá se tornar não compatível se um usuário com os privilégios necessários alterar a reserva da VM e limitar os valores usando a API do vCloud. Se houver uma VM não compatível, a interface de usuário do VMware Cloud Director Tenant Portal exibirá uma mensagem de aviso. O tenant pode ver informações detalhadas sobre a causa da não conformidade e pode tornar a VM compatível novamente, o que reaplicará as políticas à VM.

Uso sugerido dos modelos de alocação

Cada modelo de alocação pode ser usado para diferentes níveis de controle e gerenciamento de desempenho.

A tabela a seguir contém informações sobre o uso sugerido de cada modelo de alocação.

Modelo de alocação	Uso sugerido
Modelo de alocação flexível	Com o modelo de alocação flexível, você pode alcançar um controle preciso do desempenho no nível da carga de trabalho. Ao utilizar o modelo de alocação flexível, os administradores de sistema do VMware Cloud Director podem gerenciar a elasticidade de VDCs de organização individuais. O modelo de alocação flexível usa o gerenciamento baseado em políticas de cargas de trabalho. Com o modelo de alocação flexível, os provedores de nuvem têm mais controle sobre a sobrecarga de memória em um VDC de organização e podem aplicar um uso de capacidade intermitente estrito para tenants.
Modelo de alocação do pool de alocação	Use o modelo de alocação do pool de alocação para cargas de trabalho de longa duração, em que os tenants se inscrevem para o consumo de recursos de processamento fixos e onde os provedores de nuvem podem prever e gerenciar a capacidade dos recursos de processamento. O modelo de alocação do pool de alocações é ideal para cargas de trabalho com requisitos de desempenho diversificados. Com o modelo de alocação do pool de alocações, todas as cargas de trabalho compartilham os recursos alocados dos pools de recursos do vCenter Server. Independentemente disso, se você ativar ou desativar a elasticidade, os tenants receberão uma quantidade limitada de recursos de cálculo. Com o modelo de alocação do pool de alocações, os provedores de nuvem ativam ou desativam a elasticidade no nível do sistema, e a configuração se aplica a todos os VDCs de organização do pool de alocações. Se você usar a alocação do pool de alocações não elástico, o VDC de organização reservará previamente o pool de recursos do VDC, e os tenants poderão comprometer vCPUs em excesso, mas não poderão fazer o mesmo com a memória. Se você usar a alocação de pool elástica, o VDC de organização não reservará previamente nenhum recurso de cálculo, e a capacidade poderá abranger vários clusters. Os provedores de nuvem gerenciam o excesso de comprometimento de recursos físicos de processamento, e os tenants não podem exceder o comprometimento de vCPUs e memória.
Pago pelo uso	Use o modelo pago pelo uso quando você não precisar alocar recursos de cálculo no vCenter Server antecipadamente. A reserva, o limite e os compartilhamentos são aplicados em cada carga de trabalho que os tenants implantam no VDC. Com o modelo de alocação pago pelo uso, cada carga de trabalho no VDC de organização recebe a mesma porcentagem dos recursos de cálculo configurados reservados. Para o VMware Cloud Director, considere que a velocidade da CPU de cada vCPU para cada carga de trabalho é a mesma, e você só pode definir a velocidade da CPU no nível do VDC de organização. Do ponto de vista do desempenho, como não é possível alterar as configurações de reserva de cargas de trabalho individuais, cada carga de trabalho recebe a mesma preferência. O modelo de alocação pago pelo uso é ideal para tenants que precisam de cargas de trabalho com diferentes requisitos de desempenho em execução no mesmo VDC de organização. Devido à elasticidade, o modelo pago pelo uso é adequado para cargas de trabalho genéricas e de vida útil curta que fazem parte de aplicativos com dimensionamento automático. Com o modelo pago pelo uso, os tenants podem corresponder picos na demanda por recursos de cálculo em um VDC de organização.
Pool de reservas	Use o modelo de alocação do pool de reservas quando precisar de um controle detalhado sobre o desempenho de cargas de trabalho em execução no VDC da organização. Sob a perspectiva do provedor de nuvem , o modelo de alocação do pool de reservas requer uma alocação antecipada de todos os recursos de processamento no vCenter Server. O modelo de alocação do pool de reservas não é elástico. O modelo de alocação do pool de reservas é ideal para cargas de trabalho que são executadas em um hardware dedicado a um tenant específico. Nesses casos, os usuários do tenant podem gerenciar o uso e o excesso de comprometimento dos recursos de cálculo.

Modelo de alocação flexível

A partir do VMware Cloud Director 9.7, **administradores de sistema** podem criar centros de dados virtuais (VDC) de organização usando o modelo de alocação flexível. Com a combinação

de distribuição flexível e políticas de dimensionamento de VM, os **administradores de sistema** podem controlar o consumo de CPU e RAM no VDC e os níveis de máquina virtual (VM) individuais. O modelo de alocação flexível oferece suporte a todas as configurações de alocação disponíveis nos modelos de alocação existentes.

No VMware Cloud Director 10.0 e versões posteriores, todos os VDCs de organização não flexíveis podem ser convertidos em VDCs flexíveis.

Ao criar um VDC de organização flexível, os **administradores do sistema** controlam os seguintes parâmetros do VDC de organização:

Parâmetro	Descrição
Elasticity	Ative ou desative o recurso de pool elástico.
Include VM Memory Overhead	Incluir ou excluir a sobrecarga de memória neste VDC. Quando definido como "true", talvez você não consiga usar a capacidade total do VDC, pois a sobrecarga de memória de cada VM ligada também é obtida da capacidade disponível do VDC. Quando definido como "false", a sobrecarga de memória é obtida do VDC de provedor e não da capacidade alocada do VDC.
CPU allocation	A quantidade de CPU alocada a esse VDC em MHz ou GHz. A alocação de CPU define a capacidade de CPU do VDC. A CPU total usada por todas as VMs em execução no VDC não pode exceder esse valor.
CPU limit	O limite de CPU define a quota de CPU de um VDC. Na maioria dos casos, o limite de CPU é igual à capacidade alocada da CPU do VDC. Às vezes, pode ser necessário não alocar uma CPU ao VDC, como no modelo de pagamento conforme o uso. Nesse caso, você deve definir uma cota para o consumo de CPU geral definindo a alocação de CPU como zero e o limite de CPU como um valor diferente de zero. Você também pode usar essa configuração para permitir uma cota de CPU ilimitada. Se definida como ilimitada, os pools de recursos de suporte do VDC no vCenter Server receberão CPUs ilimitadas.
CPU resources guaranteed	A porcentagem de alocação de CPU que é reservada fisicamente para o VDC.
vCPU speed	A velocidade padrão do vCPU para VMs no VDC.
Memory allocation	A quantidade de memória alocada para esse VDC em MB ou GB. Esse parâmetro define a capacidade total de memória do VDC. O total de memória configurada por todas as VMs em execução no VDC não pode exceder esse valor.
Memory resources guaranteed	A porcentagem de alocação de memória reservada fisicamente para o VDC.
Maximum number of VMs	O número máximo de VMs no VDC.

Como **administrador de sistema do VMware Cloud Director**, você pode configurar um VDC de organização flexível para ser elástico ou não. Quando os VDCs de organização flexíveis têm o recurso de pool elástico habilitado, o VDC da organização expande e usa todos os pools de recursos associados ao VDC do seu provedor. No VMware Cloud Director 9.7, se você converter um VDC de organização não elástico em um VDC de organização elástico, não poderá converter o mesmo VDC de organização novamente em um não elástico.

O modelo de alocação flexível oferece suporte aos recursos das políticas de dimensionamento de VM sem nenhuma das restrições que os outros modelos de alocação apresentam. No modelo de alocação flexível, a alocação de recursos de processamento de VM depende das políticas de dimensionamento de VM. Se você não definir uma política de dimensionamento de VM para um VDC de organização, a alocação de recursos de cálculo dependerá do modelo de alocação do VDC de organização. Usando a combinação do modelo de alocação flexível e as políticas de dimensionamento de VM de organização, um único VDC de organização pode acomodar VMs que usam a configuração comum a todos os outros modelos de alocação. Para obter mais informações, consulte [Compreendendo políticas de dimensionamento e posicionamento de VM](#).

Para criar um VDC de organização flexível, você pode usar o VMware Cloud Director Service Provider Admin Portal ou o vCloud API. Para obter informações sobre a API do vCloud, consulte *Guia de programação da API do VMware Cloud Director*.

Modelo de alocação do pool de alocação

Com o modelo de alocação do pool de alocações, uma porcentagem dos recursos alocados do VDC (centro de dados virtual) de provedor é comprometida ao VDC de organização. Você pode especificar a porcentagem para CPU e memória. Essa porcentagem é conhecida como o fator de garantia percentual e permite o excesso de comprometimento de recursos.

Como administrador do sistema, você pode configurar VDCs de organização do pool de alocações para serem elásticos ou não elásticos. A elasticidade é uma configuração global que afeta todos os VDCs de organização de pool de alocações. Consulte [Modificar as configurações gerais do sistema](#).

Por padrão, os VDCs de organização de pool de alocações têm um pool de alocações elástico habilitado. Os sistemas atualizados do VMware Cloud Director 5.1 que têm VDCs de organização de pool de alocações com máquinas virtuais abrangendo vários pools de recursos têm um pool de alocações elástico habilitado por padrão.

Quando os VDCs de pool de alocações têm o recurso de pool de alocações elástico habilitado, o VDC de organização abrange e usa todos os pools de recursos associados ao VDC de provedor. Como resultado, a frequência de vCPU é agora um parâmetro obrigatório para um pool de alocação.

Defina a frequência de vCPU e o fator de garantia percentual de tal forma que máquinas virtuais suficientes possam ser implantadas no VDC da organização sem que a CPU seja um fator de gargalo.

Quando uma máquina virtual é criada, o mecanismo de posicionamento a coloca no pool de recursos do VDC de provedor que melhor se adapta aos requisitos da máquina virtual. Um pool de sub-recursos é criado para esse VDC de organização sob o pool de recursos do VDC de provedor, e a máquina virtual é colocada sob esse pool de sub-recursos.

Quando a máquina virtual é ligada, o mecanismo de posicionamento verifica o pool de recursos do VDC de provedor para garantir se ele ainda pode ligar a máquina virtual. Em caso negativo, o mecanismo de posicionamento move a máquina virtual para um pool de recursos de VDC de provedor com recursos suficientes para executar a máquina virtual. Um pool de sub-recursos do VDC de organização será criado se ainda não houver um.

O pool de sub-recursos é configurado com recursos suficientes para executar a nova máquina virtual. A reserva de memória do pool de sub-recursos é aumentada pelo tamanho de memória configurado da máquina virtual vezes o fator de garantia percentual para o VDC de organização. A reserva de CPU do pool de sub-recursos é aumentada pelo número de vCPUs configuradas para a máquina virtual vezes a vCPU especificada no nível de VDC de organização vezes o fator de garantia percentual para a CPU definido no nível de VDC de organização. Se o recurso de pool de alocações elástico estiver habilitado, o limite de memória do pool de sub-recursos será aumentado pelo tamanho da memória configurado da máquina virtual e do limite de CPU do pool de sub-recursos será aumentado pelo número de vCPUs com as quais a máquina virtual está configurada vezes a frequência de vCPU especificada no nível de VDC de organização. A máquina virtual é reconfigurada para definir sua memória e reserva de CPU como zero, e o mecanismo de posicionamento de máquina virtual coloca a máquina virtual em um pool de recursos de VDC de provedor.

Com o modelo de alocação de pool de alocações elástico, os limites são monitorados e gerenciados somente pelo VMware Cloud Director. Se o recurso elástico estiver desativado, o limite do pool de recursos será definido corretamente.

Os benefícios do modelo de pool de alocação são que uma máquina virtual pode tirar proveito dos recursos de uma máquina virtual ociosa no mesmo pool de sub-recursos. Esse modelo pode aproveitar os novos recursos adicionados ao VDC de provedor.

Em casos raros, uma máquina virtual é comutada do pool de recursos ao qual foi atribuída na criação a um pool de recursos diferente na ocasião da ativação devido à falta de recursos no pool de recursos original. Essa alteração pode envolver um custo secundário para mover os arquivos de disco da máquina virtual para um novo pool de recursos.

Quando o recurso pool de alocações elástico está desativado, o comportamento dos VDCs de organização de pool de alocações é semelhante ao modelo do pool de alocações no VMware Cloud Director 1.5. Nesse modelo, a frequência da vCPU não é configurável. O excesso de comprometimento é controlado pela definição da porcentagem de recursos garantidos.

Por padrão, em um VDC de pool de alocações, as máquinas virtuais obtêm as configurações de reserva, limite e compartilhamentos das configurações do VDC. Para criar ou reconfigurar uma máquina virtual com configurações de alocação de recursos personalizadas para CPU e memória, você pode usar a API do vCloud. Consulte *Guia de programação da API do VMware Cloud Director*.

Modelo de alocação Pago pelo Uso

Com o modelo de alocação Pago pelo Uso, os recursos são confirmados somente quando os usuários criam vApps no VDC da organização. Você pode especificar uma porcentagem de

recursos para garantir, o que permite que você comprometa recursos em excesso. Você pode tornar um VDC de organização pago pelo uso elástico adicionando vários pools de recursos ao seu VDC de provedor.

Os recursos confirmados com a organização são aplicados no nível da máquina virtual.

Quando uma máquina virtual está ligada, se o pool de recursos original não puder acomodar a máquina virtual, o mecanismo de posicionamento verificará o pool de recursos e atribuirá a máquina virtual a outro pool de recursos. Se um pool de sub-recursos não estiver disponível para o pool de recursos, o VMware Cloud Director criará um com um limite infinito e uma taxa zero. A taxa da máquina virtual é definida como seu limite vezes seus recursos confirmados, e o mecanismo de posicionamento de máquina virtual coloca a máquina virtual em um pool de recursos de VDC de provedor.

O benefício do modelo pago pelo uso é que ele pode tirar proveito dos novos recursos adicionados ao VDC de provedor.

Em casos raros, uma máquina virtual é comutada do pool de recursos ao qual foi atribuída na criação a um pool de recursos diferente na ocasião da ativação devido à falta de recursos no pool de recursos original. Essa alteração pode envolver um custo secundário para mover os arquivos de disco da máquina virtual para um novo pool de recursos.

No modelo pago pelo uso, nenhum recurso é reservado antes do tempo e, portanto, uma máquina virtual pode falhar ao ligar se não houver recursos suficientes. As máquinas virtuais operando esse modelo não podem tirar proveito dos recursos de máquinas virtuais ociosas no mesmo pool de sub-recursos, porque os recursos são definidos no nível da máquina virtual.

Por padrão, em um VDC pago pelo uso, máquinas virtuais obtêm suas configurações de reserva, limite e compartilhamentos das configurações do VDC. Para criar ou reconfigurar uma máquina virtual com configurações de alocação de recursos personalizadas para CPU e memória, você pode usar a API do vCloud. Consulte *Guia de programação da API do VMware Cloud Director*.

Modelo de alocação de pool de reserva

Com o modelo de alocação de pool de reserva, todos os recursos que você aloca são imediatamente confirmados no VDC da organização. Os usuários da organização podem controlar o excesso de comprometimento especificando as configurações de reserva, limite e prioridade para máquinas virtuais individuais.

Como apenas um pool de recursos e um pool de sub-recursos estão disponíveis nesse modelo, o mecanismo de posicionamento não reatribui o pool de recursos de uma máquina virtual quando ela é ligada. A taxa e o limite da máquina virtual não são modificados.

Com o modelo de pool de reservas, as fontes estão sempre disponíveis quando necessárias. Esse modelo também oferece controle sobre a taxa de máquinas virtuais, limites e compartilhamentos, o que pode levar ao uso ideal dos recursos reservados se você planejar com cuidado. Para obter informações sobre como definir as configurações de alocação de recursos de máquina virtual em VDCs de pool de reserva, consulte o *vCloud Air - Guia do Usuário do Virtual Private Cloud OnDemand*.

Nesse modelo, a reserva é sempre feita no cluster primário. Se recursos suficientes não estiverem disponíveis para criar um VDC de organização no cluster primário, a criação do VDC falhará.

Outras limitações desse modelo são que ele não é elástico e os usuários da organização podem definir compartilhamentos, taxas e limites não ideais em máquinas virtuais, levando ao subuso de recursos.

Compreendendo políticas de dimensionamento e posicionamento de VM

Você pode controlar a alocação e o posicionamento de recursos de máquina virtual (VM) em um cluster ou host específico usando políticas de dimensionamento ou posicionamento de VM.

Os **administradores do sistema** do VMware Cloud Director criam e gerenciam políticas de dimensionamento de VM em um nível global e podem publicar políticas individuais em um ou mais VDCs de organização. Para o VMware Cloud Director 10.2.1 e versões anteriores, você pode criar e gerenciar políticas de posicionamento de VM para cada VDC de provedor separadamente, pois uma política de posicionamento de VM tem escopo no nível do VDC do provedor. No VMware Cloud Director 10.2.2, é possível incluir mais de um VDC do provedor no escopo de uma política de posicionamento de VM. Além disso, na versão 10.2.2, se um usuário salvar um vApp como um modelo de vApp em um catálogo, o modelo incluirá também as políticas de posicionamento e dimensionamento do vApp original como políticas marcadas não modificadas.

Quando você publica uma política em um VDC de organização, essa política fica disponível para os usuários na organização. Ao criar e gerenciar máquinas virtuais no VDC de organização, os tenants podem atribuir as políticas disponíveis a essas máquinas virtuais. Tenants e usuários no VDC de organização não podem analisar a configuração específica de uma política de posicionamento ou dimensionamento de VM.

As políticas de posicionamento e dimensionamento de VM são um mecanismo para que os provedores de nuvem definam e ofereçam níveis diferenciados de serviço, por exemplo, um perfil de uso intenso de CPU ou um perfil de alto uso de memória. Se você publicar várias políticas de posicionamento e dimensionamento de VM em um VDC de organização, os usuários do tenant poderão selecionar entre todas as políticas personalizadas e a política padrão ao criar e gerenciar VMs no VDC de organização. A política padrão do sistema é gerada automaticamente para cada VDC. Você pode excluir a política padrão do sistema no VDC e marcar outra política personalizada como a padrão. A política padrão não define nenhum valor e permite todas as configurações de máquina virtual.

Política de posicionamento de VM

Uma política de posicionamento de VM define o posicionamento de uma máquina virtual em um host ou grupo de hosts. É um mecanismo para **administradores de provedores de nuvem** criarem um grupo nomeado de hosts dentro de um VDC de provedor. O grupo nomeado de hosts é um subconjunto de hosts nos clusters do VDC de provedor que podem ser selecionados com base em qualquer critério, como camada de desempenho ou

licenciamento. No VMware Cloud Director 10.2.2, é possível expandir o escopo de uma política de posicionamento de VM para mais de um VDC do provedor.

Uma política de posicionamento de provedor define regras de afinidade de VM/host que afetam diretamente o posicionamento das cargas de trabalho do tenant. Os administradores do definem ou expõem grupos de hosts nomeados usando grupos de VMs no vCenter Server. Um grupo de VMs tem afinidade direta com um grupo de hosts e representa o grupo de hosts com o qual ele tem a afinidade.

Você define a política de posicionamento de VM no nível do VDC de provedor. Uma política de posicionamento de VM inclui os seguintes atributos:

- Nome (deve ser exclusivo no VDC de provedor)
- Descrição
- Um conjunto de um ou mais grupos de VMs selecionados dos clusters subjacentes no VDC de provedor. Você pode selecionar um grupo de VMs por cluster

Uma política de posicionamento de VM é opcional durante a criação de uma máquina virtual, e um tenant pode atribuir apenas uma política de posicionamento de VM a uma máquina virtual.

Quando um tenant cria uma máquina virtual no VDC da organização e seleciona a política de posicionamento de VM, o VMware Cloud Director adiciona a máquina virtual a um ou mais dos grupos de VMs referenciados nessa política. Como resultado, o VMware Cloud Director cria a máquina virtual no host apropriado.

Uma política de posicionamento de VM pode ter zero ou um grupo de VMs de cada cluster. Por exemplo, a política de posicionamento de VM *oracle_license* pode incluir os grupos de VMs *oracle_license1* e *oracle_license2*, em que o grupo de VMs *oracle_license1* pertence ao cluster *oracle_cluster1* e o grupo de VMs *oracle_license2* pertence ao cluster *oracle_cluster2*.

Quando você atribui uma política de posicionamento de VM a uma máquina virtual, o mecanismo de posicionamento adiciona essa máquina virtual ao grupo de VMs correspondente do cluster no qual ela reside. Por exemplo, se você optar por implantar uma máquina virtual no cluster *oracle_cluster1* e atribuir a política de posicionamento de VM *oracle_license* a essa máquina virtual, o mecanismo de posicionamento adicionará a máquina virtual ao grupo de VMs *oracle_license1*.

Política de dimensionamento de VM

Uma política de dimensionamento de VM define a alocação de recursos de processamento para máquinas virtuais em um VDC de organização. A alocação de recursos de cálculo inclui a alocação de CPU e memória, reservas, limites e compartilhamentos.

Com políticas de dimensionamento de VM, os **administradores de sistema** do VMware Cloud Director podem controlar os seguintes aspectos do consumo de recursos de processamento no nível da máquina virtual:

- Número de vCPUs e velocidade de relógio das vCPUs
- Quantidade de memória alocada à máquina virtual

- Reserva de memória e CPU, limite e compartilhamentos
- Configurações extras.

O parâmetro da API do `extraConfigs` representa um mapeamento entre pares de chave e valor que são aplicados como valores de configuração extras em uma máquina virtual. Você pode criar uma política com configurações extras somente usando a API do vCloud. As configurações extras existentes aparecem na interface de usuário do Service Provider Admin Portal em **Configurações Extras** na exibição da política de dimensionamento de VM detalhada.

Você define as políticas de dimensionamento de VM em nível global. Para obter mais informações sobre os atributos de políticas de dimensionamento de VM, consulte [Atributos das políticas de dimensionamento de VM](#).

O VMware Cloud Director gera uma política de dimensionamento de VM padrão para todos os VDCs. A política de dimensionamento de VM padrão contém apenas um nome e uma descrição, e todos os atributos de política restantes estão vazios.

Você também pode definir outra política de dimensionamento de VM como a política padrão para um VDC de organização. A política de dimensionamento de VM padrão controla a alocação de recursos e o consumo das máquinas virtuais que os tenants criam no VDC de organização, a menos que um tenant atribua outra política de dimensionamento de VM específica à máquina virtual.

Para limitar os recursos máximos de processamento que os tenants podem alocar a máquinas virtuais individuais em um VDC de organização, os provedores de nuvem podem definir uma política de dimensionamento de VM máxima. Quando atribuída a um VDC de organização, a política de dimensionamento de VM máxima atua como um limite superior para a configuração de recursos de processamento para todas as máquinas virtuais no VDC de organização. A política de dimensionamento de VM máxima não está disponível para os usuários do tenant ao criar uma máquina virtual. Quando você define uma política de dimensionamento de VM como a política máxima, o VMware Cloud Director copia internamente o conteúdo dessa política e usa o conteúdo copiado como a política de dimensionamento de VM máxima. Como resultado, o VDC de organização não depende da política de dimensionamento de VM usada inicialmente.

Usando políticas de dimensionamento de VM, os provedores de nuvem podem restringir o consumo de recursos de processamento para todas as máquinas virtuais em um VDC de organização para, por exemplo, três tamanhos predefinidos, como *Tamanho Pequeno*, *Tamanho Médio* e *Tamanho Grande*. O fluxo de trabalho é o seguinte.

- 1 Um **administrador do sistema** cria três políticas de dimensionamento de VM com os seguintes atributos.

Nome	Atributos
Tamanho Pequeno	<ul style="list-style-type: none"> ■ Descrição: política de VM de tamanho pequeno ■ Nome: Tamanho Pequeno ■ Memória: 1024 ■ Número de vCPUs: 1
Tamanho Médio	<ul style="list-style-type: none"> ■ Descrição: política de VM de tamanho médio ■ Nome: Tamanho Médio ■ Memória: 2048 ■ Número de vCPUs: 2
Tamanho Grande	<ul style="list-style-type: none"> ■ Descrição: política de VM de tamanho grande ■ Nome: Tamanho Grande ■ Memória: 4096 ■ Número de vCPUs: 4

- 2 Publique as novas políticas de dimensionamento de VM em um VDC de organização.
- 3 Opcionalmente, defina uma das políticas de dimensionamento de VM como uma política de dimensionamento de VM padrão para o VDC de organização.

Estas são as operações de política disponíveis para provedores de nuvem:

- Para definir o posicionamento de uma máquina virtual em um host ou grupo de hosts, crie uma política de posicionamento. Consulte [Criar uma política de posicionamento de VM em um VDC do provedor](#).
- Para controlar a alocação de recursos de processamento física para cargas de trabalho do tenant, crie uma política de dimensionamento. Consulte [Criar uma política de dimensionamento de VM](#).
- Publique uma política de posicionamento ou dimensionamento de VM em um ou mais VDCs de organização. Consulte [Adicionar uma política de posicionamento de VM a um VDC de organização](#).
- Defina uma política de posicionamento ou dimensionamento de VM como padrão.
- Edite uma política de posicionamento de VM e uma política de dimensionamento de VM. Você só pode editar o nome e a descrição da política na interface de usuário do VMware Cloud Director.
- Cancele a publicação de uma política de posicionamento ou dimensionamento de VM de um VDC de organização.

- Exclua uma política de posicionamento ou dimensionamento de VM. Consulte [Excluir uma política de posicionamento de VM](#) e [Excluir uma política de dimensionamento de VM](#).

Os usuários que têm o direito **ORG_VDC_MANAGE_COMPUTE_POLICIES** podem criar, atualizar e publicar políticas de posicionamento ou dimensionamento de VM.

A tabela a seguir lista as operações de políticas de posicionamento e dimensionamento de VM disponíveis para usuários do tenant.

Tabela 6-1. Operações de políticas de posicionamento e dimensionamento de VM para usuários do tenant

Operação	Descrição
Atribua uma política a uma máquina virtual durante a criação da máquina virtual.	<p>Os usuários de tenant que estão autorizados a criar máquinas virtuais em um VDC de organização podem opcionalmente atribuir políticas de posicionamento e dimensionamento de VM a essas máquinas virtuais usando o VMware Cloud Director Tenant Portal. Como resultado, os parâmetros definidos na política de dimensionamento de VM controlam o consumo de CPU e de memória da máquina virtual. Atribuir uma política de posicionamento ou dimensionamento de VM não é um requisito para tenants durante a criação de uma máquina virtual. Se um tenant não selecionar explicitamente uma política de dimensionamento de VM para atribuir a uma máquina virtual, o dimensionamento de VM padrão será aplicado à máquina virtual.</p> <p>Se você não criar uma política de posicionamento de VM, a opção de política de posicionamento de VM não será visível para os tenants. Se o tenant selecionar uma política de posicionamento com informações de dimensionamento, a opção de política de dimensionamento de VM se tornará oculta para esse tenant. Você pode criar uma política de posicionamento de VM com informações de dimensionamento somente usando a API do vCloud.</p> <p>Se houver apenas uma política de dimensionamento de VM, a opção de política de dimensionamento de VM não será visível para os tenants.</p> <p>Quando o administrador do sistema define os atributos Contagem de vCPU, Núcleos por soquete e Memória em uma política de dimensionamento de VM, se um tenant selecionar essa política, esses valores serão exibidos, mas não serão editáveis.</p>
Atribua uma política a uma máquina virtual existente.	<p>Os usuários do tenant com autorização para gerenciar máquinas virtuais em um VDC de organização podem atribuir ou alterar as políticas de posicionamento e dimensionamento de VM de uma máquina virtual existente usando o VMware Cloud Director Tenant Portal. Quando um tenant altera a política de posicionamento de VM, a máquina virtual é movida para um novo host, de acordo com a regra de afinidade de VM-host definida na nova política de posicionamento de VM. Quando um tenant altera uma política de dimensionamento de VM, o sistema reconfigura a máquina virtual para consumir recursos de processamento, conforme especificado na nova política de dimensionamento de VM.</p>

O fluxo de trabalho para políticas de posicionamento e dimensionamento de VM é o seguinte.

- 1 Um **administrador do sistema** cria uma ou mais políticas de posicionamento de VM. Consulte [Criar uma política de posicionamento de VM em um VDC do provedor](#).
- 2 Um **administrador do sistema** cria uma ou mais políticas de dimensionamento de VM. Consulte [Criar uma política de dimensionamento de VM](#).

O nome de uma política de dimensionamento de VM é exclusivo em um único site do VMware Cloud Director. O nome de uma política de posicionamento de VM é exclusivo dentro do escopo do VDC de provedor da política.

- 3 Um **administrador do sistema** publica as políticas de posicionamento e dimensionamento de VM em um ou mais VDCs de organização. Consulte [Adicionar uma política de posicionamento de VM a um VDC de organização](#).

A publicação de uma política de posicionamento de VM a disponibiliza para os usuários do tenant em VDCs de organização durante a criação e a edição da máquina virtual.

- 4 Ao criar ou atualizar uma máquina virtual, os tenants podem usar a API do vCloud ou o VMware Cloud Director Tenant Portal para atribuir uma política de posicionamento e de dimensionamento de VM a uma máquina virtual.

Criar uma política de posicionamento de VM em um VDC do provedor

Uma política de posicionamento de VM é uma política de processamento de VDC que contém uma referência a uma política de VDC de provedor. No VMware Cloud Director 10.2.2, é possível adicionar vários VDCs do provedor ao escopo de uma política de posicionamento de VM. Você pode usar uma política de posicionamento de VM para definir o posicionamento de uma VM em um host específico, um grupo de hosts ou um cluster.

Começando com o VMware Cloud Director 10.2.2, uma política de posicionamento de VM pode conter uma referência a uma ou mais políticas de VDC do provedor. Ao criar uma política de posicionamento a partir de um VDC do provedor, essa política faz referência apenas ao VDC do provedor selecionado. Você pode incluir mais VDCs do provedor no escopo de uma política de posicionamento de VM editando essa política ou pode criar uma política de posicionamento na guia **Políticas de Posicionamento de VM** para incluir mais de um VDC do provedor no seu escopo. Consulte [Editar uma política de posicionamento de VM](#) e [Criar uma política de posicionamento de VM global](#).

Pré-requisitos

- Verifique se você tem pelo menos um VDC de provedor no seu ambiente.
- Verifique se você tem pelo menos um grupo de VMs no seu ambiente.

Um grupo de VMs é um conjunto de VMs que você pode vincular a um grupo de hosts com afinidades positivas. Por meio de uma regra de afinidade positiva, você causa o posicionamento de um grupo de VMs em um host específico. Você pode criar um grupo de VMs por meio da interface de usuário do vCenter Server ou da API do VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.
- 3 Clique em um VDC de provedor na lista.

- 4 Clique na guia **Políticas de posicionamento de VM** e clique em **Novo**.
- 5 (Opcional) Na página **O que é uma política de posicionamento de VM** do assistente, marque a caixa de seleção para parar de mostrar as informações da política de posicionamento de VM.
- 6 Clique em **Avançar**.
- 7 Insira um nome para a política de posicionamento de VM e, opcionalmente, uma descrição.
- 8 Selecione os grupos de VMs ou os grupos de VMs lógicas aos quais você deseja que a VM seja vinculada e clique em **Avançar**.

Quando você seleciona mais de um grupo lógico, se um tenant aplicar essa política a uma VM, a VM se tornará membro de todos os grupos de VM incluídos nos grupos de VM lógicas selecionados. A VM é condicionada a uma combinação de todas as afinidades que se aplicam às VMs nesses grupos. Começando com o VMware Cloud Director 10.2.2, você pode selecionar simultaneamente grupos de VMs e grupos lógicos.

Você pode criar um grupo de VMs lógicas in-line selecionando um grupo de VMs por cluster. Esse grupo de VMs lógicas não tem um nome e pode ser usado apenas para a política de posicionamento de VM selecionada.

- 9 Revise as configurações de política de posicionamento de VM e clique em **Concluir**.

Próximo passo

- [Criar uma política de dimensionamento de VM](#).
- [Adicionar uma política de posicionamento de VM a um VDC de organização](#).
- Começando com o VMware Cloud Director 10.2.2, é possível [Editar uma política de posicionamento de VM](#).
- [Excluir uma política de posicionamento de VM](#).

Criar uma política de posicionamento de VM global

Começando com o VMware Cloud Director 10.2.2, uma política de posicionamento de VM pode conter uma referência a uma ou mais políticas de VDC do provedor. Você pode usar uma política de posicionamento de VM para definir o posicionamento de uma VM em um host específico, em um grupo de hosts ou em um ou mais clusters.

Ao criar uma política de posicionamento a partir de um VDC do provedor, essa política faz referência apenas ao VDC do provedor selecionado. Consulte [Criar uma política de posicionamento de VM em um VDC do provedor](#). Começando com o VMware Cloud Director 10.2.2, é possível incluir mais VDCs do provedor no escopo de uma política de posicionamento de VM editando essa política, ou você tem a opção de criar uma política de posicionamento global.

Pré-requisitos

- Verifique se você tem pelo menos um VDC de provedor no seu ambiente.
- Verifique se você tem pelo menos um grupo de VMs no seu ambiente.

Um grupo de VMs é um conjunto de VMs que você pode vincular a um grupo de hosts com afinidades positivas. Por meio de uma regra de afinidade positiva, você causa o posicionamento de um grupo de VMs em um host específico. Você pode criar um grupo de VMs por meio da interface de usuário do vCenter Server ou da API do VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Políticas de Posicionamento de VM** e clique em **Novo**.
- 3 (Opcional) Na página **O que é uma política de posicionamento de VM** do assistente, marque a caixa de seleção para parar de mostrar as informações da política de posicionamento de VM.
- 4 Clique em **Avançar**.
- 5 Insira um nome para a política de posicionamento de VM e, opcionalmente, uma descrição.
- 6 Selecione os grupos de VMs e os grupos de VMs lógicas aos quais você deseja que a VM seja vinculada e clique em **Avançar**.

É possível selecionar um grupo de VMs por cluster.

Quando você seleciona mais de um grupo lógico, se um tenant aplicar essa política a uma VM, a VM se tornará membro de todos os grupos de VM incluídos nos grupos de VM lógicas selecionados. A VM é condicionada a uma combinação de todas as afinidades que se aplicam às VMs nesses grupos. Começando com o VMware Cloud Director 10.2.2, você pode selecionar simultaneamente grupos de VMs e grupos lógicos.

Você pode criar um grupo de VMs lógicas in-line selecionando um grupo de VMs por cluster. Esse grupo de VMs lógicas não tem um nome e pode ser usado apenas para a política de posicionamento de VM selecionada.

- 7 Revise as configurações de política de posicionamento de VM e clique em **Concluir**.

Próximo passo

- [Criar uma política de dimensionamento de VM](#).
- [Adicionar uma política de posicionamento de VM a um VDC de organização](#).
- Começando com o VMware Cloud Director 10.2.2, é possível [Editar uma política de posicionamento de VM](#).
- [Excluir uma política de posicionamento de VM](#).

Editar uma política de posicionamento de VM

No VMware Cloud Director 10.2.2, é possível editar e alterar o escopo de uma política de posicionamento de VM.

Pré-requisitos

[Criar uma política de posicionamento de VM global](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Políticas de Posicionamento de VM**.
- 3 Selecione uma política de posicionamento de VM e clique em **Editar**.
- 4 (Opcional) Na página **O que é uma política de posicionamento de VM** do assistente, marque a caixa de seleção para parar de mostrar as informações da política de posicionamento de VM.
- 5 Clique em **Avançar**.
- 6 Edite o nome da política de posicionamento de VM e, opcionalmente, a descrição.
- 7 Edite os grupos de VMs e os grupos de VMs lógicas aos quais você deseja que a VM seja vinculada e clique em **Avançar**.

É possível selecionar um grupo de VMs por cluster. Não é possível desmarcar clusters em uso no momento, por exemplo, quando você publica a política de posicionamento em um VDC da organização.

- 8 Revise as configurações de política de posicionamento de VM e clique em **Concluir**.

Próximo passo

- [Criar uma política de dimensionamento de VM](#).
- [Adicionar uma política de posicionamento de VM a um VDC de organização](#).
- [Excluir uma política de posicionamento de VM](#).

Adicionar uma política de posicionamento de VM a um VDC de organização

Quando você cria uma política de posicionamento de VM, ela não é visível para os tenants. Você pode publicar uma política de posicionamento de VM em um VDC de organização para disponibilizá-la aos tenants.

Publicar uma política de posicionamento de VM em um VDC de organização torna essa política visível para tenants. No VMware Cloud Director 10.2.2 e versões posteriores, para publicar uma política de posicionamento em um VDC da organização, você deve primeiro incluir o VDC do provedor de suporte no escopo da política de posicionamento da VM, [Criar uma política de posicionamento de VM global](#) ou [Editar uma política de posicionamento de VM](#). O tenant pode selecionar a política ao criar uma nova VM autônoma ou uma VM a partir de um modelo, editar uma VM, adicionar uma VM a um vApp e criar um vApp a partir de um modelo de vApp. Não é possível excluir uma política de posicionamento de VM que está disponível para os tenants.

Pré-requisitos

- Verifique se você tem pelo menos um VDC de organização no seu ambiente. Consulte [Criar um centro de dados virtual da organização](#).

- Verifique se você tem pelo menos uma política de posicionamento de VM. Consulte [Criar uma política de posicionamento de VM em um VDC do provedor](#). No VMware Cloud Director 10.2.2 e versões posteriores, você pode criar uma política de posicionamento global que contenha uma referência a uma ou mais políticas de VDC do provedor. Consulte [Criar uma política de posicionamento de VM global](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Selecione um VDC de organização e clique na guia **Políticas de Posicionamento de VM**.
- 4 Clique em **Adicionar**.
- 5 Selecione as políticas de posicionamento de VM que você deseja adicionar ao VDC de organização e clique em **OK**.

Próximo passo

- Selecione uma política e clique em **Remover** para cancelar a publicação da política.
- Selecione uma política de posicionamento de VM e clique em **Definir como padrão** para fazer com que essa política apareça como a opção padrão para os tenants durante uma criação de VM e vApp e a edição da VM. Se houver mais de uma política de posicionamento de VM publicada para um VDC de organização, o tenant poderá selecionar uma política diferente da padrão.

Excluir uma política de posicionamento de VM

Se uma política de posicionamento de VM não estiver publicada para tenants, você poderá excluí-la do VDC de provedor.

Pré-requisitos

- Verifique se você tem pelo menos uma política de posicionamento de VM no seu ambiente.
- Verifique se a política de posicionamento de VM não foi adicionada a um VDC de organização. Não é possível excluir políticas de posicionamento de VM que estão disponíveis para tenants.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor**.
- 3 Clique em um VDC de provedor na lista.
- 4 Clique na guia **Políticas de Posicionamento de VM** e selecione uma política de posicionamento de VM.
- 5 Clique em **Excluir**.

Atributos das políticas de dimensionamento de VM

Ao criar uma política de dimensionamento de máquina virtual (VM), você pode especificar um subconjunto de todos os atributos disponíveis. O único atributo obrigatório é o nome da política de dimensionamento de VM.

Há dois tipos de parâmetros em uma política de dimensionamento de VM.

- Configuração de dimensionamento de VM individual — Você pré-configura a RAM especificada, a contagem de vCPUs e os núcleos por soquete para as VMs na política atual.
- Restrições sobre os recursos máximos — Você pré-configura uma limitação para consumo de memória e CPU por uma única VM na política atual.

A tabela a seguir lista todos os atributos que podem ser definidos dentro de uma política de dimensionamento de VM.

Tabela 6-2. Atributos da política de processamento de VDC

Atributo da política de processamento de VDC	Parâmetro da API	Descrição
Name	name	Parâmetro obrigatório que é usado como um identificador para a política de dimensionamento de VM.
Description	description	Representa uma descrição resumida da política de política de dimensionamento de VM.
vCPU Speed	cpuSpeed	Define a velocidade da vCPU de um núcleo em MHz ou GHz.
vCPU Count	cpuCount	Define o número de vCPUs configuradas para uma VM. Esta é uma configuração de hardware de VM. Quando um tenant atribui a política de dimensionamento de VM a uma VM, essa contagem se torna o número configurado de vCPUs para essa VM.
Cores Per Socket	coresPerSocket	O número de núcleos por soquete para uma VM. Esta é uma configuração de hardware de VM. O número de vCPUs definido na política de dimensionamento de VM deve ser divisível pelo número de núcleos por soquete. Se o número de vCPUs não for divisível pelo número de núcleos por soquete, o número de núcleos por soquete se tornará inválido.
CPU Reservation Guarantee	cpuReservationGuarantee	Define o quanto dos recursos da CPU de uma VM estão reservados. A CPU alocada para uma VM é igual ao número de vCPUs vezes a velocidade da vCPU em MHz. O valor do atributo varia entre 0 e 1. O valor da garantia de reserva de CPU 0 define nenhuma reserva de CPU. O valor de 1 define 100% da CPU reservada.
CPU Limit	cpuLimit	Define o limite da CPU em MHz ou GHz para uma VM. Se não for definido na política de processamento de VDC, o limite de CPU será igual à velocidade da vCPU multiplicada pelo número de vCPUs.

Tabela 6-2. Atributos da política de processamento de VDC (continuação)

Atributo da política de processamento de VDC	Parâmetro da API	Descrição
CPU Shares	cpuShares	Define o número de compartilhamentos de CPU para uma VM. Compartilhamentos especificam a importância relativa de uma VM em um centro de dados virtual. Se uma VM tiver o dobro de compartilhamentos de CPU que outra VM, ela poderá consumir o dobro de CPU quando essas duas máquinas virtuais estiverem competindo por recursos. Se não estiver definido na política de processamento do VDC, os compartilhamentos normais serão aplicados à VM.
Memory	memory	Define a memória configurada para uma VM em MB ou GB. Esta é uma configuração de hardware de VM. Quando um tenant atribui a política de dimensionamento de VM a uma VM, a VM recebe a quantidade de memória definida por esse atributo.
Memory Reservation Guarantee	memoryReservationGuarantee	Define a quantidade reservada de memória que está configurada para uma VM. O valor do atributo varia entre 0 e 100%.
Memory Limit	memoryLimit	Define o limite de memória em MB ou GB para uma VM. Se não estiver definido na política de dimensionamento de VM, o limite de memória será igual à memória alocada para a VM.
Memory Shares	memoryShares	Define o número de compartilhamentos de memória para uma VM. Compartilhamentos especificam a importância relativa de uma VM em um centro de dados virtual. Se uma VM tiver o dobro de compartilhamentos de memória que outra VM, ela poderá consumir o dobro de memória quando essas duas máquinas virtuais estiverem competindo por recursos. Se não estiver definido na política de processamento do VDC, os compartilhamentos normais serão aplicados à VM.
Extra Configurations	extraConfigs	Representa um mapeamento entre pares de chave e valor que são aplicados como valores de configuração extras em uma VM. Você pode criar uma política com configurações extras somente por meio da API do vCloud. As configurações extras existentes aparecem na interface de usuário do Service Provider Admin Portal em Configurações Extras na exibição da política de dimensionamento de VM detalhada.

Criar uma política de dimensionamento de VM

Você pode criar uma política de dimensionamento de VM para disponibilizar para os tenants restrições de consumo de memória e CPU predefinidas que podem ser aplicadas a VMs individuais em um VDC de organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Políticas de dimensionamento de VM**.
- 3 Clique em **Novo**.

- 4 Insira um nome para a política de dimensionamento de VM e, opcionalmente, uma descrição.
- 5 Clique em **Avançar**.
- 6 Na página **CPU**, selecione as configurações de alocação de CPU que você deseja aplicar à política e clique em **Avançar**.
- 7 Selecione as configurações de alocação de memória que você deseja aplicar à política e clique em **Avançar**.
- 8 Revise as configurações de política de dimensionamento de VM e clique em **Concluir**.

Próximo passo

- Depois de criar uma política de dimensionamento de VM, você apenas pode editar o nome e a descrição dessa política. Consulte [Editar uma política de dimensionamento de VM](#).
- [Adicionar uma política de dimensionamento de VM a um VDC de organização](#).
- [Criar uma política de posicionamento de VM em um VDC do provedor](#).

Adicionar uma política de dimensionamento de VM a um VDC de organização

Quando você cria uma política de dimensionamento de VM, ela não é visível para os tenants. É possível publicar uma política de dimensionamento de VM em um VDC de organização para disponibilizá-la aos tenants.

Publicar uma política de dimensionamento de VM em um VDC de organização torna essa política visível para tenants. O tenant pode selecionar a política ao criar uma nova VM autônoma ou uma VM a partir de um modelo, editar uma VM, adicionar uma VM a um vApp e criar um vApp a partir de um modelo de vApp. Não é possível excluir uma política de dimensionamento de VM que está disponível para os tenants.

Pré-requisitos

- Verifique se você tem pelo menos um VDC de organização no seu ambiente. Consulte [Criar um centro de dados virtual da organização](#).
- Verifique se você tem pelo menos uma política de dimensionamento de VM. Consulte [Criar uma política de dimensionamento de VM](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Selecione um VDC de organização e clique na guia **Políticas de Dimensionamento de VM**.
- 4 Clique em **Adicionar**.
- 5 Selecione as políticas de dimensionamento de VM que você deseja adicionar ao VDC de organização e clique em **OK**.

Próximo passo

- Selecione uma política e clique em **Remover** para cancelar a publicação da política.
- Selecione uma política de dimensionamento de VM e clique em **Definir como padrão** para fazer com que essa política apareça como a opção padrão para os tenants durante uma criação de VM e vApp e a edição da VM. Se houver mais de uma política de dimensionamento de VM publicada para um VDC de organização, o tenant poderá selecionar uma política diferente da padrão.

Editar uma política de dimensionamento de VM

Depois de criar uma política de dimensionamento de VM, você pode editar apenas seu nome e descrição. Não há suporte para a edição de parâmetros de CPU e memória.

Pré-requisitos

- Verifique se você tem pelo menos um VDC de organização no seu ambiente. Consulte [Criar um centro de dados virtual da organização](#).
- Verifique se você tem pelo menos uma política de dimensionamento de VM. Consulte [Criar uma política de dimensionamento de VM](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Políticas de dimensionamento de VM**.
- 3 Clique no nome da política de dimensionamento de VM que você deseja editar.
- 4 Para editar o nome e a descrição da política, clique em **Editar**.
- 5 Clique em **Salvar**.

Próximo passo

[Adicionar uma política de dimensionamento de VM a um VDC de organização](#)

Excluir uma política de dimensionamento de VM

Você pode excluir políticas de dimensionamento de VM que não estão publicadas para tenants.

Pré-requisitos

- Verifique se você tem pelo menos uma política de dimensionamento de VM no seu ambiente.
- Verifique se a política de dimensionamento de VM não foi adicionada a um VDC de organização. Não é possível excluir políticas de dimensionamento de VM que estão disponíveis para tenants.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

- 2 No painel esquerdo, clique em **Políticas de dimensionamento de VM**.
- 3 Selecione uma política de dimensionamento de VM e clique em **Excluir**.

Usando o Kubernetes com o VMware Cloud Director

Ao usar o Kubernetes com o VMware Cloud Director, você pode fornecer um serviço Kubernetes de vários tenants para seus tenants.

Container Service Extension

Kubernetes Container Clusters são o plug-in do Container Service Extension para o VMware Cloud Director. Provedores de serviços e tenants devem usar o plug-in Kubernetes Container Clusters para criar clusters do Kubernetes. A partir do VMware Cloud Director 10.2, não é necessário baixar manualmente o plug-in e carregá-lo no VMware Cloud Director Service Provider Admin Portal. O plug-in está disponível no VMware Cloud Director por padrão. No entanto, você deve publicá-lo nos tenants para permitir que eles criem clusters do Kubernetes.

Tanto provedores de serviços quanto tenants devem usar o Container Service Extension versão 3.0 para criar clusters nativos e VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). Você deve concluir a configuração do Container Service Extension 3.0 do servidor e publicar uma política de posicionamento nativa do Container Service Extension para um ou mais VDCs de organização.

vSphere with VMware Tanzu no VMware Cloud Director

Você pode usar o vSphere with VMware Tanzu no VMware Cloud Director para criar centros de dados virtuais (VDCs) de provedor com o suporte de Clusters de Supervisor. Um cluster de host com o vSphere with VMware Tanzu ativado é chamado de Cluster de Supervisor. Você pode definir restrições sobre os usos dos recursos e limitar os recursos disponíveis, incluindo o número de clusters do Kubernetes por organização, usuário ou grupo. Para obter mais informações, consulte [Gerenciar cotas sobre o consumo de recursos de uma organização](#).

Para usar o vSphere with VMware Tanzu no VMware Cloud Director, primeiro você deve ativar a funcionalidade do vSphere with VMware Tanzu em um cluster do vSphere 7.0 ou posterior e configurar esse cluster como um Cluster de Supervisor. Consulte o guia de *Configuração e gerenciamento do vSphere with Kubernetes* na documentação do vSphere. A instância do vCenter Server que você deseja usar pode ter clusters de hosts e Clusters de Supervisor.

Para criar clusters do Tanzu Kubernetes, você deve publicar uma política do Kubernetes do VDC de provedor em uma organização e aplicar a política do Kubernetes do VDC de organização durante a criação. Clusters nativos e TKGI não usam as políticas do Kubernetes do VDC de provedor e organização.

Tipos de cluster do Kubernetes

- 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. Para a implantação do cluster do Kubernetes nativo, você deve configurar um servidor do Container Service Extension. Consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).

- Clusters do Tanzu Kubernetes - Você pode usar o vSphere com a opção de tempo de execução do Tanzu para criar clusters do Tanzu Kubernetes gerenciados pelo vSphere with VMware Tanzu. 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 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, recuperação automática e atualizações contínuas para clusters do Kubernetes. Para obter mais informações sobre clusters TKGI, consulte a documentação do *VMware Tanzu Kubernetes Grid Integrated Edition*.

Fluxo de trabalho para criação de clusters do Tanzu Kubernetes

- 1 Adicione uma instância do vCenter Server 7.0 ou posterior com uma funcionalidade do vSphere with VMware Tanzu ativada ao VMware Cloud Director. Consulte [Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager](#).
- 2 Verifique as configurações de rede em cada Cluster de Supervisor para ativá-las para executar cargas de trabalho do Kubernetes.

Importante Os intervalos de endereços IP para os parâmetros `Ingress CIDRs` e `Services CIDR` não devem se sobrepor aos endereços IP 10.96.0.0/12 e 192.168.0.0/16 que são os valores de vSphere padrão para os parâmetros `services` e `pods`. Consulte os parâmetros de configuração para informações de clusters do Tanzu Kubernetes no guia *Gerenciamento e configuração do vSphere with Kubernetes*.

Observação No VMware Cloud Director 10.2.2, se você modificar as configurações de rede do cluster supervisor após a configuração inicial, deverá atualizar a instância do vCenter Server para ajustar as políticas de firewall e regras NAT automáticas que bloqueiam o acesso ao cluster do Tanzu Kubernetes de fora do centro de dados virtual da organização no qual esse cluster é criado.

- 3 Crie um VDC de provedor com o suporte de um Cluster de Supervisor. Consulte [Criar um centro de dados virtual do provedor](#).

Como alternativa, você pode adicionar um Cluster de Supervisor a um VDC de provedor existente. Se você tiver um ambiente do vSphere 6.7 ou anterior, também poderá atualizar esse ambiente para a versão 7.0 e ativar o vSphere with VMware Tanzu em um cluster existente.

VDCs de provedor com o suporte de um Cluster de Supervisor aparecem com um ícone do Kubernetes ao lado do seu nome na grade que lista todos os VDCs de provedor.

- 4 (Opcional) O VMware Cloud Director gera automaticamente uma política do Kubernetes de VDC de provedor padrão para VDCs de provedor com o suporte de um Cluster de Supervisor. Você pode criar políticas do Kubernetes do VDC de provedor adicionais para clusters do Tanzu Kubernetes. Consulte [Criar uma política do Kubernetes do VDC de provedor](#).
- 5 [Publicar uma política do Kubernetes do VDC de provedor para um VDC de organização](#) na guia **VDCs de Provedor** ou [Adicionar uma política do Kubernetes do VDC de Organização](#) na guia **VDCs de Organização**.
- 6 Publique o plug-in Kubernetes Container Clusters para provedores de serviços. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#). Se quiser permitir que os tenants criem clusters do Kubernetes, você deverá publicar o plug-in Kubernetes Container Clusters para essas organizações. Para obter mais informações sobre como gerenciar plug-ins do VMware Cloud Director, consulte [Gerenciando plug-ins](#).
- 7 Se quiser conceder aos tenants os direitos para criar e gerenciar clusters do Tanzu Kubernetes, você deverá publicar o pacote de direitos **vmware:tkgcluster Entitlement** a todas as organizações que você deseja trabalhar com clusters. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit: Tanzu Kubernetes Guest Cluster** às funções que deseja criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control: Tanzu Kubernetes Guest Cluster** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- 8 Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).
- 9 [Criar um cluster do Tanzu Kubernetes](#)

Fluxo de trabalho para a criação de clusters nativos e TKGI

- 1 Publique o plug-in Kubernetes Container Clusters para provedores de serviços. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#). Se quiser permitir que os tenants criem clusters do Kubernetes, você deverá publicar o plug-in Kubernetes Container Clusters para essas organizações. Para obter mais informações sobre como gerenciar plug-ins do VMware Cloud Director, consulte [Gerenciando plug-ins](#).

- 2 Configure um servidor Container Service Extension e publique a política de posicionamento nativa do Container Service Extension ou os metadados de ativação do TKGI para o VDC de organização. Para obter mais informações sobre como configurar o servidor CSE, consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- 3 Se quiser conceder aos tenants os direitos para criar e gerenciar clusters nativos, você deverá publicar o pacote de direitos **cse:nativeCluster Entitlement** a todas as organizações que você deseja trabalhar com clusters nativos. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit CSE:NATIVECLUSTER** às funções que deseja criar e modificar clusters nativos. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control CSE:NATIVECLUSTER** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que exibam todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- 4 Se você deseja conceder aos tenants os direitos de criar e gerenciar clusters do TKGI, deverá publicar **{cse}:PKS DEPLOY RIGHT** para as organizações específicas e adicionar o direito **{cse}:PKS DEPLOY RIGHT** às funções que você deseja que criem e gerenciem clusters do TKGI. O direito **{cse}:PKS DEPLOY RIGHT** é criado durante a instalação do servidor Container Service Extension.
- 5 Para clusters nativos, conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).
- 6 [Criar um cluster do Kubernetes nativo](#) ou [Criar um cluster do VMware Tanzu Kubernetes Grid Integrated Edition](#).

Adicionar uma política do Kubernetes do VDC de Organização

Você pode adicionar uma política do Kubernetes do VDC de organização usando uma política do Kubernetes do VDC de provedor. Os tenants podem usar a política do Kubernetes do VDC de organização para criar clusters do Tanzu Kubernetes.

Ao adicionar ou publicar uma política do Kubernetes do VDC de provedor a um VDC de organização, você torna essa política disponível para os tenants. 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 pelo menos um VDC de organização flexível no seu ambiente. Consulte [Criar um centro de dados virtual da 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**. Para obter mais informações sobre o vSphere with VMware Tanzu no VMware Cloud Director, consulte [Usando o Kubernetes com o VMware Cloud Director](#).
- 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Organização** e clique no nome de um VDC de organização flexível.
- 3 Em Políticas, selecione **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

[Gerenciar cotas sobre o consumo de recursos de uma organização](#)

Editar uma política do Kubernetes do VDC de organização

Você pode modificar uma política do Kubernetes do VDC de organização para alterar sua descrição e os limites de CPU e memória.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Organização** e clique no nome de um VDC de organização flexível.

- 3 Em Políticas, selecione **Kubernetes**, selecione a política que você deseja editar e clique em **Editar**.

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

- 4 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.

- 5 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.

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

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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

- Publique o plug-in Kubernetes Container Clusters em qualquer organização que você deseja gerenciar clusters do Tanzu Kubernetes.
- 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](#).
- Você deve publicar o pacote de direitos **vmware:tkgcluster Entitlement** para todas as organizações que você deseja trabalhar com clusters. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit: Tanzu Kubernetes Guest Cluster** às funções que deseja criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control: Tanzu Kubernetes Guest Cluster** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja

que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).

- Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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**.
- Para ativar o VDC de organização para implantação de cluster do Kubernetes nativo, configure o servidor Container Service Extension. Consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- Publique a política nativa de CSE criada durante a configuração do servidor CSE em um VDC de organização. Para usar a interface de usuário, consulte [Adicionar uma política de posicionamento de VM a um VDC de organização](#). Como alternativa, você pode usar o CSE 3.0 CLI para publicar a política executando o comando `vcd cse ovdc enable Organization_VDC_Name --org Organization_Name --native`.

- Você deve publicar o pacote de direitos **cse:nativeCluster Entitlement** para qualquer organização que queira trabalhar com clusters nativos. Depois de compartilhar o pacote de direitos, você deve adicionar o direito **Edit CSE:NATIVECLUSTER** às funções que deseja para criar e modificar clusters do Tanzu Kubernetes. Se você deseja que os usuários também excluam clusters, deverá adicionar o direito **Full Control CSE:NATIVECLUSTER** às funções. Além disso, é possível atribuir direitos de administrador aos usuários que você deseja que visualizem todos os clusters do Tanzu Kubernetes em uma organização ou usuários que você deseja que gerenciem clusters entre os sites. Para obter informações sobre os direitos e os níveis de acesso para Runtime Defined Entities (RDEs), consulte [Capítulo 14 Gerenciamento de entidades definidas](#).
- Conceda acesso a tenants ou administradores do sistema criando entradas da Lista de Controle de Acesso (ACL). Para obter mais informações sobre o compartilhamento de Runtime Defined Entities (RDEs), consulte [Compartilhamento de entidades definidas](#).

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 [Usando o Kubernetes com o VMware Cloud Director](#).

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

Ao usar os metadados de ativação do TKGI, você pode fornecer acesso aos tenants para criar clusters do TKGI e acessar o VDC de organização ativado para TKGI. Se você deseja limitar a capacidade dos tenants de criar clusters do TKGI, poderá fornecer acesso apenas ao VDC de organização. Nesse caso, os tenants podem gerenciar clusters do TKGI existentes, mas não podem criar novos.

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**.
- Para ativar o VDC de organização para implantação de cluster do Kubernetes TKGI, configure o servidor Container Service Extension. Para obter informações sobre como usar a CSE CLI para ativar um VDC de organização para o TKGI, consulte o capítulo [Gerenciamento do servidor CSE](#) na documentação do Container Service Extension (CSE).
- Se você deseja fornecer acesso de tenant à criação e ao gerenciamento de TKGI, deverá publicar **{cse}:PKS DEPLOY RIGHT** para as organizações específicas e adicionar o direito **{cse}:PKS DEPLOY RIGHT** às funções que você deseja criar e gerenciar clusters do TKGI. O direito **{cse}:PKS DEPLOY RIGHT** é criado durante a instalação do servidor Container Service Extension.

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.

Criar um centro de dados virtual da organização

Para alocar recursos a uma organização, você deve criar um centro de dados virtual (VDC) de organização. Um centro de dados virtual da organização obtém seus recursos de um VDC de provedor. Uma organização pode ter vários VDCs de organização.

Pré-requisitos

Crie um VDC de provedor. Consulte [Criar um centro de dados virtual do provedor](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de organização** e clique em **Novo**.
- 3 Digite um nome e, opcionalmente, uma descrição para o novo VDC de organização.
- 4 (Opcional) Para desativar o novo VDC de organização na criação, desative a opção **Ativar o VDC de organização**.

Os usuários não podem implantar vApps em um VDC de organização desativado.
- 5 Clique em **Avançar**.
- 6 Selecione o botão de opção ao lado do nome da organização à qual deseja adicionar esse VDC e clique em **Próximo**.

- 7 Selecione o botão de opção ao lado do nome do VDC de provedor do qual deseja que o VDC de organização obtenha recursos de cálculo e armazenamento e clique em **Próximo**.

A lista de VDCs de provedor exibe todos os VDCs de provedor ativados no site com informações sobre os recursos disponíveis. A lista de redes exibe informações sobre as redes disponíveis para o VDC de provedor selecionado.

- 8 Selecione um modelo de alocação para o VDC da organização e clique em **Avançar**.

Opção	Descrição
Pool de alocações	Uma porcentagem dos recursos alocados do VDC do provedor é comprometida no VDC da organização. Você pode especificar a porcentagem para CPU e memória.
Pago pelo uso	Os recursos são confirmados somente quando os usuários criam vApps no VDC da organização.
Pool de reservas	Todos os recursos alocados são imediatamente fornecidos ao VDC da organização.
Flex	Você pode controlar o consumo de recursos nos níveis de VDC e de máquina virtual individual. O modelo de alocação flexível oferece suporte aos recursos das políticas de processamento do VDC de organização. O modelo de alocação flexível oferece suporte a todas as configurações de alocação disponíveis nos outros modelos de alocação.

- 9 Defina as configurações de alocação para o modelo de alocação selecionado e clique em **Próximo**.

Opção	Descrição	Modelo de alocação
Elasticidade	Ative ou desative o recurso de pool elástico. Um VDC de organização elástico abrange e usa todos os pools de recursos associados ao VDC de provedor.	Flex
Incluir sobrecarga de memória da VM	Incluir ou excluir sobrecarga de memória.	Flex
Alocação de CPU	A quantidade máxima de CPU que você deseja alocar às máquinas virtuais em execução neste VDC de organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas ■ Flex
Permitir que os recursos da CPU ultrapassem o valor reservado	Para fornecer recursos de CPU ilimitados para este VDC de organização, ative essa opção.	Pool de Reservas
Cota da CPU	A quantidade máxima de consumo de CPU para este VDC de organização.	<ul style="list-style-type: none"> ■ Pago pelo uso ■ Flex
Recursos da CPU garantidos	<p>A porcentagem de recursos da CPU que você deseja garantir para uma máquina virtual em execução neste VDC de organização. Você pode controlar o comprometimento dos recursos da CPU garantindo menos de 100 por cento.</p> <p>Para um modelo de alocação de Pool de Alocação, a garantia de porcentagem também determina qual porcentagem da alocação da CPU é confirmada para esse VDC de organização.</p>	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo uso ■ Flex

Opção	Descrição	Modelo de alocação
Velocidade da vCPU	A velocidade da vCPU. As máquinas virtuais em execução no VDC de organização recebem essa quantidade de GHz por vCPU.	<ul style="list-style-type: none"> ■ Pago pelo uso ■ Flex
Alocação de memória	A quantidade máxima de memória que você deseja alocar às máquinas virtuais em execução no VDC de organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas
Cota de memória	A quantidade máxima de consumo de memória para este VDC de organização.	<ul style="list-style-type: none"> ■ Pago pelo uso ■ Flex
Recursos de memória garantidos	<p>A porcentagem de recursos de memória que você deseja garantir para as máquinas virtuais em execução no VDC de organização. Você pode comprometer os recursos garantindo menos de 100 por cento.</p> <p>Para um modelo de alocação de Pool de Alocação, a garantia de porcentagem também determina qual porcentagem da alocação de memória é confirmada para esse VDC de organização.</p>	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo uso ■ Flex
Número máximo de VMs	O número máximo de máquinas virtuais que podem existir no VDC de organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo uso ■ Pool de Reservas ■ Flex

10 Defina as configurações de armazenamento para este VDC de organização e clique em **Próximo.**

A lista contém as políticas de armazenamento ativadas no VDC do provedor de origem.

- Marque as caixas de seleção de uma ou mais políticas de armazenamento que você deseja adicionar a este VDC de organização.
- (Opcional) Para limitar a quantidade de capacidade de armazenamento alocada para uma política de armazenamento selecionada, selecione **Limitado** no menu suspenso na célula **Tipo de alocação** e digite a capacidade máxima na célula **Armazenamento alocado**.
- (Opcional) Para alterar a política de armazenamento padrão, no menu suspenso **Política de instanciação padrão**, selecione a política de armazenamento padrão de destino.
O VMware Cloud Director usa a política de armazenamento padrão para todas as operações de provisionamento de máquina virtual na qual a política de armazenamento não é especificada no nível da máquina virtual ou do modelo do vApp.
- (Opcional) Para ativar o provisionamento dinâmico para máquinas virtuais no VDC de organização, ative a opção **Provisionamento dinâmico**.
- (Opcional) Para desativar o provisionamento rápido para máquinas virtuais no VDC de organização, desative a opção **Provisionamento rápido**.

11 Defina as configurações do pool de redes para este VDC de organização e clique em **Avançar.**

O VMware Cloud Director usa o pool de redes para criar redes do vApp e redes internas do VDC de organização.

- Para ignorar a adição de um pool de redes neste estágio, desative a opção **Usar Pool de Redes**.

- Para configurar um pool de redes, selecione o botão de opção ao lado do nome do pool de redes de destino e insira a Cota para esse VDC de organização.

A cota é o número máximo de redes provisionadas no VDC da organização com o suporte desse pool de redes. Ela não deve exceder o número de redes disponíveis para o pool de redes selecionado.

Observação Os VDCs de organização com suporte do NSX-T Data Center são compatíveis apenas com pools de redes Geneve.

12 Revise a página **Pronto para ser Concluído** e clique em **Concluir**.

Ativar ou desativar um centro de dados virtual da organização

Para evitar que máquinas virtuais e vApps adicionais usem os recursos de cálculo e armazenamento do centro de dados virtual de uma organização, você poderá desativar esse centro de dados virtual da organização. vApps em execução e máquinas virtuais ligadas continuam sendo executados, mas não é possível criar ou iniciar máquinas virtuais ou vApps adicionais.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Habilitar** ou **Desabilitar**.
- 4 Para confirmar, clique em **OK**.

Excluir um centro de dados virtual da organização

Para remover todos os recursos de um centro de dados virtual da organização, você pode excluir esse centro de dados. Os recursos permanecem inalterados no centro de dados virtual do provedor de origem.

Importante Esta operação remove permanentemente o centro de dados virtual da organização e todos os seus vApps, VMs, redes de centros de dados virtuais da organização e edge gateways.

Pré-requisitos

Se você quiser manter determinados VMs, vApps, modelos do vApp ou arquivos de mídia que pertencem ao centro de dados virtual da organização de destino, mova-os para outro centro de dados virtual da organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização que você deseja remover e clique em **Excluir**.
- 4 Se esse centro de dados virtual da organização contiver recursos, como VMs, vApps, redes de centro de dados virtual da organização e edge gateways, para confirmar a remoção, marque a caixa de seleção de cada tipo de recurso.
- 5 Para confirmar, clique em **Excluir**.

Gerenciando modelos de centro de dados virtual

No VMware Cloud Director 10.2.2, é possível criar e compartilhar modelos de centro de dados virtual (VDC) com organizações de tenant para que os **administradores da organização** possam usar os modelos para criar VDCs.

Ao criar e compartilhar modelos de VDC com organizações, você pode ativar o fornecimento de autoatendimento de VDCs da organização e, ao mesmo tempo, manter o controle administrativo sobre a alocação de recursos do sistema, como VDCs do provedor e redes externas.

Um modelo de VDC especifica o modelo de alocação, a memória, a configuração de recursos de CPU e as políticas de armazenamento para o novo VDC de organização e, opcionalmente, um edge gateway e uma rede de VDC da organização.

Criar um modelo de centro de dados virtual da organização

No VMware Cloud Director 10.2.2, é possível usar a UI HTML5 para criar modelos de centro de dados virtual da organização (VDC) da organização para VDCs com o suporte do NSX Data Center for vSphere ou do NSX-T Data Center.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Modelos de VDC de Organização** e clique em **Novo**.
- 3 Selecione um tipo de provedor de rede, selecione um par de redes externa e VDC do provedor e clique em **Avançar**.

Para o NSX Data Center for vSphere, quando um usuário instancia um VDC da organização com base desse modelo, o VMware Cloud Director aplica os edge clusters selecionados ao novo VDC da organização. Todos os edge gateways recém-implantados no novo VDC da organização usam os edge clusters primário e secundário como posicionamentos.

Para o NSX-T Data Center, o VMware Cloud Director usa o **Cluster do Edge de Serviços** para implantar serviços de rede, como serviços DHCP, VPN e DNS. O VMware Cloud Director usa o **Cluster do Edge para o Gateway do NSX-T** para implantar o gateway.

Depois de iniciar um modelo de VDC da organização, você não poderá editar os edgee clusters.

- 4 Selecione um modelo de alocação para o VDC da organização e clique em **Avançar**.

Opção	Descrição
Pool de alocações	Uma porcentagem dos recursos alocados do VDC do provedor é comprometida no VDC da organização. Você pode especificar a porcentagem para CPU e memória.
Pago pelo Uso	Os recursos são confirmados somente quando os usuários criam vApps no VDC da organização.
Pool de reservas	Todos os recursos alocados são imediatamente fornecidos ao VDC da organização.
Flex	Você pode controlar o consumo de recursos nos níveis de VDC e de máquina virtual individual. O modelo de alocação flexível oferece suporte aos recursos das políticas de processamento do VDC de organização. O modelo de alocação flexível oferece suporte a todas as configurações de alocação disponíveis nos outros modelos de alocação.

- 5 Defina as configurações de alocação para o modelo de alocação selecionado e clique em **Próximo**.

Opção	Descrição	Modelo de Alocação
Elasticidade	Ative ou desative o recurso de pool elástico. Um VDC de organização elástico abrange e usa todos os pools de recursos associados ao VDC de provedor.	Flex
Incluir sobrecarga de memória da VM	Incluir ou excluir sobrecarga de memória.	Flex
Alocação de CPU	A quantidade máxima de CPU que você deseja alocar para as máquinas virtuais em execução neste centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas ■ Flex
Permitir que os recursos da CPU ultrapassem o valor reservado	Para fornecer recursos de CPU ilimitados para este centro de dados virtual da organização, ative essa opção.	Pool de Reservas
Cota da CPU	A quantidade máxima de consumo de CPU para este centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex
Recursos da CPU garantidos	A porcentagem de recursos da CPU que deseja garantir para uma máquina virtual em execução neste centro de dados virtual da organização. Você pode controlar o comprometimento dos recursos da CPU garantindo menos de 100 por cento. Para um modelo de alocação de Pool de alocações, a garantia de porcentagem também determina qual porcentagem da alocação de CPU é fornecida para esse centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Flex
Velocidade da vCPU	A velocidade da vCPU. As máquinas virtuais em execução no centro de dados virtual da organização recebem essa quantidade de GHz por vCPU.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex

Opção	Descrição	Modelo de Alocação
Alocação de memória	Quantidade máxima de memória que deseja alocar para as máquinas virtuais em execução no centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas
Limite de Memória	A quantidade máxima de consumo de memória para este centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex
Recursos de memória garantidos	<p>A porcentagem de recursos de memória que deseja garantir para as máquinas virtuais em execução neste centro de dados virtual da organização. Você pode comprometer os recursos garantindo menos de 100 por cento.</p> <p>Para um modelo de alocação de Pool de alocações, a garantia de porcentagem também determina qual porcentagem da alocação de memória é fornecida para esse centro de dados virtual da organização.</p>	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Flex
Número máximo de VMs	O número máximo de máquinas virtuais que podem existir no centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Pool de Reservas ■ Flex

- 6 Defina as configurações de armazenamento para este centro de dados virtual da organização e clique em **Próximo**.

A lista contém as políticas de armazenamento ativadas no VDC do provedor de origem.

- a Selecione uma ou mais políticas de armazenamento que você deseja adicionar a este VDC da organização.
- b (Opcional) Para limitar a quantidade de capacidade de armazenamento alocada para uma política de armazenamento selecionada, selecione **Limitado** no menu suspenso na célula **Tipo de alocação** e digite a capacidade máxima na célula **Armazenamento alocado**.
- c (Opcional) Para alterar a política de armazenamento padrão, no menu suspenso **Política de instanciação padrão**, selecione a política de armazenamento padrão de destino.

O VMware Cloud Director usa a política de armazenamento padrão para todas as operações de provisionamento de máquina virtual na qual a política de armazenamento não é especificada no nível da máquina virtual ou do modelo do vApp.
- d (Opcional) Para ativar o provisionamento dinâmico para máquinas virtuais no VDC da organização, ative a opção **Provisionamento dinâmico**.
- e (Opcional) Para desativar o provisionamento rápido para máquinas virtuais no VDC de organização, desative a opção **Provisionamento rápido**.

7 (Opcional) Crie um edge gateway.

- a Insira um nome e, opcionalmente, uma descrição para o novo edge gateway.
- b Se você estiver criando um modelo para um VDC com o suporte do NSX Data Center for vSphere, poderá personalizar as configurações gerais do edge gateway e clicar em **Avançar**.

Configuração geral	Descrição
Roteamento Distribuído	Configura um gateway avançado para fornecer roteamento lógico distribuído.
Modo FIPS	Configura o edge gateway para usar o modo NSX FIPS.
Alta Disponibilidade	Permite o failover automático para um edge gateway de backup.

- c Se você estiver criando um modelo para um VDC com o suporte do NSX Data Center for vSphere, poderá alterar a configuração do edge gateway para os recursos do sistema.

Configuração	Descrição
Compactar	Requer menos memória e menos recursos de computação.
Grande	Fornecer maior capacidade e desempenho do que a configuração Compacta. Configurações grandes e extragrandes fornecem funções de segurança idênticas.
Extragrande	Usado para ambientes que possuem um balanceador de carga com um grande número de sessões simultâneas.
Quádruplo	Usado para ambientes com alta taxa de transferência. Requer uma alta taxa de conexão.

- d (Opcional) Especifique quantos IPs você deseja alocar para o uso dos serviços de gateway.

8 Configure a rede do VDC da organização e clique em **Avançar**.

- a Insira um nome e, opcionalmente, uma descrição para a rede.
- b 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**.

- c Para tornar a rede de VDC da organização disponível para outros VDCs na mesma organização, ative o botão de alternância **Compartilhada**.

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 o modelo de pagamento por consumo e executar temporariamente mais VMs nessa rede.

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

- 9 Adicione um intervalo de endereços IP a partir dos intervalos dos pools de IPs estáticos disponíveis e clique em **Avançar**.
- 10 (Opcional) Defina as configurações do pool de redes para o VDC da organização e clique em **Avançar**.

A cota é o número máximo de redes provisionadas no VDC da organização com o suporte desse pool de redes. Ela não deve exceder o número de redes disponíveis para o pool de redes selecionado.

- 11 Selecione as organizações que você deseja visualizar e instancie os VDCs a partir deste modelo. Em seguida, clique em **Avançar**.

Administradores de sistema podem instanciar um VDC de qualquer modelo de VDC da organização. Ao usar o VMware Cloud Director Tenant Portal, os **administradores de organização** poderão instanciar um VDC se as organizações estiverem na lista de acesso de um modelo.

- 12 Insira um nome de sistema e um nome de modelo voltado para o tenant. Em seguida, clique em **Avançar**.
- 13 Revise a configuração do modelo de VDC da organização e clique em **Concluir**.

Próximo passo

- [Instanciar um centro de dados virtual a partir de um modelo.](#)
- [Editar um modelo de VDC da organização.](#) Você pode editar todas as propriedades de um modelo de VDC existente, exceto o tipo de provedor de rede.
- Para criar uma cópia de um modelo de VDC de organização personalizável, clone esse modelo. As etapas para clonagem são semelhantes às etapas para a edição de um modelo.
- Exclua um modelo de VDC da organização.

Instanciar um centro de dados virtual a partir de um modelo

Para criar um centro de dados virtual (VDC) da organização a partir de um modelo de VDC, instancie um VDC.

Administradores de sistema podem instanciar um VDC de qualquer modelo de VDC da organização. Ao usar o VMware Cloud Director Tenant Portal, os **administradores de organização** poderão instanciar um VDC se as organizações estiverem na lista de acesso de um modelo.

Pré-requisitos

[Criar um modelo de centro de dados virtual da organização](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Modelos de VDC da organização**.
- 3 Selecione um modelo de VDC da organização e clique em **Criar Instância do VDC**.

- 4 Insira um nome e, opcionalmente, uma descrição para o novo centro de dados virtual da organização.
- 5 Selecione uma organização para o VDC da organização e clique em **Criar**.

Editar um modelo de VDC da organização

Você pode modificar todas as propriedades de um modelo de centro de dados virtual (VDC) existente, exceto o tipo de provedor de rede.

Pré-requisitos

[Criar um modelo de centro de dados virtual da organização](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Modelos de VDC de Organização** e clique em **Editar**.
- 3 Selecione um par de redes externa e VDC do provedor e clique em **Avançar**.

Para o NSX Data Center for vSphere, quando um usuário instancia um VDC da organização com base desse modelo, o VMware Cloud Director aplica os edge clusters selecionados ao novo VDC da organização. Todos os edge gateways recém-implantados no novo VDC da organização usam os edge clusters primário e secundário como posicionamentos.

Para o NSX-T Data Center, o VMware Cloud Director usa o **Cluster do Edge de Serviços** para implantar serviços de rede, como serviços DHCP, VPN e DNS. O VMware Cloud Director usa o **Cluster do Edge para o Gateway do NSX-T** para implantar o gateway.

Depois de iniciar um modelo de VDC da organização, você não poderá editar os edge clusters.

- 4 Selecione um modelo de alocação para o VDC da organização e clique em **Avançar**.

Opção	Descrição
Pool de alocações	Uma porcentagem dos recursos alocados do VDC do provedor é comprometida no VDC da organização. Você pode especificar a porcentagem para CPU e memória.
Pago pelo Uso	Os recursos são confirmados somente quando os usuários criam vApps no VDC da organização.
Pool de reservas	Todos os recursos alocados são imediatamente fornecidos ao VDC da organização.
Flex	Você pode controlar o consumo de recursos nos níveis de VDC e de máquina virtual individual. O modelo de alocação flexível oferece suporte aos recursos das políticas de processamento do VDC de organização. O modelo de alocação flexível oferece suporte a todas as configurações de alocação disponíveis nos outros modelos de alocação.

5 Defina as configurações de alocação para o modelo de alocação selecionado e clique em **Próximo**.

Opção	Descrição	Modelo de Alocação
Elasticidade	Ative ou desative o recurso de pool elástico. Um VDC de organização elástico abrange e usa todos os pools de recursos associados ao VDC de provedor.	Flex
Incluir sobrecarga de memória da VM	Incluir ou excluir sobrecarga de memória.	Flex
Alocação de CPU	A quantidade máxima de CPU que você deseja alocar para as máquinas virtuais em execução neste centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas ■ Flex
Permitir que os recursos da CPU ultrapassem o valor reservado	Para fornecer recursos de CPU ilimitados para este centro de dados virtual da organização, ative essa opção.	Pool de Reservas
Cota da CPU	A quantidade máxima de consumo de CPU para este centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex
Recursos da CPU garantidos	<p>A porcentagem de recursos da CPU que deseja garantir para uma máquina virtual em execução neste centro de dados virtual da organização. Você pode controlar o comprometimento dos recursos da CPU garantindo menos de 100 por cento.</p> <p>Para um modelo de alocação de Pool de alocações, a garantia de porcentagem também determina qual porcentagem da alocação de CPU é fornecida para esse centro de dados virtual da organização.</p>	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Flex
Velocidade da vCPU	A velocidade da vCPU. As máquinas virtuais em execução no centro de dados virtual da organização recebem essa quantidade de GHz por vCPU.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex
Alocação de memória	A quantidade máxima de memória que você deseja alocar para as máquinas virtuais em execução no centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pool de Reservas
Limite de Memória	A quantidade máxima de consumo de memória para este centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pago pelo Uso ■ Flex
Recursos de memória garantidos	<p>A porcentagem de recursos de memória que deseja garantir para as máquinas virtuais em execução neste centro de dados virtual da organização. Você pode comprometer os recursos garantindo menos de 100 por cento.</p> <p>Para um modelo de alocação de Pool de alocações, a garantia de porcentagem também determina qual porcentagem da alocação de memória é fornecida para esse centro de dados virtual da organização.</p>	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Flex
Número máximo de VMs	O número máximo de máquinas virtuais que podem existir no centro de dados virtual da organização.	<ul style="list-style-type: none"> ■ Pool de Alocações ■ Pago pelo Uso ■ Pool de Reservas ■ Flex

- 6 Defina as configurações de armazenamento para este centro de dados virtual da organização e clique em **Próximo**.

A lista contém as políticas de armazenamento ativadas no VDC do provedor de origem.

- a Selecione uma ou mais políticas de armazenamento que você deseja adicionar a este VDC da organização.
- b (Opcional) Para limitar a quantidade de capacidade de armazenamento alocada para uma política de armazenamento selecionada, selecione **Limitado** no menu suspenso na célula **Tipo de alocação** e digite a capacidade máxima na célula **Armazenamento alocado**.
- c (Opcional) Para alterar a política de armazenamento padrão, no menu suspenso **Política de instanciação padrão**, selecione a política de armazenamento padrão de destino.
O VMware Cloud Director usa a política de armazenamento padrão para todas as operações de provisionamento de máquina virtual na qual a política de armazenamento não é especificada no nível da máquina virtual ou do modelo do vApp.
- d (Opcional) Para ativar o provisionamento dinâmico para máquinas virtuais no VDC da organização, ative a opção **Provisionamento dinâmico**.
- e (Opcional) Para desativar o provisionamento rápido para máquinas virtuais no VDC de organização, desative a opção **Provisionamento rápido**.

- 7 (Opcional) Crie um edge gateway.

- a Insira um nome e, opcionalmente, uma descrição para o novo edge gateway.
- b Se você estiver editando um modelo para um VDC com o suporte do NSX Data Center for vSphere, poderá personalizar as configurações gerais do edge gateway e clicar em **Avançar**.

Configuração geral	Descrição
Roteamento Distribuído	Configura um gateway avançado para fornecer roteamento lógico distribuído.
Modo FIPS	Configura o edge gateway para usar o modo NSX FIPS.
Alta Disponibilidade	Permite o failover automático para um edge gateway de backup.

- c Se você estiver editando um modelo para um VDC com o suporte do NSX Data Center for vSphere, poderá alterar a configuração do edge gateway para os recursos do sistema.

Configuração	Descrição
Compactar	Requer menos memória e menos recursos de computação.
Grande	Fornecer maior capacidade e desempenho do que a configuração Compacta. Configurações grandes e extragrandes fornecem funções de segurança idênticas.
Extragrande	Usado para ambientes que possuem um balanceador de carga com um grande número de sessões simultâneas.
Quádruplo	Usado para ambientes com alta taxa de transferência. Requer uma alta taxa de conexão.

- d (Opcional) Especifique quantos IPs você deseja alocar para o uso dos serviços de gateway.

8 Configure a rede do VDC da organização e clique em **Avançar**.

- a Insira um nome e, opcionalmente, uma descrição para a rede.
- b 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**.

- c Para tornar a rede de VDC da organização disponível para outros VDCs na mesma organização, ative o botão de alternância **Compartilhada**.

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 o modelo de pagamento por consumo e executar temporariamente mais VMs nessa rede.

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

- 9** Adicione um intervalo de endereços IP a partir dos intervalos dos pools de IPs estáticos disponíveis e clique em **Avançar**.
- 10** (Opcional) Defina as configurações do pool de redes para o VDC da organização e clique em **Avançar**.
A cota é o número máximo de redes provisionadas no VDC da organização com o suporte desse pool de redes. Ela não deve exceder o número de redes disponíveis para o pool de redes selecionado.
- 11** Selecione as organizações que você deseja visualizar e instancie os VDCs a partir deste modelo. Em seguida, clique em **Avançar**.
- 12** Insira um nome de sistema e um nome de modelo voltado para o tenant. Em seguida, clique em **Avançar**.

- 13 Revise a configuração do modelo de VDC da organização e clique em **Concluir**.

Modificar o nome e a descrição de um centro de dados virtual da organização

Como a sua instalação do VMware Cloud Director expande, você pode querer atribuir um nome ou uma descrição mais significativa a um centro de dados virtual da organização existente.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Na guia **Geral**, no canto superior direito, clique em **Editar**.
- 4 Insira um novo nome e descrição, e clique em **Salvar**.

Modificar as configurações do modelo de alocação de um centro de dados virtual da organização

Não é possível alterar o modelo de alocação para um centro de dados virtual da organização, mas você pode alterar as configurações de alocação para o modelo de alocação especificado durante a criação do centro de dados virtual da organização.

Você pode modificar as configurações de alocação para o modelo de alocação que configurou durante a criação do centro de dados virtual da organização. Consulte [Etapa 9](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Na guia **Alocação**, no canto superior direito, clique em **Editar**.
- 4 Edite as configurações do modelo de alocação e clique em **Salvar**.

Modificação das configurações de armazenamento de um centro de dados virtual de organização

Você pode modificar as configurações de armazenamento que configurou durante a criação do centro de dados virtual da organização.

Habilitando a criptografia da VM em políticas de armazenamento de um centro de dados virtual da organização

Você pode adicionar uma política de armazenamento habilitada para criptografia a um VDC de organização. Você pode criptografar VMs e discos associando uma VM ou um disco a uma política de armazenamento que tenha o recurso de criptografia de VM.

A partir do VMware Cloud Director 10.1, você pode melhorar a segurança dos seus dados usando a criptografia da 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 provedor tiver uma política de armazenamento com criptografia de VM habilitada, você poderá adicionar a política habilitada para criptografia a um VDC de organização. Consulte [Habilitando a criptografia da VM em políticas de armazenamento de um centro de dados virtual do provedor](#) e [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#). Depois, usando o VMware Cloud Director Tenant Portal, os tenants podem associar uma VM ou um disco a uma política de armazenamento com criptografia de VM habilitada.

Limitações de criptografia da VM

As seguintes ações não são suportadas no VMware Cloud Director 10.1.

- 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 VMs e discos. Para obter mais informações sobre funções e direitos, consulte [Funções predefinidas e seus direitos](#).

Você pode ver todos os recursos de armazenamento na coluna **Recursos** em **Recursos > Recursos do vSphere > Políticas de Armazenamento**. Essa coluna exibe a criptografia da VM, a associação baseada em tags, o vSAN e o IOPS limitando os recursos de armazenamento. Para visualizar a lista completa de recursos de armazenamento, expanda a linha clicando na seta à esquerda do nome da política de armazenamento.

Você também pode visualizar as informações de recurso de armazenamento na guia **Armazenamento** de um VDC de organização.

Modificar as configurações de provisionamento da VM de um centro de dados virtual de organização

Você pode modificar o provisionamento dinâmico e as configurações de provisionamento rápido da máquina virtual que você configurou durante a criação do centro de dados virtual de organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **armazenamento** e clique em **Editar**.
- 4 (Opcional) Modificar a configuração de provisionamento dinâmico.
 - Para desativar o provisionamento dinâmico para máquinas virtuais no centro de dados virtual de organização, desative a opção **Provisionamento dinâmico**.
 - Para ativar o provisionamento dinâmico para máquinas virtuais no centro de dados virtual de organização, ative a opção **Provisionamento dinâmico**.
- 5 (Opcional) Modificar a configuração de provisionamento rápido.
 - Para ativar o provisionamento rápido para máquinas virtuais no centro de dados virtual de organização, ative o botão de alternância de **Provisionamento rápido**.
 - Para desativar o provisionamento rápido para máquinas virtuais no centro de dados virtual de organização, desative a opção **Provisionamento rápido**.
- 6 Clique em **Editar**.

Adicionar uma política de armazenamento de VM a um data center virtual da organização

É possível configurar um data center virtual da organização para oferecer suporte a uma política de armazenamento de VM que você adicionou anteriormente ao data center virtual do provedor de suporte.

Pré-requisitos

Você adicionou a política de armazenamento da VM de destino ao centro de dados virtual do provedor de origem. Consulte [Adicionar uma política de armazenamento de VM a um datacenter virtual do provedor](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento** e clique em **Adicionar**.

Você pode ver uma lista das políticas de armazenamento adicionais disponíveis no centro de dados virtual do provedor de origem.
- 4 Marque as caixas de seleção de uma ou mais políticas de armazenamento que deseja adicionar e clique em **Adicionar**.

Alterar a política de armazenamento padrão em um centro de dados virtual da organização

Você pode alterar a política de armazenamento padrão que configurou durante a criação de um centro de dados virtual da organização.

O VMware Cloud Director usa a política de armazenamento padrão para todas as operações de provisionamento de máquina virtual na qual a política de armazenamento não é especificada no nível da máquina virtual ou do modelo do vApp.

Pré-requisitos

- A política de armazenamento padrão de destino é adicionada ao centro de dados virtual da organização. Consulte [Adicionar uma política de armazenamento de VM a um data center virtual da organização](#).
- A política de armazenamento padrão de destino é ativada no centro de dados virtual da organização. Consulte [Ativar ou desativar uma política de armazenamento em um centro de dados virtual da organização](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado do nome da política de armazenamento padrão de destino e clique em **Definir como padrão**.
- 5 Para confirmar, clique em **OK**.

Editar o limite de uma política de armazenamento em um centro de dados virtual da organização

Você pode alterar o limite da capacidade de armazenamento alocado que configurou para uma política de armazenamento durante a criação de um centro de dados virtual da organização.

Você pode definir a capacidade de armazenamento alocada como ilimitada ou configurar uma quantidade máxima de capacidade de armazenamento alocada para uma política de armazenamento em um centro de dados virtual da organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado do nome da política de armazenamento de destino e clique em **Editar limite**.
- 5 Defina a configuração de limite para essa política de armazenamento.
 - Para definir um limite, selecione o botão de opção superior e insira a quantidade máxima de recursos de armazenamento para essa política de armazenamento neste centro de dados virtual da organização.
 - Para definir nenhum limite, selecione o botão de opção **Ilimitado**.
- 6 Clique em **Editar**.

Modificar os metadados de uma política de armazenamento de VM em um centro de dados virtual da organização

Você pode adicionar, editar e excluir metadados para uma política de armazenamento em um centro de dados virtual da organização.

Ao usar os metadados do objeto, você pode associar pares de *nome =valor* definidos pelo usuário com uma política de armazenamento em um centro de dados virtual da organização. Você pode usar os metadados do objeto nas expressões de filtro de consulta da API do vCloud.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado do nome da política de armazenamento de destino e clique em **Metadados**.
- 5 Clique em **Editar**.
- 6 (Opcional) Para adicionar um par chave-valor, clique em **Adicionar**, insira um nome e um valor e selecione um tipo para o novo par chave-valor.
- 7 (Opcional) Para editar um par de chave-valor, insira um novo nome e um valor e selecione um novo tipo para o par chave-valor.
- 8 (Opcional) Para remover um par de chave/valor, na extremidade direita da linha, clique no ícone **Excluir**.
- 9 Clique em **Salvar** e em **OK**.

Ativar ou desativar uma política de armazenamento em um centro de dados virtual da organização

Para evitar que máquinas virtuais e vApps adicionais usem uma política de armazenamento em um centro de dados virtual da organização, você poderá desativar essa política de armazenamento no centro de dados virtual da organização. Os vApps em execução e máquinas virtuais ligadas continuam sendo executados, mas não é possível criar ou iniciar máquinas virtuais ou vApps adicionais nesta política de armazenamento.

Não é possível desativar a política de armazenamento padrão.

Pré-requisitos

Se quiser desativar a política de armazenamento padrão, [Alterar a política de armazenamento padrão em um centro de dados virtual da organização](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado do nome da política de armazenamento de destino e clique em **Habilitar** ou **Desabilitar**.
- 5 Para confirmar, clique em **OK**.

Excluir uma política de armazenamento de um centro de dados virtual da organização

Para evitar que um centro de dados virtual da organização use uma política de armazenamento, você pode removê-la do centro de dados virtual da organização. Os vApps em execução e máquinas virtuais ligadas continuam sendo executados, mas não é possível criar ou iniciar máquinas virtuais ou vApps adicionais nesta política de armazenamento.

Pré-requisitos

Desative a política de armazenamento que você deseja remover. Consulte [Ativar ou desativar uma política de armazenamento em um centro de dados virtual da organização](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado do nome da política de armazenamento de destino e clique em **Remover**.
- 5 Para confirmar, clique em **Remover**.

Editar as configurações da política de armazenamento de VDC de organização

É possível alterar as configurações de operações de E/S por segundo (IOPS) de uma política de armazenamento de VDC de organização. Por padrão, as políticas de armazenamento de VDC de organização herdam as configurações de políticas de armazenamento de VDC de provedor. Você pode personalizar as configurações por política de armazenamento de VDC de organização.

Pré-requisitos

[Adicionar uma política de armazenamento de VM a um data center virtual da organização](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs de Organização** e, em seguida, clique no nome do centro de dados virtual de organização de destino.
- 3 Em **Políticas**, selecione **Armazenamento**.
- 4 Clique no botão de opção ao lado da política de armazenamento de destino e clique em **Editar Configurações**.

- 5 Se quiser que as configurações de IOPS da política de armazenamento de VDC de organização sejam diferentes da política de armazenamento de VDC de provedor, desative o botão de alternância **Herdar do VDC de Provedor**.
- 6 Se quiser limitar as operações de E/S por segundo, ative o botão de alternância **Limitação de IOPS**.
- 7 Se quiser que as operações de IOPS sejam consideradas durante o posicionamento, ative o botão de alternância **Afetar Posicionamento**.

Se o botão de alternância de **Afetar Posicionamento** estiver ativado, o VMware Cloud Director fornecerá balanceamento de carga de IOPS entre os repositórios de dados. Quando você define as configurações de IOPS para um disco, o VMware Cloud Director considera os repositórios de dados com capacidade de IOPS suficiente para o disco selecionado. Se o botão de alternância de **Afetar Posicionamento** estiver desativado, você não precisará definir as capacidades de IOPS por repositório de dados e poderá usar os clusters de DRS de Armazenamento.

- 8 (Opcional) Defina as configurações máximas e padrão para IOPS.
- 9 Clique em **Salvar**.

Editar as configurações de rede de um data center virtual de organização

Você pode alterar o pool de redes do qual as novas redes são provisionadas em um centro de dados virtual da organização. Você também pode habilitar os data centers virtuais de organização para se qualificarem para a rede entre data centers virtuais.

Um pool de redes é um grupo de redes não diferenciadas que você pode usar para criar redes do vApp, redes de VDC de organização roteadas e redes de VDC de organização internas. Você pode alterar o pool de redes para novas redes. As redes existentes continuam a usar os pools de redes antigos.

Com data centers virtuais de organização habilitados para a rede entre data centers virtuais, os usuários da organização com direitos relevantes podem criar grupos de data centers e redes de camada 2 estendidas nesses grupos.

Pré-requisitos

Se quiser habilitar a rede entre VDCs para um centro de dados virtual da organização, verifique se configurou o NSX entre o vCenter no centro de dados virtual de provedor de suporte.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.

- 3 Na guia **Pool de Redes**, no canto superior direito, clique em **Editar**.

Você pode ver o número de redes usadas por esse data center virtual de organização.

- 4 (Opcional) Defina as configurações do pool de redes para esse data center virtual de organização.

Observação Os VDCs de organização com suporte do NSX-T Data Center são compatíveis apenas com pools de redes Geneve.

- Se você não quiser um pool de redes para esse data center virtual de organização, desative a opção **Usar pool de redes**.
 - Se quiser configurar um pool de redes para esse data center virtual de organização, siga estas etapas:
 - a Ative o botão de alternância **Usar pool de redes**.
 Você pode ver uma lista dos pools de redes disponíveis, com informações sobre seu uso, sobre as redes disponíveis e sobre a capacidade.
 - b Selecione o botão de opção ao lado do nome do pool de recursos de destino.
 - c Configure a cota deste pool de redes neste centro de dados virtual da organização.
 A cota é o número máximo de redes provisionadas. Ela não deve exceder o número de redes disponíveis para o pool de redes selecionado.
- 5 Para habilitar a rede entre data centers virtuais para este data center virtual de organização, ative o botão de alternância **Redes em VDCs**.

- 6 Clique em **Salvar**.

Resultados

No Portal de Tenant do VMware Cloud Director, os centros de dados virtuais ativados para redes entre centros de dados virtuais aparecem na lista dos centros de dados para a criação de um grupo de centros de dados. Para obter informações sobre a criação de grupos de centros de dados, consulte *Guia do Portal de Tenants do VMware Cloud Director*.

Configurando a rede do centro de dados virtual cruzada

O recurso de rede do centro de dados virtual cruzada permite que organizações que possuem centros de dados virtuais respaldados por várias instâncias do vCenter Server ampliem as redes da camada 2 em até quatro centros de dados virtuais. A rede do centro de dados virtual cruzada depende do vCenter NSX cruzado e pode abranger vários sites do VMware Cloud Director.

A rede entre centros de dados virtuais requer o NSX Data Center for vSphere.

Com a rede de centro de dados virtual cruzada, as organizações podem agrupar até quatro centros de dados virtuais e configurar redes egressas e estendidas de camada 2 em cada grupo.

Os centros de dados virtuais da organização participante podem pertencer a diferentes sites do VMware Cloud Director. Consulte [Configurando e gerenciando implantações em multissites](#).

As organizações podem usar a rede de centro de dados virtual cruzada para implementar soluções de alta disponibilidade ou arquiteturas de sistemas distribuídos, em que um aplicativo pode ser distribuído entre vários centros de dados virtuais ou sites.

O **administrador do sistema** deve configurar o ambiente do vCenter NSX cruzado subjacente, os servidores do VMware Cloud Director, e ativar a rede do centro de dados virtual cruzada para cada centro de dados virtual.

- 1 Configure uma das instâncias do NSX Manager como uma instância Primária do NSX Manager. Consulte o *Guia de instalação do vCenter NSX cruzado*.
 - a Implante o cluster do NSX na instância primária do NSX Manager.
 - b Prepare os hosts do ESXi na instância primária do NSX Manager.
 - c Configure o VXLAN da instância primária do NSX Manager.
 - d Atribua a função primária para a instância do NSX Manager.
 - e Crie um pool de IP de segmento para a zona de transporte universal.
 - f Adicione uma zona de transporte universal.
- 2 Configure o restante das instâncias do NSX Manager como NSX Managers Secundários. Consulte o *Guia de instalação do vCenter NSX cruzado*.
 - a Prepare os hosts do ESXi em cada instância secundária do NSX Manager.
 - b Configure o VXLAN de cada instância secundária do NSX Manager.
 - c Atribua a função secundária para cada instância do NSX Manager.
 - d Conecte-se os clusters do ESXi à zona de transporte universal.
- 3 Configure as propriedades da VM de controle para cada instância do NSX Manager. Consulte [Modificar as configurações do NSX Manager](#).
- 4 Crie um pool de rede com backup VXLAN usando uma zona de transporte de tipo universal de qualquer instância do vCenter Server. Consulte [Criar um pool de redes com suporte de zona de transporte do NSX Data Center for vSphere](#).

Observação Para implantações em vários sites, você deve criar um pool de rede com backup VXLAN em cada site do VMware Cloud Director.

- 5 Ative a rede do centro de dados virtual cruzada em cada centro de dados virtual da organização. Consulte [Editar as configurações de rede de um data center virtual de organização](#).

- 6 Se a organização tiver centros de dados virtuais de vários sites, verifique se as IDs da instalação nos diferentes sites do VMware Cloud Director são diferentes. Se houver VMware Cloud Director sites configurados com o mesmo ID de instalação, consulte [Regenerando endereços MAC para redes estendidas multissite](#) no *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

O **administrador da organização** agora pode criar e configurar grupos de centros de dados, e redes egressas e estendidas. Para obter informações sobre como gerenciar uma rede entre vários centros de dados virtuais, consulte o *Guia do Portal de Tenants do VMware Cloud Director*.

Modificar os metadados de um centro de dados virtual da organização

Você pode adicionar, editar e excluir metadados para um centro de dados virtual da organização.

Ao usar os metadados do objeto, você pode associar os pares `nome= valor` definidos pelo usuário com um centro de dados virtual da organização. Você pode usar os metadados do objeto nas expressões de filtro de consulta da API do vCloud.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Clique na guia **Metadados**.
- 4 Clique em **Editar**.
- 5 (Opcional) Para adicionar um par chave-valor, clique em **Adicionar**, insira um nome e um valor e selecione um tipo para o novo par chave-valor.
- 6 (Opcional) Para editar um par de chave-valor, insira um novo nome e um valor e selecione um novo tipo para o par chave-valor.
- 7 (Opcional) Para remover um par de chave/valor, na extremidade direita da linha, clique no ícone **Excluir**.
- 8 Clique em **Salvar** e em **OK**.

Visualizar os pools de recursos de um centro de dados virtual de organização

Você pode visualizar uma lista dos pools de recursos do vCenter Server que um centro de dados virtual de organização utiliza.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.

- 2 No painel esquerdo, clique em **VDCs de Organização** e, em seguida, clique no nome do data center virtual de organização de destino.
- 3 Clique na guia **Pools de Recursos**.

Resultados

Você pode ver uma tabela com os pools de recursos em uso pelo centro de dados virtual de organização e a instância do vCenter Server à qual cada pool de recursos pertence.

Gerenciamento do firewall distribuído em um centro de dados virtual da organização

Para fornecer segurança de rede de camada 2 e 3 em um centro de dados virtual da organização, você pode ativar e criar regras para o firewall distribuído neste centro de dados virtual da organização. Com as regras do firewall distribuído, você pode proteger o tráfego viajando entre máquinas virtuais em um centro de dados virtual da organização.

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.

Para criar as regras de firewall distribuído, você pode usar vários objetos de agrupamento e grupos de segurança. Consulte [Objetos de agrupamento personalizados](#) e [Trabalhando com grupos de segurança](#).

Para obter informações sobre como proteger o tráfego de e para um edge gateway, consulte [Gerenciando um firewall do edge gateway do NSX Data Center for vSphere](#).

Ativar o firewall distribuído em um centro de dados virtual de organização

Antes de gerenciar as configurações do firewall distribuído em um centro de dados virtual de organização, você deverá ativar o firewall distribuído neste centro de dados virtual de organização.

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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Na guia **Firewall Distribuído > Geral**, ative a opção **Habilitar Firewall Distribuído**.

Resultados

Você pode ver as regras de firewall padrão, que permitem que todo o tráfego da camada 3 e da camada 2 passe pelo centro de dados virtual da organização.

- Na guia **Firewall Distribuído > Geral**, você pode ver a regra de firewall distribuído padrão para o tráfego de camada 3, chamado Regra de Permissão Padrão.
- Na guia **Firewall Distribuído > Ethernet**, você pode ver a regra de firewall distribuído padrão para o tráfego de camada 2, chamado Regra de Permissão Padrão.

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](#)
- 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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 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**.

- 5 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.

- 6 Clique na célula **Nome** e digite um nome.
- 7 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.	Aplicável a regras definidas na guia Geral . 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 any . 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"> ■ Use a janela Selecionar objetos para adicionar objetos que correspondem às suas seleções e clique em Manter para adicioná-los à regra. ■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela Selecionar objetos e selecione o ícone de exclusão de alternância a fim de excluir essa origem dessa regra. 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 Selecionar objetos .

8 Clique na célula **Destino** e execute uma das seguintes ações:

Ação	Descrição
Clique no ícone IP.	Aplicável a regras definidas na guia Geral . 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 any . 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"> ■ Use a janela Selecionar objetos para adicionar objetos que correspondem às suas seleções e clique em Manter para adicioná-los à regra. ■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela Selecionar objetos e, em seguida, selecione o ícone de exclusão de alternância para excluir essa origem dessa regra. 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 Selecionar objetos .

9 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"> Selecione o protocolo de serviço. Digite os números para as portas de origem e de destino ou especifique any e clique em Manter.
Clique no ícone +	Para selecionar um serviço ou um grupo de serviços predefinido ou definir um novo: <ol style="list-style-type: none"> Selecione um ou mais objetos e adicione-os ao filtro. Clique em Manter.

10 Na célula **Ação** da nova regra, configure a ação para a regra.

Opção	Descrição
Permitir	Permite o tráfego de ou para origens, destinos e serviços especificados.
Negar	Bloqueia o tráfego de ou para origens, destinos e serviços especificados.

11 Na célula **Direção** da nova regra, selecione se a regra se aplica a tráfego de entrada, tráfego de saída ou a ambos.

12 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**.

- 13 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.

- 14 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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 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.
- 5 Clique em **Salvar Alterações**.

Objetos de agrupamento personalizados

O software NSX 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**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

- 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

- 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 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**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.


Procedimentos

- 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

- 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 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.

É possível visualizar os serviços disponíveis usando a página **Objetos de Agrupamento**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

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.

É possível visualizar os grupos de serviços disponíveis usando a página **Objetos de Agrupamento**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

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.

Trabalhando com grupos de segurança

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 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.


- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Objetos de Agrupamento > Grupos de Segurança**.

- 5 Clique no botão **Criar** ().

- 6 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.

- 7 (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**.

- 8 (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.

- 9 (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.

- 10 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 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Objetos de Agrupamento > Grupos de Segurança**.
- 5 Selecione o grupo de segurança que você deseja editar.
Os detalhes do grupo de segurança são exibidos abaixo da lista de grupos de segurança.
- 6 (Opcional) Edite o nome e a descrição do grupo de segurança.
- 7 (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**.
- 8 (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**.
- 9 (Opcional) Exclua um conjunto de membros dinâmico clicando no ícone **Excluir** ao lado do conjunto de membros que você deseja excluir.


- 10 (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.
- 11 (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.
- 12 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 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Objetos de Agrupamento > Grupos de Segurança**.
- 5 Selecione o grupo de segurança que você deseja excluir.
- 6 Clique no botão **Excluir** ()
- 7 Para confirmar a exclusão, clique em **OK**.

Resultados

O grupo de segurança é excluído.

Trabalho com marcas de segurança

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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Marcas de Segurança**.
- 5 Clique no botão **Criar** () e insira um nome para a marca de segurança.
- 6 (Opcional) Insira uma descrição para a marca de segurança.

- 7 (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.

- 8 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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Marcas de Segurança**.
- 5 Na lista de marcas de segurança, selecione a marca de segurança que você deseja editar e clique no botão **Editar** ()...
clique no botão **Editar** ()...
- 6 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.

- 7 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.

- 8 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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 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**.
- 5 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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Marcas de Segurança**.
- 5 Na lista de marcas de segurança, selecione a marca de segurança que você deseja editar.
- 6 Clique no botão **Editar** ().
- 7 Edite o nome e a descrição da marca de segurança.
- 8 Atribua a marca ou remova a atribuição das máquinas virtuais que você selecionar.
- 9 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 [Trabalhando com grupos de segurança](#).

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 barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **VDCs de Organização**.
- 3 Clique no botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em **Gerenciar Firewall**.
- 4 Clique na guia **Marcas de Segurança**.
- 5 Na lista de marcas de segurança, selecione a marca de segurança que você deseja excluir.
- 6 Clique no botão **Excluir** ()
- 7 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 [Trabalhando com grupos de segurança](#).

Gerenciando Edge Gateways do NSX Data Center for vSphere

7

Um edge gateway do NSX Data Center for vSphere oferece uma rede de centro de dados virtual roteada da organização 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.

A partir do VMware Cloud Director 9.7, a carga de trabalho de processamento e a carga de trabalho de rede são isoladas usando diferentes pools de recursos e políticas de armazenamento do vSphere. Os edge gateways residem em edge clusters que você deve criar anteriormente. Consulte [Como trabalhar com edge clusters do NSX Data Center for vSphere](#).

Você pode migrar edge gateways legados para os edge clusters correspondentes, reimplantando esses edge gateways. Consulte [Reimplantar um edge gateway](#).

Importante A partir da versão 9.7, o VMware Cloud Director suporta somente edge gateways avançados. Você deve converter qualquer edge gateway não avançado herdado em um gateway avançado. Consulte <https://kb.vmware.com/kb/66767>.

Este capítulo inclui os seguintes tópicos:

- [Como trabalhar com edge clusters do NSX Data Center for vSphere](#)
- [Adicionar um edge gateway do NSX Data Center for vSphere](#)
- [Configurando serviços do edge gateway do NSX Data Center for vSphere](#)
- [Visualizar o uso de redes e as alocações de IP em um edge gateway](#)
- [Edição das propriedades do edge gateway](#)
- [Reimplantar um edge gateway](#)
- [Excluir um edge gateway](#)
- [Estatísticas e logs para um edge gateway](#)
- [Habilitar o acesso pela linha de comando SSH a um edge gateway](#)

Como trabalhar com edge clusters do NSX Data Center for vSphere

Para isolar as cargas de trabalho de processamento das cargas de trabalho de rede, o VMware Cloud Director oferece suporte ao objeto de edge cluster. Um edge cluster consiste em uma política de armazenamento e um pool de recursos do vSphere que são usados somente para edge gateways do VDC de organização. Os centros de dados virtuais do provedor não podem usar recursos dedicados a edge cluster, e os edge clusters não podem usar recursos dedicados a centros de dados virtuais do provedor.

Os edge clusters fornecem um domínio de broadcast L2 dedicado, o que reduz as proliferações de VLAN e garante a segurança e o isolamento da rede. Por exemplo, o edge cluster pode conter VLANs adicionais para emparelhamento com roteadores físicos.

Você pode criar qualquer número de edge cluster. Você pode atribuir um edge cluster a um VDC de organização como um edge cluster primário ou secundário.

- O edge cluster primário para um VDC de organização é usado para o appliance principal do edge de um edge gateway do VDC de organização.
- O edge cluster secundário para um VDC de organização é usado para o appliance do edge em espera quando um edge gateway está no modo HA.

Diferentes VDCs de organização podem compartilhar edge cluster ou podem ter seus próprios edge cluster dedicados.

A partir da versão vCloud Director 9.7, o processo antigo para usar metadados para controlar o posicionamento do edge gateway é obsoleto. Consulte <https://kb.vmware.com/kb/2151398>.

Você pode migrar edge gateways legados para edge cluster recém-criados reimplantando esses edge gateways. Consulte [Reimplantar um edge gateway](#).

Preparando seu ambiente para um edge cluster

- 1 No vSphere, crie o pool de recursos para o edge cluster de destino.

Se um centro de dados virtual da organização estiver usando um pool de redes VLAN, o pool de redes VLAN e o edge cluster para esse centro de dados virtual da organização deverão residir no mesmo switch distribuído do vSphere.

- 2 Se um centro de dados virtual da organização estiver usando um pool de redes VXLAN, no NSX, adicione o edge cluster à zona de transporte VXLAN, após o qual sincronizar o pool de redes VXLAN no VMware Cloud Director.

- 3 No vSphere, crie o perfil de armazenamento do edge cluster.

Criando e gerenciando edge clusters

Depois de preparar seu ambiente, para criar e gerenciar edge clusters, você deve usar os métodos de `EdgeClusters` do OpenAPI do VMware Cloud Director. Consulte *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

A visualização de edge clusters requer o direito de **Exibição do Edge Cluster**. A criação, a atualização e a exclusão de edge clusters exigem o direito de **Gerenciamento do Edge Cluster**.

Ao criar um edge cluster, especifique o nome, o pool de recursos do vSphere e o nome do perfil de armazenamento.

Depois de criar um edge cluster, você pode modificar seu nome e descrição. Depois de excluir ou mover seus edge gateways, você pode excluir um edge cluster.

Atribuindo um edge cluster a um VDC de organização

Depois de criar um edge cluster, você pode atribuir esse edge cluster a um VDC de organização atualizando o perfil de rede do VDC de organização. Você pode atribuir um edge cluster a um VDC de organização como um edge cluster primário ou secundário.

Se você não atribuir um edge cluster secundário, o appliance do edge em espera de um edge gateway no modo HA será implantado no edge cluster primário, mas em um host diferente do host que executa o appliance do edge primário.

Para atualizar, exibir e excluir perfis de rede de VDC de organização, você deve usar os métodos VMware Cloud Director do OpenAPI do `VdcNetworkProfile`. Consulte *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

Considerações:

- Os edge clusters primário e secundário devem residir no mesmo switch distribuído do vSphere.
- Se o VDC de organização usar um pool de redes VXLAN, a zona de transporte do NSX deverá abranger os edge clusters e de processamento.
- Se o VDC de organização usar um pool de redes VLAN, os edge clusters e os clusters de processamento deverão estar no mesmo switch distribuído do vSphere.

Se você atualizar novamente o edge cluster primário ou secundário de um VDC de organização, para mover um edge gateway existente para o novo cluster, deverá reimplantar esse edge gateway. Consulte [Reimplantar um edge gateway](#).

Adicionar um edge gateway do NSX Data Center for vSphere

Um edge gateway do NSX Data Center for vSphere oferece uma rede de VDC 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.

A partir do VMware Cloud Director 9.7, os edge gateways do NSX Data Center for vSphere são implantados em edge clusters criados anteriormente e atribuídos ao VDC de organização.

Você pode adicionar um edge gateway IPv4 ou IPv6 que se conecta a uma ou mais redes externas.

Observação Os gateways de borda IPv6 fornecem suporte aos serviços limitados. Os edge gateways IPv6 oferecem suporte aos firewalls de borda, firewalls distribuídos e ao roteamento estático.

Pré-requisitos

- Para obter informações sobre os requisitos do sistema para implantar um edge gateway do NSX Data Center for vSphere, consulte o *Guia de Administração do NSX*.
- Se você quiser implantar o edge gateway em um edge cluster dedicado, crie e atribua um edge cluster ao centro de dados virtual da organização. Consulte [Como trabalhar com edge clusters do NSX Data Center for vSphere](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e em **Novo**.
- 3 Selecione o centro de dados virtual de organização com suporte no NSX-V no qual você deseja criar o edge gateway e clique em **Avançar**.
- 4 Digite um nome e, opcionalmente, uma descrição para o novo edge gateway.
- 5 Ative ou desative cada uma das configurações gerais do edge gateway conforme desejar.

Configuração geral	Descrição
Roteamento Distribuído	Configura o edge gateway para fornecer roteamento lógico distribuído.
Modo FIPS	Configura o edge gateway para usar o modo NSX FIPS.
Alta Disponibilidade	Permite o failover automático para um edge gateway de backup.

- 6 Selecione a configuração do edge gateway para os recursos do sistema e clique em **Avançar**.

Configuração	Descrição
Compactar	Requer menos memória e menos recursos de computação.
Grande	Fornecer maior capacidade e desempenho do que a configuração Compacta. Configurações grandes e extragrandes fornecem funções de segurança idênticas.
Extragrande	Usado para ambientes que possuem um balanceador de carga com um grande número de sessões simultâneas.
Quádruplo	Usado para ambientes com alta taxa de transferência. Requer uma alta taxa de conexão.

- 7 Selecione uma ou mais sub-redes das redes externas às quais o edge gateway pode se conectar e clique em **Avançar**.

Se você tiver atribuído um edge cluster ao VDC de organização, a lista exibida conterá as redes externas acessíveis a esse edge cluster.

- 8 (Opcional) Configure uma rede como o gateway padrão.
 - a Ative a opção **Configurar gateway padrão**.
 - b Clique no botão de opção ao lado do nome da rede externa de destino e clique no botão de opção ao lado do endereço IP de destino.
 - c (Opcional) Ative a opção **Usar gateway padrão para retransmissão de DNS**.
- 9 Clique em **Avançar**.
- 10 Ative ou deixe desativadas essas configurações avançadas do edge gateway e clique em **Avançar**.

Configuração avançada	Descrição
Configurações de IP	Você pode inserir manualmente um endereço IP para cada sub-rede no edge gateway.
Subalocar Pools de IPs	Você pode subalocar vários pools de IPs estáticos dos pools de IPs disponíveis de cada rede externa no edge gateway.
Limites de Taxa	Você pode configurar os limites de taxa de entrada e saída para cada rede externa no edge gateway.

- 11 (Opcional) Se você tiver ativado uma ou mais configurações avançadas na [Etapa 10](#), defina todas as configurações habilitadas.

Configuração avançada	Etapas
Configurações de IP	<p>Para cada rede no edge gateway, na célula Endereços IP, insira um endereço IP e clique em Avançar.</p> <p>Se você não inserir um endereço IP para uma rede, o sistema atribuirá um endereço IP arbitrário a essa rede.</p>
Subalocar Pools de IPs	<ol style="list-style-type: none"> 1 Clique no botão de seleção ao lado do nome de uma rede externa e clique em Editar. Você pode ver os pools de IPs disponíveis para esta rede externa e os pools de IPs atuais de subalocados, se configurados. 2 Edite os pools de IPs subalocados para esta rede externa e clique em Salvar. Você pode adicionar endereços IP e intervalos dos pools de IPs disponíveis. 3 Clique em Salvar. O sistema combina intervalos de IP sobrepostos. 4 Clique em Avançar. <p>Observação A alocação de endereços IP para um edge gateway é um processo no qual o provedor atribui propriedade de endereços IP ao gateway. O VMware Cloud Director configura automaticamente a interface de gateway apropriada com os endereços secundários durante o processo de alocação. Se qualquer um dos endereços IP for usado fora do VMware Cloud Director, isso poderá causar conflitos de endereço IP.</p>
Limites de taxa	<p>Para cada rede externa no edge gateway, ative a opção Habilitar, insira os limites nas células Taxa de Entrada e Taxas de Saída e clique em Avançar.</p>

- 12 Revise a página **Pronto para ser Concluído** e clique em **Concluir**.

Configurando serviços do edge gateway do NSX Data Center for vSphere

Você pode configurar serviços como DHCP, firewall, conversão de endereços de rede (NAT) e VPN em um edge gateway.

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 do firewall distribuído em um centro de dados virtual da organização](#).

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.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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 any . 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"> ■ Use a janela Selecionar objetos para adicionar objetos que correspondem às suas seleções e clique em Manter para adicioná-los à regra. ■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela Selecionar objetos e selecione o ícone de exclusão de alternância a fim de excluir essa origem dessa regra. <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 Selecionar objetos.</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 any . 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"> ■ Use a janela Selecionar objetos para adicionar objetos que correspondem às suas seleções e clique em Manter para adicioná-los à regra. ■ Para excluir uma origem da regra, adicione-a a essa regra usando a janela Selecionar objetos e, em seguida, selecione o ícone de exclusão de alternância para excluir essa origem dessa regra. <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 Selecionar objetos.</p>

- 7 Clique na célula **Serviço** da nova regra e clique no ícone **+** para especificar o serviço como uma combinação de porta-protocolo:
 - a Selecione o protocolo de serviço.
 - b Digite os números de porta para as portas de origem e de destino ou especifique **qualquer**.
 - c Clique em **Manter**.
- 8 Na célula **Ação** da nova regra, configure a ação para a regra.

Opção	Descrição
Aceitar	Permite o tráfego de ou para origens, destinos e serviços especificados.
Negar	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

- 1 Abra Serviços de Edge Gateway.
 - a Na barra de navegação superior, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.
- 2 Clique na guia **Firewall**.
- 3 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.

4 Clique em **Salvar alterações**.

Aplicar as configurações do servidor de syslog a um edge gateway do NSX Data Center for vSphere

Se você tiver ativado o log para uma ou mais regras de firewall de edge gateway, o gateway de borda se conectará ao servidor de syslog. Se você tiver criado um edge gateway antes da configuração inicial do servidor de syslog ou tiver alterado as configurações do servidor de syslog, deverá sincronizar as configurações do servidor de syslog para esse edge gateway.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no botão de seleção ao lado do nome do edge gateway de destino e clique em **Sincronizar syslog**.
- 4 Para confirmar, clique em **OK**.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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 Servidor de Nome Primário e o Servidor de Nome Secundário serão definidos para Automático .
Servidor de Nome Primário	Quando você não ativar a opção Configurar DNS Automaticamente , 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 Configurar DNS Automaticamente , 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.
Lease Nunca Expira	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 Tempo de Lease fica definido como infinito.
Tempo de Lease (Segundos)	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). Observação Não é possível especificar um tempo de lease quando você seleciona Lease Nunca Expira .

- 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.
- 2 Na guia **DHCP > Vinculações**, clique no botão **Criar** () , especifique os detalhes da associação e clique em **Manter**.

Opção	Descrição
Endereço MAC	Digite o endereço MAC da máquina virtual que você deseja vincular ao endereço IP.
Nome do Host	Digite o nome do host que deseja definir para essa máquina virtual quando a máquina virtual solicitar uma concessão de DHCP.
Endereço IP	Digite o endereço IP que você deseja vincular ao endereço MAC.
Máscara de Sub-Rede	Digite a máscara de sub-rede da interface do edge gateway.
Nome de Domínio	Digite o nome do domínio do servidor DNS.
Configurar DNS Automaticamente	Ative esta opção para usar a configuração do serviço DNS para esta vinculação de DNS. Se ativados, o Servidor de Nome Primário e o Servidor de Nome Secundário serão definidos para Automático .
Servidor de Nome Primário	Quando você não selecionar a opção Configurar DNS Automaticamente , 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 selecionar a opção Configurar DNS Automaticamente , 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.

Opção	Descrição
Lease Nunca Expira	Ative essa opção para manter o endereço IP vinculado a esse endereço MAC para sempre. Quando você seleciona essa opção, o Tempo de Lease fica definido como infinito.
Tempo de Lease (Segundos)	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). Observação Não é possível especificar um tempo de lease quando você seleciona Lease Nunca Expira .

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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**.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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 Qualquer .
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 Protocolo está definido como ICMP ou Qualquer .
Tipo de ICMP	Quando você selecionar ICMP (um relatório de erros e um utilitário de diagnóstico usado entre dispositivos para comunicar informações de erro) para o Protocolo , selecione o Tipo de ICMP 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.
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 avançado

Você pode configurar os recursos de roteamento estático e dinâmico fornecidos pelo software do NSX para 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 fornece, consulte *Roteamento* na documentação de *Administração do NSX*.

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 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Ativar Reinicialização Normal	Especifica que o encaminhamento de pacotes deve permanecer sem interrupção quando os serviços OSPF forem reiniciados.
Ativar Origem Padrão	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 Normal ou NSSA.</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"> ■ Nenhuma <p>Nenhuma autenticação é necessária.</p> ■ Senha <p>Com essa opção, a senha especificada no campo Valor de autenticação de área é incluída no pacote transmitido.</p> ■ MD5 <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 Valor de autenticação de área.</p>

- 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** () , 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
Intervalo de Saudação	Intervalo (em segundos) entre os pacotes de saudação enviados na interface.
Intervalo de Encerramento	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.
Prioridade	Prioridade da interface. A interface com a prioridade mais alta é o roteador de edge gateway designado.
Custo	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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Ativar Reinicialização Normal	Especifica que o encaminhamento de pacotes deve permanecer sem interrupção quando os serviços BGP forem reiniciados.
Ativar Origem Padrão	Permite que o edge gateway se anuncie como um gateway padrão para seus vizinhos BGP.
AS Local	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
Endereço IP	Digite o endereço IP de um vizinho BGP para este edge gateway.
AS Remoto	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.
Peso	O peso padrão para a conexão vizinha. Ajuste conforme apropriado para as necessidades da sua organização.

Opção	Descrição
Tempo de Keep Alive	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.
Tempo de Pressionamento	<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>
Senha	<p>Se esse vizinho BGP exigir autenticação, digite a senha de autenticação. 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>
Filtros BGP	<p>Use esta tabela para especificar a filtragem de rota usando uma lista de prefixos desse vizinho BGP.</p> <p>Cuidado Uma regra de bloquear todos é aplicada no final dos filtros.</p> <p>Adicione um filtro à tabela clicando no ícone + e configurando as opções. Clique em Manter para salvar cada filtro.</p> <ul style="list-style-type: none"> ■ Selecione a direção para indicar se você está filtrando o tráfego de ou para o vizinho. ■ Selecione a ação para indicar se você está permitindo ou negando o tráfego. ■ Digite a rede que você deseja filtrar para ou a partir do vizinho. Digite <code>ANY</code> ou uma rede em um formato CIDR. ■ Digite o GE de Prefixo do IP e o LE de Prefixo do IP para usar as palavras-chave <code>le</code> e <code>ge</code> na lista de prefixos de IP.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Nome do Prefixo	Selecione um prefixo de IP específico ao qual aplicar esses critérios ou selecione Qualquer para aplicar os critérios a todas as rotas de rede.
Protocolo do Aluno	Selecione o protocolo que deve aprender rotas de outros protocolos sob esses critérios de redistribuição.
Permitir aprendizado de	Selecione os tipos de rede dos quais rotas podem ser aprendidas para o protocolo selecionado na lista Protocolo do Aluno .
Ação	Selecione se deseja permitir ou negar a redistribuição dos tipos de redes selecionados.

- 6 Clique em **Salvar alterações**.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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 Aceleração Habilitada 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>Observação 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.
- 2 Navegue até **Balanceador 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
Tipo	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.
Permitir Passagem SSL	Clique para habilitar que a autenticação SSL seja transmitida ao servidor virtual. Caso contrário, a autenticação SSL ocorrerá no endereço de destino.
URL de Redirecionamento HTTP	(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"> ■ IP de Origem <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> ■ MSRDP <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> ■ ID da Sessão SSL <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>
Nome do Cookie	<p>(HTTP e HTTPS) Se você especificou Cookie 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"> ■ Inserir <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> ■ Prefixo <p>Selecione essa opção quando o cliente não oferecer suporte a mais de um cookie.</p> <p>Observação 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> ■ Sessão do Aplicativo 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.
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>Observação 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 Insert X-Forwarded-For HTTP 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>Observação 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 Ativar SSL no Lado do Pool 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
Certificados de Servidor Virtual	Selecione o certificado, as CAs ou as CRLs usadas para descriptografar o tráfego HTTPS.
Certificados de Pool	Defina o certificado, as CAs ou as CRLs usadas para autenticar o balanceador de carga no lado do servidor. Observação Selecione Habilitar SSL no Lado do Pool para ativar essa guia.
Codificação	Selecione os algoritmos de codificação (ou o pacote de codificação) negociados durante o handshake SSL/TLS.
Autenticação de Cliente	Especifique se a autenticação do cliente deve ser ignorada ou se é necessária. Observação Quando definido como Obrigatório , 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - No painel esquerdo, clique em **Edge Gateways**.
 - Clique no botão de opção ao lado do nome do edge gateway de destino 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 Método 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 Método 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 Novo Monitor de Serviço 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. Observação Ao selecionar o método POST, você deve especificar um valor para Enviar .
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. Observação Quando Esperado não corresponde, o monitor não tenta corresponder o conteúdo Receber .
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><extension>delay=2 critical=3 escape</extension></pre>

6 Para preservar as alterações, clique em **Manter**.

Exemplo: Extensões com suporte para cada protocolo**Tabela 7-1. 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. Observação 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 7-2. 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 7-3. 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
ROUND-ROBIN	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.
IP-HASH	Selecione um servidor com base em um hash do endereço IP de origem e de destino de cada pacote.
LEASTCONN	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.
URI	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=<name></code> . Por exemplo, você pode usar host 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=<url></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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Ativar Servidor Virtual	Clique para ativar o servidor virtual.
Ativar Aceleração	Clique para ativar a aceleração.
Perfil de Aplicativo	Selecione um perfil de aplicativo a ser associado ao servidor virtual.
Nome	Digite um nome para o servidor virtual.
Descrição	Digite uma descrição opcional para o servidor virtual.
Endereço IP	Digite ou procure para selecionar o endereço IP que o balanceador de carga detecta.
Protocolo	Selecione o protocolo que o servidor virtual aceita. Você deve selecionar o mesmo protocolo usado pelo Perfil de Aplicativo selecionado.
Porta	Digite o número da porta que o balanceador de carga escuta.
Pool Padrão	Escolha o pool de servidores que o balanceador de carga vai usar.
Limite de Conexão	(Opcional) Digite o máximo de conexões simultâneas que o servidor virtual pode processar.
Limite de Taxa de Conexão (CPS)	(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](#)

Proteger o acesso usando redes virtuais privadas

Você pode configurar os recursos de VPN fornecidos pelo software NSX para 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 certificados SSL](#).

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Intervalo de IPs	Insira um intervalo de endereços IP para este pool de IPs, como 127.0.0.1-127.0.0.9.. Esses endereços IP serão atribuídos aos clientes VPN quando eles autenticarem e se conectarem ao túnel VPN SSL.
Máscara de Rede	Insira a máscara de rede do pool de IPs, como 255.255.255.0.
Gateway	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 Intervalo de IPs.
Descrição	(Opcional) Insira uma descrição para este pool de IPs.
Status	Selecione se deseja ativar ou desativar este pool de IPs.
DNS Primário	(Opcional) Insira o nome do servidor DNS primário que será usado para a resolução de nomes desses endereços IP virtuais.
DNS Secundário	(Opcional) Insira o nome do servidor DNS secundário a ser usado.
Sufixo DNS	(Opcional) Insira o sufixo DNS para o domínio no qual os sistemas cliente estão hospedados, para resolução de nome de host baseada em domínio.
Servidor WINS	(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 192169.1.0/24 .
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"> ■ Pelo Túnel O cliente VPN envia a rede privada e o tráfego de Internet por meio do edge gateway ativado para SSL VPN-Plus. ■ Ignorar Túnel O cliente VPN ignora o edge gateway e envia o tráfego diretamente para o servidor privado.

Opção	Ação
Ativar Otimização de TCP	<p>(Opcional) Para otimizar a velocidade da Internet, ao selecionar Pelo Túnel para enviar o tráfego, você também deve selecionar Ativar Otimização de TCP.</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 Ativar Otimização de TCP elimina o risco de esse problema ocorrer.</p> <hr/> <p>Observação Quando você ativa a otimização de TCP:</p> <ul style="list-style-type: none"> ■ Você deve inserir os números de porta para otimizar o tráfego de Internet. ■ 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. <hr/>
Portas	<p>Quando você selecionar Pelo Túnel, digite um intervalo de números de porta que deseja abrir para o usuário remoto acessar os servidores internos, como 20–21, para o tráfego de FTP, e 80–81, para o tráfego HTTP.</p> <p>Para conceder acesso irrestrito aos usuários, deixe o campo em branco.</p> <hr/>
Status	<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
Ativar política de senha	Ative a aplicação das configurações de política de senha que você configurar aqui.
Tamanho da Senha	Insira o número mínimo e máximo de caracteres permitidos para a senha.
Nº mínimo de letras	(Opcional) Digite o número mínimo de caracteres alfabéticos necessários na senha.
Nº mínimo de dígitos	(Opcional) Digite o número mínimo de caracteres numéricos necessários na senha.
Nº mínimo de caracteres especiais	(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.
Senha não deve conter a ID de usuário	(Opcional) Ative esta opção para que a senha não contenha a ID de usuário.
Senha expira em	(Opcional) Digite o número máximo de dias que uma senha pode existir antes de o usuário ter de alterá-la.
Notificação de expiração em	(Opcional) Digite o número de dias antes da expiração da senha em Senha expira em 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
Ativar política de bloqueio de conta	Ative a aplicação das configurações de política de bloqueio de conta que você configurar aqui.
Contagem de Tentativas	Insira o número de vezes que um usuário pode tentar acessar sua conta.
Duração da Nova Tentativa	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 Contagem de Tentativas como 5 e Duração da Nova Tentativa como 1 minuto, a conta do usuário será bloqueada após cinco tentativas de login malsucedidas dentro de um minuto.
Duração do Bloqueio	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 Adicionar () 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
Impedir vários logins com o mesmo nome de usuário	Ative para restringir um usuário remoto a ter apenas uma sessão de login ativa com o mesmo nome de usuário.
Compactação	Ative para habilitar a compactação inteligente de dados baseada em TCP e melhorar a velocidade de transferência de dados.
Ativar Log	Ative para manter um log do tráfego que passa pelo gateway VPN SSL. O registro em log está habilitado por padrão.
Forçar teclado virtual	Ative para exigir que os usuários remotos usem um teclado virtual (na tela) apenas para inserir informações de login.
Tornar aleatórias as chaves do teclado virtual	Ative para que o teclado virtual use um layout de teclas aleatório.
Tempo limite de sessão ociosa	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.
Notificação do usuário	Digite a mensagem a ser exibida aos usuários remotos após o login.
Ativar acesso à URL pública	Ative para permitir que usuários remotos acessem sites que não estão explicitamente configurados por você para acesso remoto de usuários.
Ativar tempo limite forçado	Ative para que o sistema desconecte usuários remotos após o período de tempo especificado no campo Tempo limite forçado .
Tempo limite forçado	Digite o período de tempo limite em minutos. Este campo é exibido quando o botão de alternância Ativar tempo limite forçado 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
- b No painel esquerdo, clique em **Edge Gateways**.
- c Clique no botão de opção ao lado do nome do edge gateway de destino 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

- 1 Na guia **VPN IPsec**, clique em **Sites VPN IPsec**.
- 2 Clique no botão **Adicionar** ()
- 3 Defina as configurações de conexões de VPN IPsec.

Opção	Ação
Ativado	Habilite essa conexão entre os dois endpoints de VPN.
Ativar Perfect Forward Secrecy (PFS)	<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>Importante 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>
Nome	(Opcional) Insira um nome para a conexão.
ID Local	<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>
Endpoint Local	<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>
Sub-Redes Locais	<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, 192.168.99.0/24.</p>

Opção	Ação
ID de Peer	<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>
Endpoint de Peer	<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>Observação Quando a NAT estiver configurada para o peer, insira o endereço IP público que o dispositivo usa para a NAT.</p>
Sub-Redes de Peer	<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, 192.168.99.0/24.</p>
Algoritmo de Criptografia	<p>Selecione o tipo de algoritmo de criptografia no menu suspenso.</p> <p>Observação O tipo de criptografia selecionado deve corresponder ao tipo de criptografia configurado no dispositivo de VPN do site remoto.</p>
Autenticação	<p>Selecione uma autenticação. As opções são:</p> <ul style="list-style-type: none"> ■ PSK <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> ■ Certificado <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 Configuração Global da guia VPN IPsec.</p>
Alterar Chave Compartilhada	<p>(Opcional) Ao atualizar as configurações de uma conexão existente, você pode ativar essa opção para tornar o campo Chave Pré-compartilhada disponível e, assim, poder atualizar a chave compartilhada.</p>
Chave Pré-Compartilhada	<p>Se você selecionou PSK como tipo de autenticação, digite uma cadeia de caracteres de segredo alfanumérica, que pode ter um comprimento máximo de 128 bytes.</p> <p>Observação 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>
Exibir Chave Compartilhada	<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>Observação 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"> ■ <code>securelocaltrafficbyip=IPAddress</code> para redirecionar o tráfego local do edge gateway pelo túnel de VPN IPsec. <p>Esse é o valor padrão.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code> para oferecer suporte a sub-redes sobrepostas.

4 Clique em **Manter**.

5 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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](#).

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.

Procedimentos

1 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**.

2 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.

3 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.

4 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.

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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.

- 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 Alterar o certificado do servidor para selecionar o certificado a ser vinculado ao servidor VPN L2. Na janela Alterar certificado do servidor , ative Validar certificado do servidor , selecione um certificado do servidor na lista e clique em OK .

- Para configurar os sites pares, clique na guia **Sites do servidor**.

- Clique no botão **Adicionar** ().

- 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	
Interfaces Estendidas	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.
Endereço do Gateway de Otimização de Saída	(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.

- Clique em **Manter**.
- 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
Endereço do Servidor	Insira o endereço IP do servidor VPN L2 ao qual este cliente deve ser conectado.
Porta do Servidor	Insira a porta do servidor VPN L2 à qual o cliente deve se conectar. A porta padrão é 443.
Algoritmo de Criptografia	Selecione o algoritmo de criptografia para comunicação com o servidor.
Interfaces Estendidas	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.
Endereço do Gateway de Otimização de Saída	(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.
Detalhes do Usuário	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
Ativar Proxy Seguro	Selecione para habilitar o proxy seguro.
Endereço	Insira o endereço IP do servidor proxy.
Porta	Insira a porta do servidor proxy.
Nome de Usuário	Insira as credenciais de autenticação do servidor proxy.
Senha	

- 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 certificados SSL

O software NSX 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 (SACs), 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.
- 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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
Nome Comum	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.
Unidade Organizacional	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.
Nome da Organização	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.
Localidade	Insira a cidade ou localidade na qual sua empresa está legalmente registrada.
Nome do Estado ou Província	Insira o nome completo (não use abreviação) do estado, da província, da região ou do território no qual sua empresa está legalmente registrada.
Código do País	Insira o nome do país no qual sua empresa está legalmente registrada.

Opção	Descrição
Algoritmo de Private Key	<p>Insira o tipo de chave, RSA ou DSA, para o certificado.</p> <p>A RSA normalmente é usada. O tipo de chave define o algoritmo de criptografia para a comunicação entre os hosts. Quando o modo FIPS está ativo, os tamanhos de chaves RSA devem ser superiores ou iguais a 2048 bits.</p> <hr/> <p>Observação O SSL VPN-Plus só é compatível com certificados RSA.</p>
Tamanho da Chave	<p>Insira o tamanho da chave em bits.</p> <p>O mínimo é de 2048 bits.</p>
Descrição	(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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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

O software NSX 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**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ul style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

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.

- 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**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.


Procedimentos

- Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ol style="list-style-type: none"> Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. No painel esquerdo, clique em VDCs de Organização. Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ol style="list-style-type: none"> Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. No painel esquerdo, clique em Edge Gateways. Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. Clique na guia Objetos de Agrupamento.

- Clique na guia **Conjuntos de MACs**.

Os conjuntos de MACs já definidos são exibidos na tela.

- Para adicionar um conjunto de MACs, clique no botão **Criar** ().
- Digite um nome para o conjunto e, opcionalmente, uma descrição, bem como os endereços MAC a serem incluídos nele.
- 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.

É possível visualizar os serviços disponíveis usando a página **Objetos de Agrupamento**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

- 1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em VDCs de Organização. c Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. d Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ol style="list-style-type: none"> a Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. b No painel esquerdo, clique em Edge Gateways. c Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. d Clique na guia Objetos de Agrupamento.

- 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.

É possível visualizar os grupos de serviços disponíveis usando a página **Objetos de Agrupamento**. Para abrir esta página, você deve navegar para as configurações de firewall distribuído do VDC de organização ou para as configurações de serviços de um edge gateway que pertença ao VDC de organização.

Procedimentos

1 Abra a página **Objetos de Agrupamento**.

Opção	Ação
Nas configurações de firewall distribuído do VDC da organização	<ol style="list-style-type: none"> Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. No painel esquerdo, clique em VDCs de Organização. Selecione o botão de opção ao lado do nome do centro de dados virtual da organização de destino e clique em Gerenciar Firewall. Clique na guia Objetos de Agrupamento.
Nas configurações de serviços de um edge gateway no VDC da organização	<ol style="list-style-type: none"> Na barra de navegação superior, em Recursos, selecione Recursos de Nuvem. No painel esquerdo, clique em Edge Gateways. Selecione o botão de opção ao lado do nome de um gateway de borda que pertence ao centro de dados virtual da organização de destino e clique em Serviços. Clique na guia Objetos de Agrupamento.

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.

Visualizar o uso de redes e as alocações de IP em um edge gateway

Você pode visualizar as redes em um edge gateway com informações sobre o uso de pools de IPs e sub-redes. Também pode visualizar o endereço IP alocado a cada rede.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Para exibir as redes externas com informações sobre o uso de pools de IPs e sub-redes, clique na guia **Redes Externas > Redes e sub-redes**.
- 4 Para exibir as redes externas com informações sobre seus endereços IP e categorias, clique na guia **Redes Externas > Alocações de IP**.

Edição das propriedades do edge gateway

Ativar ou desativar o roteamento distribuído em um edge gateway

Depois de ativar o roteamento distribuído do VMware Cloud Director em um edge gateway, o administrador da organização poderá criar várias redes de centros de dados virtuais da organização roteadas com interfaces distribuídas conectadas a esse edge gateway. O tráfego nessas redes é otimizado para comunicação de VM-para-VM.

Pré-requisitos

A instância do NSX Manager de suporte é configurada com um cluster do NSX Controller. Consulte o *Guia de Administração do NSX*.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Selecione o botão de opção ao lado do nome do edge gateway de destino e clique em **Habilitar roteamento distribuído** ou **Desabilitar roteamento distribuído**.
- 4 Para confirmar, clique em **OK**.

Modificar as configurações de redes externas e do edge gateway

Para modificar as configurações de redes externas e de edge gateway, você pode usar o assistente **Editar edge gateway**, que contém as mesmas páginas do assistente que você usou para criar o edge gateway.

Você pode modificar as configurações que definiu ao adicionar o edge gateway. Consulte [Adicionar um edge gateway do NSX Data Center for vSphere](#).

Para modificar a configuração de roteamento distribuído, consulte [Ativar ou desativar o roteamento distribuído em um edge gateway](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no botão de opção ao lado do nome do edge gateway que você deseja modificar e clique em **Editar**.
- 4 Para modificar as configurações do edge gateway, passe pelas páginas do assistente **Editar o edge gateway** clicando em **Próximo** e, na página **Pronto para ser Concluído**, clique em **Concluir**.

Editar as configurações gerais de um edge gateway

Você pode modificar o nome e a descrição de um edge gateway, ativar ou desativar o modo FIPS e o estado de alta disponibilidade e alterar a configuração do tamanho do edge gateway.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Na guia **Geral**, no canto superior direito, clique em **Editar**.
- 4 (Opcional) Edite o nome e a descrição do edge gateway.
- 5 (Opcional) Ative ou desative as configurações gerais de cada edge gateway.

Configuração geral	Descrição
Modo FIPS	Configura o edge gateway para usar o modo NSX FIPS.
Alta Disponibilidade	Permite o failover automático para um edge gateway de backup.

- 6 (Opcional) Altere a configuração do edge gateway para os recursos do sistema.

Configuração	Descrição
Compactar	Requer menos memória e menos recursos de computação.
Grande	Fornece maior capacidade e desempenho do que a configuração Compacta. Configurações grandes e extragrandes fornecem funções de segurança idênticas.
Extragrande	Usado para ambientes que possuem um balanceador de carga com um grande número de sessões simultâneas.
Quádruplo	Usado para ambientes com alta taxa de transferência. Requer uma alta taxa de conexão.

- 7 Para confirmar as alterações, clique em **Salvar**.

Editar o gateway padrão de um edge gateway

Você pode alterar a rede que um edge gateway usa como um gateway padrão.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Na guia **Redes Externas > Gateway padrão**, no canto superior direito, clique em **Editar**.
- 4 (Opcional) Configure uma rede como o gateway padrão.
 - a Ative a opção **Configurar gateway padrão**.
 - b Selecione o botão de opção ao lado do nome da rede externa de destino e selecione o botão de opção ao lado do endereço IP de destino.
 - c (Opcional) Ative a opção **Usar gateway padrão para retransmissão de DNS**.
- 5 Para confirmar as alterações, clique em **Salvar**.

Editar as configurações de IP de um edge gateway

Você pode modificar as configurações de IP para redes externas em um edge gateway.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Na guia **Redes Externas > Configurações de IP**, clique em **Editar**.
- 4 Para cada rede no edge gateway, na célula **Endereços IP**, insira um endereço IP ou deixe a célula em branco.

Se você não inserir um endereço IP para uma rede, o sistema atribuirá um endereço IP arbitrário a essa rede.

- 5 Para confirmar as alterações, clique em **Salvar**.

Editar os pools de IPs subalocados em um edge gateway

Você pode subalocar vários pools de IPs estáticos dos pools de IPs disponíveis de uma rede externa em um edge gateway.

Observação A alocação de endereços IP para um edge gateway por meio da subalocação é um processo no qual o provedor atribui propriedade de endereços IP ao gateway. O VMware Cloud Director configura automaticamente a interface de gateway apropriada com os endereços secundários durante o processo de subalocação, o que poderá causar conflitos de endereço IP se qualquer um dos endereços IP for usado fora do VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Clique na guia **Redes Externas > Pools de IPs Subalocados**.

Você pode ver os pools de IPs atuais de subalocados para cada rede externa neste edge gateway.

- 4 Clique no botão de seleção ao lado do nome de uma rede externa e clique em **Editar**.
Você pode ver os pools de IPs disponíveis para esta rede externa e os pools de IPs atuais de subalocados, se configurados.
- 5 Edite os pools de IPs subalocados para esta rede externa e clique em **Salvar**.

É possível adicionar, modificar e remover endereços IP e intervalos dos pools de IPs disponíveis.

Resultados

O sistema combina intervalos de IP sobrepostos.

Editar os limites de taxa em um edge gateway

Você pode configurar os limites de taxa de entrada e saída para cada rede externa no edge gateway.

Os limites de taxa se aplicam apenas a redes externas suportadas por grupos de portas distribuídas com associação estática.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 3 Na guia **Limites de taxa > Redes externas**, no canto superior direito, clique em **Editar**.

Você pode ver os limites de taxa atuais para cada rede externa neste edge gateway.

- 4 Edite os limites de taxa e clique em **Salvar**.

Para cada rede externa no edge gateway, você pode ativar ou desativar os limites de taxa e alterar as taxas de entrada e saída.

Reimplantar um edge gateway

Você pode excluir e implantar um novo appliance de edge gateway com as configurações mais recentes.

Se os serviços de edge não estiverem funcionando conforme o esperado, você poderá reimplantar o dispositivo do edge gateway.

Quando você reimplanta um edge gateway, o VMware Cloud Director o exclui e o recria com as configurações mais recentes.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Reimplantar**.
- 4 Para confirmar, clique em **OK**.

Resultados

A máquina virtual do edge gateway é substituída por uma nova máquina virtual, e todos os serviços são restaurados.

Excluir um edge gateway

Você pode remover um edge gateway do centro de dados virtual da organização.

Pré-requisitos

Exclua todas as redes de centros de dados virtuais da organização que usam o edge gateway de destino.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **Excluir**.

Estatísticas e logs para um edge gateway

Você pode visualizar estatísticas e logs para um edge gateway.

Visualizar estatísticas

Você pode visualizar as estatísticas na tela **Serviços do Edge Gateway**.

Procedimentos

- 1 Abra Serviços de Edge Gateway.
 - a Na barra de navegação superior, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.
- 2 Clique na guia **Estatísticas**.
- 3 Navegue pelas guias dependendo do tipo de estatística que deseja ver.

Opção	Descrição
Conexões	A tela Conexões fornece visibilidade operacional. A tela exibe gráficos para o tráfego que flui pelas interfaces do edge gateway selecionado e estatísticas de conexão para os serviços do balanceador de carga e do firewall. Selecione o período cujas estatísticas deseja visualizar.
VPN IPsec	A tela VPN IPsec exibe o status e as estatísticas da VPN IPsec, bem como o status e as estatísticas de cada túnel.
VPN L2	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

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

Procedimentos

1 Abra Serviços de Edge Gateway.

- a Na barra de navegação superior, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
- b No painel esquerdo, clique em **Edge Gateways**.
- c Clique no botão de opção ao lado do nome do edge gateway de destino 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.

Habilitar o acesso pela linha de comando SSH a um edge gateway

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, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino 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 admin .
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.

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.

Este capítulo inclui os seguintes tópicos:

- Redes externas dedicadas
- Adicionar um edge gateway do NSX-T Data Center
- Adicionar um conjunto de IPs a um edge gateway do NSX-T Data Center
- Adicionar uma regra de firewall do edge gateway do NSX-T Data Center
- Adicionar uma regra de SNAT ou DNAT a um edge gateway do NSX-T
- Configurar um serviço de encaminhador de DNS em um edge gateway do NSX-T
- Editar as alocações de IP de um edge gateway do NSX-T
- Alocação de IPs rápida
- Criar perfis de portas de aplicativos personalizados
- VPN baseada em políticas IPsec para edge gateways do NSX-T Data Center
- Configurar serviços de rede externa dedicada
- Gerenciamento de balanceamento de carga avançado do NSX em um edge gateway do NSX-T Data Center

Redes externas dedicadas

Para fornecer uma topologia de rede totalmente roteada em um centro de dados virtual, você 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 nenhum outro edge gateway pode se conectar à rede externa.

Um roteador lógico de camada 0 ou um gateway VRF-lite 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.

Dedicar uma rede externa a um edge gateway fornece tenants com serviços adicionais de edge gateway, como o gerenciamento de aviso de rota e a configuração do protocolo de edge gateway (BGP).

O tenant pode decidir quais das redes de tenants 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.

Você pode dedicar uma rede externa a um edge gateway do NSX-T Data Center durante a criação do edge gateway ou posterior, editando as configurações gerais do edge gateway.

Adicionar um edge gateway do NSX-T Data Center

Um edge gateway do NSX-T Data Center oferece uma rede de VDC 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.

Pré-requisitos

Para obter informações sobre os requisitos do sistema para implantar um edge gateway do NSX-T Data Center, consulte o *Guia de administração do NSX-T Data Center*.

A partir da versão 10.1, o VMware Cloud Director oferece suporte a uma configuração de rede externa dedicada. Dedicar uma rede externa a um edge gateway fornece tenants com serviços adicionais de edge gateway, como o gerenciamento de aviso de rota e a configuração do protocolo de edge gateway (BGP). Para obter mais informações, consulte [Redes externas dedicadas](#).

O VMware Cloud Director oferece suporte à configuração básica do edge cluster do NSX-T Data Center. Para obter mais informações sobre a criação do NSX edge clusters, consulte o *Guia de instalação do NSX-T Data Center*.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique em **Novo**.
- 4 Selecione o VDC de organização com suporte no NSX-T Data Center no qual você deseja criar o edge gateway e clique em **Avançar**.
- 5 Digite um nome e, opcionalmente, uma descrição para o novo edge gateway.
- 6 Para ativar o anúncio de rota e o BGP para o edge gateway, ative a opção **Rede Externa Dedicada** e clique em **Avançar**.

- 7 Selecione uma rede externa à qual o novo edge gateway se conecta e clique em **Avançar**.

Se você tiver ativado a opção de **Rede Externa Dedicada**, outros edge gateways não poderão acessar essa rede externa.

- 8 Selecione um edge cluster no qual implantará o edge gateway e clique em **Avançar**.

Se você deseja executar os serviços de edge gateway em um edge cluster diferente daquele associado à rede externa, será possível configurar o edge gateway para usar um edge cluster diferente.

- Use o edge cluster da rede externa à qual o edge gateway está conectado.
- Selecione em uma lista de edge clusters disponíveis para o VDC de organização no qual você está implantando o edge gateway.

- 9 (Opcional) Edite os endereços IP ou os intervalos de endereços IP que são alocados para o edge gateway e clique em **Avançar**.

- 10 Revise a página **Pronto para ser Concluído** e clique em **Concluir**.

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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T.
- 4 Em **Segurança**, clique na guia **Conjuntos de IPs** e em **Novo**.
- 5 Insira um nome e, se desejar, uma descrição para o conjunto de IPs.
- 6 Insira um endereço IP ou um intervalo de endereços IP para as máquinas virtuais que o conjunto de IPs inclui e clique em **Adicionar**.
- 7 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway.
- 4 Se a tela **Firewall** ainda não estiver visível na seção **Serviços**, clique na guia **Firewall**.
- 5 Clique em **Editar Regras**.
- 6 Clique no botão **Novo no Topo**.

Uma linha para a nova regra é adicionada acima da regra selecionada.

- 7 Configure a regra de firewall.

Opção	Descrição
Nome	Digite um nome para a regra.
Estado	Para ativar a regra após a criação, ligue o botão de alternância Estado .
Aplicativos	(Opcional) Para selecionar um perfil de porta específico ao qual a regra se aplica, ative a opção Aplicativos e clique em Salvar .
Origem	<p>Selecione uma opção e clique em Manter.</p> <ul style="list-style-type: none"> ■ Para permitir ou recusar o tráfego de qualquer endereço de origem, ative a opção Qualquer Origem. ■ Para permitir ou negar o tráfego de grupos de firewall específicos, selecione os grupos de firewall na lista.
Destino	<p>Selecione uma opção e clique em Manter.</p> <ul style="list-style-type: none"> ■ Para permitir ou negar o tráfego para qualquer endereço de destino, ative a opção Qualquer Destino. ■ Para permitir ou recusar o tráfego de grupos de firewall específicos, selecione os grupos de firewall na lista.
Ação	<p>No menu suspenso Ação, selecione uma opção.</p> <ul style="list-style-type: none"> ■ Para permitir o tráfego de ou para as origens, os destinos e os serviços especificados, selecione Aceitar. ■ Para bloquear o tráfego proveniente de ou em direção a origens, destinos e serviços especificados, sem notificar o cliente bloqueado, selecione Descartar. ■ 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 Rejeitar.
Protocolo IP	Selecione se deseja aplicar a regra ao tráfego IPv4 ou IPv6.

Opção	Descrição
Direção	<p>Selecione a direção do tráfego à qual aplicar a regra.</p> <p>Observação No VMware Cloud Director 10.2.1 e versões posteriores, essa opção não está mais disponível.</p>
Ativar log.	Para que a conversão de endereços realizada por essa regra seja registrada, ative a opção Ativar o log .

8 Clique em **Salvar**.

9 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway e, em **Serviços**, clique em **NAT**.
- 4 Para adicionar uma regra, clique em **Novo**.
- 5 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"> ■ Se você estiver criando uma regra SNAT, insira o endereço IP público do edge gateway para o qual está configurando a regra SNAT. ■ Se você estiver criando uma regra NO SNAT, deixe a caixa de texto vazia.
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 Configurações Avançadas para obter algumas configurações adicionais.</p> <p>Estado</p> <p>Para ativar a regra na criação, ative para a opção Estado.</p> <p>Log</p> <p>Para que a conversão de endereço realizada por esta regra seja registrada, ative a opção Log.</p> <p>Prioridade</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>Correspondência de Firewall</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"> ■ Para aplicar regras de firewall ao endereço interno de uma regra de NAT, selecione Corresponder Endereço Interno. ■ Para aplicar regras de firewall ao endereço externo de uma regra de NAT, selecione Corresponder Endereço Externo. ■ Para ignorar a aplicação de regras de firewall, selecione Ignorar.

6 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"> ■ 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. ■ Se você estiver criando uma regra NO DNAT, deixe a caixa de texto vazia.
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 Configurações Avançadas para obter algumas configurações adicionais.</p> <p>Estado</p> <p>Para ativar a regra na criação, ative para a opção Estado.</p> <p>Log</p> <p>Para que a conversão de endereço realizada por esta regra seja registrada, ative a opção Log.</p> <p>Prioridade</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>Correspondência de Firewall</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"> ■ Para aplicar regras de firewall ao endereço interno de uma regra de NAT, selecione Corresponder Endereço Interno. ■ Para aplicar regras de firewall ao endereço externo de uma regra de NAT, selecione Corresponder Endereço Externo. ■ Para ignorar a aplicação de regras de firewall, selecione Ignorar.

7 Clique em **Salvar**.

8 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway e, em **Gerenciamento de IP**, clique em **DNS**.
- 4 Na seção **Encaminhador de DNS**, clique em **Editar**.
- 5 Para ativar o serviço de Encaminhador de DNS, ative a opção **Estado**.
- 6 Insira um nome e, opcionalmente, uma descrição para a zona DNS padrão.
- 7 Insira um ou mais endereços IP de servidor upstream, separados por vírgula.
- 8 Clique em **Salvar**.
- 9 (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**.

Editar as alocações de IP de um edge gateway do NSX-T

Você pode alocar vários endereços IP de uma rede externa para um edge gateway.

Procedimentos

- 1 Abra Serviços de Edge Gateway.
 - a Na barra de navegação superior, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Edge Gateways**.
 - c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.
- 2 Clique no edge gateway e em **Alocações de IP**.

Nas grades de gerenciamento de IP, você pode ver os endereços IP que são alocados para o edge gateway e os endereços IP que estão atualmente em uso pelo edge gateway.

3 Na seção **IPs Alocados**, clique em **Gerenciamento de IP**.

Na grade **Gerenciamento de IP**, você pode visualizar o uso de IP para cada uma das redes externas que estão disponíveis para uso pelo edge gateway.

4 Insira um intervalo de IPs e clique em **Adicionar**.

5 Clique em **Salvar**.

Resultados

Os endereços IP são alocados para o edge gateway.

Próximo passo

Visualize os endereços IP que estão alocados para o edge gateway, adicione mais endereços IP ou remova-os conforme necessário.

Alocação de IPs rápida

Você pode alocar endereços IP de uma sub-rede de rede externa para um edge gateway sem inserir endereços IP ou intervalos de endereços IP específicos usando a alocação de IP rápida.

Procedimentos

1 Abra Serviços de Edge Gateway.

- a Na barra de navegação superior, selecione **Recursos** e clique na guia **Recursos de Nuvem**.
- b No painel esquerdo, clique em **Edge Gateways**.
- c Clique no botão de opção ao lado do nome do edge gateway de destino e clique em **Serviços**.

2 Clique no edge gateway e em **Alocações de IP**.

Nas grades de gerenciamento de IP, você pode ver os endereços IP que são alocados para o edge gateway e os endereços IP que estão atualmente em uso pelo edge gateway.

3 Na seção **IPs Alocados**, clique em **Alocação de IP Rápida**.

4 No menu suspenso, selecione uma sub-rede da qual atribuir endereços IP.

Se várias sub-redes estiverem disponíveis, selecionar **Qualquer** resulta na alocação de endereços IP de uma ou mais sub-redes.

5 Insira o número de endereços IP a serem alocados ao edge gateway e clique em **Salvar**.

O número deve ser menor que o número de endereços IP disponíveis na sub-rede que você selecionou.

Resultados

Os endereços IP são alocados para o edge gateway.

Próximo passo

Visualize os endereços IP que estão alocados para o edge gateway, adicione mais endereços IP ou remova-os conforme necessário.

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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway.
- 4 Em **Segurança**, clique em **Perfis de Porta de Aplicativo**.
- 5 Na seção **Aplicativos Personalizados**, clique em **Novo**.
- 6 Insira um nome e, opcionalmente, uma descrição para o perfil de porta de aplicativo.
- 7 Selecione um protocolo no menu suspenso.
- 8 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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
IKEv1	Quando você seleciona essa opção, a VPN IPSec inicia e responde somente ao protocolo IKEv1.
IKEv2	A opção padrão. Quando você seleciona esta versão, a VPN IPSec é iniciada e responde somente ao protocolo IKEv2.
IKE-Flex	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
Copiar	Copia o bit de desfragmentação do pacote IP interno para o pacote externo.
Limpar	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).

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 você dedicou uma rede externa a um gateway de borda do NSX-T Data Center na organização. Consulte [Redes externas dedicadas](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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. Você pode editar essas configurações no gateway de camada 0 principal no NSX-T Data Center.

Pré-requisitos

- Verifique se você dedicou uma rede externa a um gateway de borda do NSX-T Data Center na organização. Consulte [Redes externas dedicadas](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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
Reinicialização auxiliar e normal	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. Observação A configuração do edge gateway se aplica a todos os vizinhos BGP, a menos que a configuração específica do vizinho a substitua.
Somente auxiliar	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.
Desabilitar	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 Alterne 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 você dedicou uma rede externa a um gateway de borda do NSX-T Data Center na organização. Consulte [Redes externas dedicadas](#).
- [Definir configurações gerais de BGP](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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 você dedicou uma rede externa a um gateway de borda do NSX-T Data Center na organização. Consulte [Redes externas dedicadas](#).
- 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways** e clique no nome do edge gateway de destino.
- 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
Desabilitar	Substitui as configurações do edge gateway global e desativa o modo de reinicialização normal para esse vizinho.
Somente auxiliar	Substitui as configurações globais do edge gateway e configura o modo de reinicialização normal como Somente auxiliar para esse vizinho.
Reinicialização normal e auxiliar	Substitui as configurações globais do edge gateway e configura o modo de reinicialização normal como Reinicialização normal e auxiliar 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.

Gerenciamento de balanceamento de carga avançado do NSX em um edge gateway do NSX-T Data Center

Como um **administrador do sistema**, ative o balanceamento de carga em um gateway do NSX-T Data Center e atribua um grupo de mecanismos de serviço ao edge gateway.

Um **administrador da organização** cria pools de servidores do balanceador de carga e serviços virtuais.

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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T Data Center no qual você deseja ativar o balanceamento de carga.
- 4 Em Balanceador de Carga, clique em **Configurações Gerais**.
- 5 Clique em **Editar** e ative a opção **Estado do Balanceador de Carga**.
- 6 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**.
- 7 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T Data Center ao qual você deseja atribuir um grupo de mecanismos de serviço.
- 4 Em Balanceador de Carga, clique em **Grupos de Mecanismos de Serviço**.
- 5 Clique em **Adicionar**.
- 6 Selecione um grupo de mecanismos de serviço disponível na lista.
- 7 Insira um número para o número máximo de serviços virtuais que podem ser colocados no edge gateway.
- 8 Insira um número para os serviços virtuais garantidos disponíveis para o edge gateway.
- 9 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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T Data Center ao qual o grupo de mecanismos de serviço está atribuído.
- 4 Em Balanceador de Carga, clique em **Grupos de Mecanismos de Serviço**.
- 5 Clique em **Editar**.
- 6 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.
- 7 Edite o número para os serviços virtuais garantidos disponíveis para o edge gateway.
- 8 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

- [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, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T Data Center para o qual você deseja configurar um pool de balanceadores de carga.
- 4 Em Balanceador de Carga, clique em **Pools** e, em seguida, clique em **Adicionar**.

5 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
Menos conexões	Novas conexões são enviadas ao servidor que atualmente tem o menor número de conexões.
Round Robin	Novas conexões são enviadas ao próximo servidor elegível no pool em ordem sequencial.
Resposta mais rápida	Novas conexões serão enviadas ao servidor que fornecer a resposta mais rápida para novas conexões ou solicitações.
Hash consistente	Novas conexões são distribuídas pelos servidores usando o endereço IP do cliente para gerar uma chave de hash de IP.
Menor carga	Novas conexões são enviadas ao servidor com a carga mais leve, independentemente do número de conexões que o servidor tem.
Menos servidores	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.
Aleatório	O balanceador de carga seleciona os servidores aleatoriamente.
Menos tarefas	A carga é de balanceamento adaptável, com base no feedback do servidor.
Afinidade de núcleos	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.

- 6 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.
- 7 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**.
- 8 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.
- 9 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

- [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.](#)
- [Adicionar um pool de servidores do balanceador de carga.](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, clique em **Edge Gateways**.
- 3 Clique no edge gateway do NSX-T Data Center no qual você deseja criar um serviço virtual.
- 4 Em Balanceador de Carga, clique em **Serviços Virtuais** e, em seguida, clique em **Adicionar**.
- 5 Insira um nome significativo e, opcionalmente, uma descrição para o serviço virtual.
- 6 Para ativar o serviço virtual na criação, ative a opção **Ativado**.
- 7 Selecione um grupo de mecanismos de serviço para o serviço virtual.
- 8 Selecione um pool de balanceadores de carga para o serviço virtual.
- 9 Insira um endereço IP para o serviço virtual.
- 10 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>

11 Clique em **Salvar**.

Gerenciando instâncias dedicadas do vCenter Server

9

Com instâncias dedicadas do vCenter Server, você pode usar o VMware Cloud Director como um ponto central de gerenciamento (CPOM) para todos os seus ambientes do vSphere.

Quando você adiciona uma instância do vCenter Server ao VMware Cloud Director, pode especificar a finalidade da instância.

vCenter Server dedicado

A infraestrutura de uma instância anexada do vCenter Server é encapsulada como um centro de dados definido por software (SDDC) e é totalmente dedicada a um único tenant. Você cria uma instância dedicada do vCenter Server ativando o acesso ao tenant para essa instância. Depois de ativar o acesso ao tenant, você pode publicar uma instância dedicada do vCenter Server em um tenant.

vCenter Server compartilhado

O provedor pode usar pools de recursos diferentes da instância do vCenter Server em vários VDCs de provedor e, em seguida, alocar esses pools de recursos para diferentes tenants. Uma instância vCenter Server compartilhada não pode ser publicada em tenants.

Nenhuma

A instância do vCenter Server não tem uma finalidade específica.

O VMware Cloud Director pode atuar como um servidor proxy HTTP para as instâncias dedicadas do vCenter Server e as instâncias do vCenter Server que não têm um propósito definido.

Com instâncias dedicadas do vCenter Server, você pode usar o VMware Cloud Director como um ponto central de gerenciamento para todos os seus ambientes vSphere.

- Você pode dedicar os recursos de uma instância do vCenter Server a um único tenant, publicando o vCenter Server dedicado correspondente somente na organização desse tenant. O tenant não compartilha esses recursos com outros tenants. O tenant pode acessar essa instância dedicada do vCenter Server usando uma interface de usuário ou um proxy de API sem uma VPN necessária.
- Você pode usar o VMware Cloud Director como um diretório leve para registrar todas as instâncias do vCenter Server.
- Você pode usar o VMware Cloud Director como um endpoint de API para todas as suas instâncias do vCenter Server.

Você pode ativar o acesso ao tenant e marcar uma instância do vCenter Server como dedicada, durante ou após a anexação da instância do vCenter Server de destino ao VMware Cloud Director. Consulte [Anexar uma instância do vCenter Server sozinha ou em conjunto com uma instância do NSX Manager](#).

Com uma instância do vCenter Server anexada, você pode criar um vCenter Server compartilhado ou um vCenter Server dedicado. Se você criou uma instância compartilhada do vCenter Server, não pode usar essa instância do vCenter Server para criar um vCenter Server dedicado, e vice-versa.

Você pode criar endpoints que os tenants podem usar para acessar o ambiente do vSphere subjacente. Ao usar suas contas do VMware Cloud Director, os usuários podem fazer login na interface de usuário ou na API de componentes com ou sem proxies.

Instâncias dedicadas do vCenter Server no VMware Cloud Director removem a exigência de que o vCenter Server seja publicamente disponível. Para controlar o acesso, você pode ativar e desativar o acesso do tenant a um SDDC no VMware Cloud Director.

Um endpoint é o ponto de acesso para um componente de um SDDC, por exemplo, uma instância do vCenter Server, um host do ESXi ou uma instância do NSX Manager. Você pode conectar um endpoint a um proxy. Ao ativar e desativar um proxy, você pode permitir e interromper o acesso do tenant por meio desse proxy.

A partir do VMware Cloud Director 10.2, se você usar a API para consultar as entidades do vCenter Server e do proxy dedicadas e sua configuração de tenant oferecer suporte a associações multissite, o VMware Cloud Director retornará uma resposta multissite. Os resultados são de todas as associações disponíveis.

Criando e gerenciando instâncias dedicadas do vCenter Server

Para criar e gerenciar instâncias e proxies dedicados do vCenter Server, você pode usar o Portal de Administração do Provedor de Serviços ou o OpenAPI do VMware Cloud Director. Para o OpenAPI do VMware Cloud Director, consulte *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

Importante O VMware Cloud Director requer uma conexão de rede direta para cada instância dedicada do vCenter Server. Se a instância do vCenter Server usar um Platform Services Controller externo, o VMware Cloud Director exigirá também uma conexão de rede direta com o Platform Services Controller.

Para usar a VMware OVF Tool em um vCenter Server dedicado com proxy, o VMware Cloud Director exige uma conexão direta com cada host do ESXi.

- 1 Crie uma instância dedicada do vCenter Server.

Ao adicionar uma instância do vCenter Server ao ambiente VMware Cloud Director, você pode criar uma instância do vCenter Server dedicada ativando o acesso do tenant no assistente para **Adicionar vCenter Server**. Consulte [Adicionar a instância do vCenter Server](#).

Criar uma instância do vCenter Server dedicada também cria um endpoint padrão para ela. Ao anexar a instância do vCenter Server, você também pode criar um proxy. No entanto, o endpoint padrão não está conectado a nenhum proxy por padrão. Você deve editar o endpoint padrão ou criar um novo para conectá-lo a um proxy. Consulte [Criar um endpoint](#).

Você pode ativar o acesso de tenant de instâncias do vCenter Server que já estão adicionadas ao VMware Cloud Director e não têm um uso especificado. Consulte [Habilitar o acesso ao tenant de um vCenter Server anexado](#). A ativação do acesso do tenant disponibiliza a publicação da instância do vCenter Server nesses tenants.

2 Adicione um proxy.

Você pode criar um proxy ao anexar uma instância do vCenter Server ao VMware Cloud Director ou depois. Se a instância do vCenter Server usar um Platform Services Controller externo, o VMware Cloud Director também criará um proxy para o Platform Services Controller. Com proxies pai e filho, você pode ocultar determinados proxies dos tenants ou pode ativar e desativar grupos de proxies filho por meio de seus proxies pai. Para obter informações sobre como criar um proxy depois de adicionar uma instância do vCenter Server ao VMware Cloud Director, consulte [Adicionar um proxy para acessar os recursos do vCenter Server subjacentes](#).

Você pode editar, ativar, desativar e excluir proxies da guia **Proxies** em **Recursos do vSphere**.

Observação Ao adicionar um proxy a uma instância dedicada do vCenter Server, você deve carregar o certificado e a impressão digital, para que os tenants possam recuperar esse certificado e essa impressão digital se o componente com proxy usar certificados autoassinados.

Para visualizar e gerenciar certificados e listas de certificados revogados (CRLs), consulte [Gerenciar os certificados de proxy e as CRLs](#).

- 3 Obtenha o certificado e a impressão digital dos proxies criados e verifique se esse certificado e essa impressão digital estão presentes e corretos. Consulte [Gerenciar os certificados de proxy e as CRLs](#).
- 4 Publique a instância dedicada do vCenter Server em uma ou mais organizações.

Você pode publicar uma instância dedicada do vCenter Server em um tenant e torná-lo visível no VMware Cloud Director Tenant Portal. Na maioria dos casos, uma instância do vCenter Server deve ser publicada somente em um tenant. Consulte [Publicar um vCenter Server dedicado](#).
- 5 Para permitir que os tenants acessem instâncias dedicadas do vCenter Server e proxies do VMware Cloud Director Tenant Portal, você deve publicar o plug-in **Extensão CPOM** em suas organizações. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#).

Este capítulo inclui os seguintes tópicos:

- [Habilitar o acesso ao tenant de um vCenter Server anexado](#)
- [Publicar um vCenter Server dedicado](#)

Habilitar o acesso ao tenant de um vCenter Server anexado

Você pode habilitar o acesso de tenant de instâncias do vCenter Server que já estão adicionadas ao VMware Cloud Director e não têm um uso especificado. Habilitar o acesso ao tenant cria uma instância dedicada do vCenter Server e a torna disponível para ser publicada nos tenants.

Com uma instância do vCenter Server anexada, você pode criar um vCenter Server compartilhado ou um vCenter Server dedicado. Se você tiver criado uma instância do vCenter Server compartilhada e quiser usá-la como um vCenter Server dedicado, deverá primeiro excluir todos os centros de dados virtuais de provedor (VDCs) que estão usando os recursos dessa instância do vCenter Server. Excluir todos os VDCs de provedor vinculados à instância compartilhada do vCenter Server altera seu status para Nenhum.

Pré-requisitos

Verifique se você tem no seu ambiente pelo menos um vCenter Server anexado que não seja dedicado ou compartilhado.

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Selecione um vCenter Server sem uma finalidade especificada na coluna **Uso**.
- 4 Clique em **Habilitar Acesso ao Tenant**.

Próximo passo

[Publicar um vCenter Server dedicado](#).

Publicar um vCenter Server dedicado

Você pode publicar um vCenter Server dedicado em um tenant e torná-lo visível por meio do VMware Cloud Director Tenant Portal. Por padrão, um vCenter Server deve ser publicado apenas em um tenant.

Por padrão, um SDDC é uma instância do vCenter Server que você dedica a um único tenant publicando a instância dedicada do vCenter Server correspondente apenas em sua organização. O tenant não compartilha os recursos da instância dedicada do vCenter Server. Publicar uma instância dedicada do vCenter Server em vários tenants viola os limites do recurso multiempresa. No entanto, às vezes, um tenant deve ter acesso a várias instâncias dedicadas do vCenter Server. Nesses casos, você pode publicar uma instância dedicada do vCenter Server em vários tenants.

Pré-requisitos

- Verifique se você tem pelo menos uma instância do vCenter Server com acesso ao tenant habilitado no seu ambiente VMware Cloud Director. Consulte [Capítulo 9 Gerenciando instâncias dedicadas do vCenter Server](#).

Procedimentos

- 1 Na barra de navegação superior, em **Recursos**, clique em **Recursos de Infraestrutura**.
- 2 No painel esquerdo, selecione **Instâncias do vCenter Server**.
- 3 Selecione um vCenter Server com acesso ao tenant habilitado.

As instâncias do vCenter Server com acesso ao tenant habilitado têm um valor Dedicado na coluna **Uso**.

- 4 Clique em **Gerenciar Tenants**.
- 5 Selecione os tenants para os quais você deseja publicar a instância do vCenter Server.
Desmarcar um tenant da lista cancelará a publicação do vCenter Server.
- 6 Clique em **Salvar**.

Próximo passo

Para permitir que os usuários acessem as instâncias dedicadas do vCenter Server e os proxies no VMware Cloud Director Tenant Portal, você deve publicar o plug-in **Extensão CPOM** em suas organizações. Consulte [Publicar ou cancelar a publicação de um plug-in de uma organização](#).

Gerenciamento de funções e administradores do sistema

10

Usando o Portal de Administração do Provedor de Serviços do VMware Cloud Director, você pode adicionar administradores de sistema 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.

Observação A partir do VMware Cloud Director 9.5, os provedores de serviços podem criar funções de provedor e gerenciar usuários e grupos de provedores usando o Portal de Administração do Provedor de Serviços do VMware Cloud Director ou por meio da OpenAPI do vCloud. Para obter informações sobre como gerenciar funções, usuários e grupos do provedor, consulte o *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*. Para examinar a documentação do OpenAPI do vCloud, vá para https://endereço_IP_ou_nome_host_vCloud_Director/docs.

Este capítulo inclui os seguintes tópicos:

- [Gerenciando direitos e funções](#)
- [Gerenciamento de grupos e usuários de provedor](#)

Gerenciando direitos e funções

Um direito é a unidade fundamental de controle de acesso no VMware Cloud Director. Uma função associa um nome de função a um conjunto de direitos. Cada organização pode ter direitos e funções diferentes.

O VMware Cloud Director usa funções e seus direitos associados para determinar se um usuário ou grupo está autorizado a executar uma operação. Muitos dos procedimentos documentados nos guias do VMware Cloud Director incluem uma função de pré-requisito. Esses pré-requisitos assumem que a função nomeada é a função predefinida não modificada ou uma função que inclui um conjunto equivalente de direitos.

Os administradores do sistema podem usar pacotes de direitos e funções do tenant global para gerenciar os direitos e as funções que estão disponíveis para cada organização.

Depois de instalar o VMware Cloud Director, o sistema contém apenas o pacote de direitos do sistema, que inclui todos os direitos disponíveis no sistema. O pacote de direitos do sistema não é publicado em nenhuma organização. O sistema também contém funções de tenant global integradas que são publicadas para todas as organizações. Para obter informações sobre as funções predefinidas, consulte [Funções predefinidas e seus direitos](#).

Depois de atualizar o VMware Cloud Director da versão 9.1 ou anterior, além do pacote de direitos do sistema, o sistema contém um pacote de direitos herdados para cada organização existente. Cada Pacote de Direitos Herdado inclui os direitos que estão disponíveis na organização associada no momento da atualização e é publicado somente para esta organização.

Observação Para começar a usar o modelo de pacotes de direitos para uma organização existente, você deve excluir o pacote de direitos herdados correspondente.

Se você atualizou o VMware Cloud Director da versão do 9.1 ou anterior, os modelos de função existentes são publicados para todas as organizações como funções de tenant global, e os direitos existentes desvinculados de modelos de função ficam disponíveis como funções específicas de tenant para suas organizações.

Terminologia de direitos

Direita

Cada direito fornece acesso de exibição ou gerenciamento a um tipo de objeto específico no VMware Cloud Director. Os direitos pertencem a diferentes categorias, dependendo dos objetos aos quais eles se relacionam, por exemplo, vApp, catálogo, organização e assim por diante. A organização do provedor contém todos os direitos disponíveis no sistema. O administrador do sistema define os direitos que estão disponíveis para cada organização. Não é possível criar ou modificar os direitos incluídos no VMware Cloud Director.

Pacote de direitos

Os administradores de sistema podem usar pacotes de direitos para gerenciar os direitos disponíveis para cada organização. Um pacote de direitos é um conjunto de direitos que o administrador do sistema pode publicar em uma ou mais organizações. O administrador do sistema pode criar e publicar pacotes de direitos que correspondem a níveis de serviço, funcionalidade monetizável separadamente ou qualquer outro agrupamento de direitos arbitrários. Somente os administradores de sistema podem exibir e gerenciar os pacotes de direitos. Você pode publicar vários pacotes na mesma organização.

Direitos da organização

Os direitos da organização são o conjunto completo de direitos que estão disponíveis para uma organização. Direitos de organização podem abranger vários pacotes de direitos, mas os administradores e usuários da organização visualizam um conjunto simples de direitos que eles podem usar para criar e modificar funções específicas dos tenants.

Terminologia de funções

Função

Uma função é um conjunto de direitos que podem ser atribuídos a um ou mais usuários e grupos. Quando você cria ou importa um usuário ou grupo, deve atribuir a ele uma função.

Funções de provedor

Funções de provedor são o conjunto de funções que estão disponíveis apenas para a organização do Provedor. Funções de provedor podem ser atribuídas somente a usuários Provedores. Administradores de sistema podem criar funções de provedor personalizadas.

Funções de tenant

Funções de tenant são o conjunto de funções disponíveis para uma organização.

Administradores de sistema podem criar e editar funções de tenant globais e publicá-las em uma ou mais organizações. Funções de tenant global podem ser atribuídas a usuários do tenant nas organizações em que elas foram publicadas. Administradores de organização não podem editar funções de tenant global.

Observação Os usuários do tenant podem usar somente os direitos de suas funções que são publicados em suas organizações.

Funções específicas do tenant

Os administradores da organização podem criar e editar funções específicas do tenant, que são locais para suas organizações. Funções específicas de tenant podem ser atribuídas somente a usuários da organização aos quais eles pertencem. As funções específicas do tenant podem conter apenas um subconjunto dos direitos da organização.

Para obter informações sobre como gerenciar funções específicas do tenant, consulte *Guia do Portal de Tenants do VMware Cloud Director*.

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 [Direitos de](#)

Administrador do Sistema. 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

Um **Administrador do Sistema** pode usar o Console Web do Service Provider Admin Portal para visualizar a lista de direitos incluídos em uma função.

- 1 Na barra de navegação superior, clique em **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Funções**.
- 3 Clique no nome da função que você deseja exibir.

Um **Administrador da Organização** pode usar o Service Provider Admin Portal ou o OpenAPI do Cloud Director para exibir os direitos em uma função ou criar funções locais para a organização.

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 de Administrador do Sistema

A função de **Administrador do sistema** existe somente na organização do provedor. Por padrão, a função de **Administrador do Sistema** tem todos os direitos do VMware Cloud Director.

A função de **Administrador do Sistema** tem todos os direitos do VMware Cloud Director. Essa lista consiste nos direitos disponíveis apenas para **Administradores de Sistema**. A função de **Administrador do Sistema** também tem os [Direitos em funções predefinidas de tenant global](#).

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema

Novidades nesta versão	Nome do direito
	Acessar todos os VDCs de organização
	Lista de Controle de Acesso: Gerenciar
	Lista de Controle de Acesso: Exibir
	Serviços Adicionais: Executar Fluxos de Trabalho
	Serviços Adicionais: Exibir Fluxos de Trabalho em Execução
	Serviços Adicionais: Exibir Fluxos de Trabalho
	Adotar Pool de Recursos: Exibir
✓	Definições de aviso: Criar e excluir
✓	Definições de aviso: Ler
	Entidade de Administrador Alternativa: Exibir
	Configurações do AMQP: Gerenciar
	Configurações do AMQP: Exibir
	Explorador de API: Exibir
	Catálogo: Adicionar um vApp da Minha Nuvem
	Catálogo: Alterar proprietário
	Catálogo: Criar/excluir um catálogo
	Catálogo: Editar Propriedades
	Catálogo: Importar Mídia do vSphere
	Catálogo: Publicar
	Catálogo: Exibição de VM Sombra
	Catálogo: Compartilhamento
	Catálogo: Publicar e Assinar VCSP
	Catálogo: Cache de Publicação/Assinatura de VCSP
	Catálogo: Exibir ACL
	Catálogo: Exibir Catálogos Particulares e Compartilhados

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Catálogo: Exibir Catálogos Publicados
	Configuração de Célula: Exibir
	Biblioteca de Certificados: Gerenciar
	Biblioteca de Certificados: Exibir
	Servidor de Túnel de Nuvem: Gerenciar
	Servidor de Túnel de Nuvem: Exibir
	Configurações do Sistema da Biblioteca de Conteúdo: Gerenciar
	Configurações do Sistema da Biblioteca de Conteúdo: Exibir
	Entidade personalizada: Criar definições de entidades personalizadas
	Entidade personalizada: Excluir definições de entidades personalizadas
	Entidade personalizada: Editar definições de entidades personalizadas
	Entidade personalizada: Exibir todas as instâncias de entidades personalizadas da organização
	Entidade personalizada: Exibir definições de entidades personalizadas
	Entidade personalizada: Exibir instância de entidade personalizada
	Repositório de Dados: Excluir
	Repositório de Dados: Editar
	Repositório de Dados: Ativar ou Desativar
	Repositório de Dados: Abrir no vSphere
	Repositório de Dados: Exibir
	Rede de vDC de Organização Direta: Gerenciar
	Switch Virtual Distribuído: Abrir no vSphere
	Edge Cluster: Gerenciar
	Edge Cluster: Exibir
	Definição de API de Serviços de Extensão: Gerenciar
	Definição de API de Serviços de Extensão: Exibir
	Serviços de Extensão: Exibir
	Extensões: Exibir

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Serviço Externo: Gerenciar
	Serviço Externo: Exibir
✓	ACL Geral: Gerenciar
✓	ACL Geral: Exibir
	Geral: Controle do administrador
	Geral: Exibição do administrador
	Geral: Enviar notificação
	Geral: Exibir Detalhes do Erro
	Função Global: Editar
	Função Global: Exibir
	Grupo/usuário: Exibir
	Host: Ativar ou Desativar
	Host: Gerenciar
	Host: Abrir no vSphere
	Host: Preparar ou Despreparar
	Host: Reparar
	Host: Atualizar
	Host: Exibir
	Operações de Nuvem Híbrida: Adquirir tíquete de controle
	Operações de Nuvem Híbrida: Adquirir tíquete de túnel proveniente da nuvem
	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

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Operações de Nuvem Híbrida: Exibir túnel com destino à nuvem
	Configurações Kerberos: Gerenciar
	Configurações Kerberos: Exibir
	Configurações LDAP: Gerenciar
	Configurações LDAP: Exibir
	Relatório de Licenças: Exibir
✓	Controlador do Balanceador de Carga: Editar
✓	Controlador do Balanceador de Carga: Exibir
✓	Atribuição do Grupo de Mecanismos de Serviço do Balanceador de Carga: Editar
✓	Atribuição do Grupo de Mecanismos de Serviço do Balanceador de Carga: Exibir
✓	Grupo de Mecanismos de Serviço do Balanceador de Carga: Editar
✓	Grupo de Mecanismos de Serviço do Balanceador de Carga: Exibir
	Recursos de Localização: Gerenciar
	Pool de Rede: Criar ou Excluir
	Pool de Rede: Editar
	Pool de Rede: Abrir no vSphere
	Pool de Rede: Reparar
	Pool de Rede: Exibir
	NSX-T: Editar
	NSX-T: Exibir
	Extensões de Objeto: Gerenciar
	Extensões de Objeto: Exibir
	Rede da Organização: Criar ou Excluir
	Rede da Organização: Editar Propriedades
	Rede da Organização: Abrir no vSphere
	Rede da organização: Exibir
✓	Cotas de Organização: Gerenciar

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Política de Processamento do vDC de Organização: Exibição de Administrador
	Política de Processamento do vDC de Organização: Gerenciar
	Política de Processamento do vDC de Organização: Exibir
	Firewall Distribuído do vDC de Organização: Configurar Regras
	Firewall Distribuído do vDC de Organização: Ativar/Desativar
	Firewall Distribuído do vDC de Organização: Exibir Regras
	Gateway do vDC de Organização: Configurar Roteamento BGP
	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
	Gateway do vDC de Organização: Configurar VPN L2
	Gateway do vDC de Organização: Configurar Balanceador de Carga
	Gateway do vDC de Organização: Configurar NAT
	Gateway do vDC de Organização: Configurar Syslog
	Gateway do vDC de Organização: Configurar Acesso Remoto
	Gateway do vDC de Organização: Configurar Aviso de Rota
✓	Gateway do vDC de Organização: Configurar Perfil SLAAC
	Gateway do vDC de Organização: Configurar VPN SSL
	Gateway do vDC de Organização: Configurar Roteamento Estático
	Gateway do vDC de Organização: Configurar Syslog
	Gateway do vDC de Organização: Configurar Log de Sistema
	Gateway do vDC de Organização: Converter em Rede Avançada
	Gateway do vDC de Organização: Criar
	Gateway do vDC de Organização: Excluir
	Gateway do vDC de Organização: Roteamento Distribuído

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Gateway do vDC de Organização: Importar
	Gateway do vDC de Organização: Modificar Fator Forma
	Gateway do vDC de Organização: Atualizar
	Gateway do vDC de Organização: Atualizar Propriedades
	Gateway do vDC de Organização: Fazer Upgrade
	Gateway do vDC de Organização: Exibir
	Gateway do vDC de Organização: Exibir Roteamento BGP
	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 VPN L2
	Gateway do vDC de Organização: Exibir o Balanceador de Carga
	Gateway do vDC de Organização: Exibir NAT
	Gateway do vDC de Organização: Exibir Roteamento OSPF
	Gateway do vDC de Organização: Exibir Acesso Remoto
	Gateway do vDC de Organização: Exibir Aviso de Rota
✓	Gateway do vDC de Organização: Exibir Perfil SLAAC
	Gateway do vDC de Organização: Exibir VPN SSL
	Gateway do vDC de Organização: Exibir Roteamento Estático
✓	Política do Kubernetes do vDC de Organização: Editar
	Disco Nomeado do vDC de Organização: Alterar Proprietário
	Disco Nomeado do vDC de Organização: Criar
	Disco Nomeado do vDC de Organização: Excluir
	Disco Nomeado do vDC de Organização: Editar Propriedades
	Disco Nomeado do vDC de Organização: Exibir Status de Criptografia
	Disco Nomeado do vDC de Organização: Exibir Propriedades

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Rede do vDC de Organização: Editar Propriedades
	Rede do vDC de Organização: Importar
	Rede do vDC de Organização: Exibir
	Pool de Recursos do vDC de Organização: Abrir no vSphere
	Pool de Recursos do vDC de Organização: Exibir
✓	Disco Nomeado Compartilhado do vDC de Organização: Criar
	Política de Armazenamento do vDC de Organização: Editar
	Política de Armazenamento do vDC de Organização: Ativar ou Desativar
	Política de Armazenamento do vDC de Organização: Abrir no vSphere
	Política de Armazenamento do vDC de Organização: Remover
	Política de Armazenamento do vDC de Organização: Exibir Recursos
	Perfil de Armazenamento do vDC de Organização: Definir Padrão
	vDC de Organização: Criar
	vDC de Organização: Excluir
	vDC de Organização: Editar ACL
	vDC de Organização: Ativar ou Desativar
	vDC de Organização: Edição Estendida
	vDC de Organização: Exibição Estendida
	vDC de organização: Gerenciar Firewall
	vDC de Organização: Edição Simples
	vDC de Organização: Exibição do Usuário
	vDC de Organização: Exibir ACL
	VDC de Organização: Exibir métricas
	vDC de Organização: Editar Afinidade entre VMs
	Organização: Ativar ou Desativar
	Organização: Criar ou Excluir
	Organização: Editar Configurações de Associação

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Organização: Editar Configurações de Federação
	Organização: Editar Configurações SMTP
	Organização: Editar Política de Concessões
	Organização: Editar Limites
	Organização: Editar Nome
	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: Migrar Armazenamento de Tenant
	Organização: Realizar Consultas de Administrador
	Organização: Usar LDAP de Provedor como Tenant
	Organização: Exibir
	Organização: Exibir métricas
	Grupo de Portas: Abrir no vSphere
	Preferência: Gerenciar Definição de Preferência
	Rede do Provedor: Criar ou Excluir
	Rede do Provedor: Editar
	Rede do Provedor: Abrir no vSphere
	Rede do Provedor: Exibir
	Política de Processamento do vDC de Provedor: Gerenciar
	Política de Processamento do vDC de Provedor: Exibir
	Pool de Recursos do vDC de Provedor: Migrar VMs
	Pool de Recursos do vDC de Provedor: Abrir no vSphere
	Pool de Recursos do vDC de Provedor: Exibir

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Pool de Recursos do vDC de Provedor: Editar
	Política de Armazenamento do vDC de Provedor: Ativar ou Desativar
	Pool de Recursos do vDC de Provedor: Abrir no vSphere
	Pool de Recursos do vDC de Provedor: Remover
	Pool de Recursos do vDC de Provedor: Exibir
	vDC de Provedor: Adicionar Pool de Recursos
	vDC de Provedor: Criar ou Excluir
	vDC de Provedor: Excluir Pool de Recursos
	vDC de Provedor: Editar
	vDC de Provedor: Ativar ou Desativar
	vDC de Provedor: Ativar ou Desativar Pool de Recursos
	vDC de Provedor: Ativar vSphere VXLAN
	vDC de Provedor: Mesclar
	vDC de Provedor: Exibir
✓	Recursos de Política de Cotas: Exibir
✓	Política de Cota: Gerenciar
✓	Política de Cota: Exibir
	Recarregar VM: Gerenciar
	Ação de Classe de Recurso: Gerenciar
	Ação de Classe de Recurso: Exibir
	Pool de Recursos: Abrir
	Pool de Recursos: Abrir no vSphere
	Pool de Recursos: Exibir
	Direito: Gerenciar
	Direito: Exibir
	Pacote de Direitos: Editar
	Pacote de Direitos: Exibir

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Função: Criar, Editar, Excluir ou Copiar
	SDDC: Gerenciar
	SDDC: Gerenciar Proxy
	SDDC: Exibir
	Extensões de Seletor: Gerenciar
	Extensões de Seletor: Exibir
	Aplicativos de Serviço: Gerenciar
	Aplicativos de Serviço: Exibir
	Autorização de Serviço: Gerenciar
	Configuração de Serviço: Gerenciar
	Configuração de Serviço: Exibir
	Biblioteca de Serviços: Criar Bibliotecas de Serviços
	Biblioteca de Serviços: Excluir serviços da biblioteca de serviços
	Biblioteca de Serviços: Editar metadados de serviço
	Biblioteca de Serviços: Editar o conteúdo de um serviço
	Biblioteca de Serviços: Exibir bibliotecas de serviços
	Link de Serviços: Gerenciar
	Link de Serviço: Exibir
	Tipo de Recurso de Serviço: Gerenciar
	Tipo de Recurso de Serviço: Exibir
	Recurso de Serviço: Gerenciar
	Recurso de Serviço: Exibir
	Rede de vDC de Organização Compartilhada: Gerenciar
	Site: Editar
	Site: Exibir
	Configurações do SSL: Exibir

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
✓ (Disponível na versão 10.2.2 e posteriores)	Configurações SSL: gerenciar
✓	SSL: Testar Conexão
	Item Subutilizado: Gerenciar
	Item Subutilizado: Exibir
✓ (Disponível na versão 10.2.2 e posteriores)	Tipo de entidade de armazenamento com suporte: Gerenciar
	Operações do Sistema: Executar Operações do Sistema
	Organização do Sistema: Gerenciar
	Organização do Sistema: Exibir
	Configurações do Sistema: Gerenciar
	Configurações do Sistema: Exibir
✓	Cluster Guest do Tanzu Kubernetes: Controle Total do Administrador
✓	Cluster Guest do Tanzu Kubernetes: Visualização do Administrador
✓	Cluster Guest do Tanzu Kubernetes: Editar
✓	Cluster Guest do Tanzu Kubernetes: Controle Total
✓	Cluster Guest do Tanzu Kubernetes: Visualizar
	Tarefa: Retomar, Abortar ou Falhar
	Tarefa: Atualizar
	Tarefa: Exibir Tarefas
	Token: Gerenciar
	Token: Gerenciar Tudo
	Truststore: Gerenciar
	Truststore: Exibir
	Plug-ins de UI: Definir, Carregar, Modificar, Excluir, Associar ou Desassociar
	Plug-ins de UI: Exibir
	Identidade Visual do Portal de UI: Gerenciar

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	Modelo/Mídia de vApp: Copiar
	Modelo/Mídia de vApp: Criar/Carregar
	Modelo/Mídia de vApp: Editar
	Modelo/Mídia de vApp: Exibir
	Modelo de vApp: Adicionar à Minha Nuvem
	Modelo de vApp: Alterar Proprietário
	Modelo de vApp: Baixar
	Modelo de vApp: Forçar expiração da concessão de armazenamento
	Modelo de vApp: Importar
	Modelo de vApp: Abrir no vSphere
	vApp: Permitir Todas as Configurações Extras
	vApp: Permitir Configuração Extra de Coalescência de Ethernet
	vApp: Permitir Configuração Extra de Latência
	vApp: Permitir Configuração Extra de Correspondência
	vApp: Permitir Configuração Extra de Afinidade de Nó NUMA
	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 configurações de reserva de CPU e Memória da CPU em todos os tipos de VDC
	vApp: Editar Disco Rígido da VM
	vApp: Editar Memória da VM
	vApp: Editar Rede da VM

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	vApp: Editar Propriedades da VM
	vApp: Entrar/Sair no/do Modo de Manutenção
	vApp: Forçar expiração de concessão de tempo de execução
	vApp: Forçar expiração de concessão de armazenamento
	vApp: Opções de Importação
	vApp: Gerenciar manutenção
	vApp: Gerenciar Configurações de Senha da VM
	vApp: Abrir no vSphere
	vApp: Operações de Energia
	vApp: Exibição de VM Sombra
	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 da VM
	vApp: Opções de Inicialização de VM
	vApp: Verificação de Conformidade da VM
	vApp: Migrar, Impor Cancelamento de Implementação, Realocar, Consolidar VM
	VAPP_VM_METADATA_TO_VCENTER
	Extensão de VCD: Registrar, Cancelar Registro, Atualizar, Associar ou Desassociar
	Extensão de VCD: Exibir
	vCenter: Anexar ou Desanexar
	vCenter: Ativar ou Desativar
	vCenter: Abrir no vSphere
	vCenter: Atualizar

Tabela 10-1. Direitos Disponíveis por Padrão somente para Administradores do Sistema (continuação)

Novidades nesta versão	Nome do direito
	vCenter: Exibir
	Grupo de vDCs: Configurar
✓	Grupo de vDCs: Configurar Log
	Grupo de vDC: Exibir
	Modelo de VDC: Gerenciar ACL
	Modelo de VDC: Exibição Estendida
	Modelo de VDC: Instanciar
	Modelo de VDC: Gerenciar
	Modelo de VDC: Exibir
	VMC: Registrar SDDC
✓	VMWARE:NATIVECLUSTER: Controle Total do Administrador
✓	VMWARE:NATIVECLUSTER: Exibição do Administrador
✓	VMWARE:NATIVECLUSTER: Editar
✓	VMWARE:NATIVECLUSTER: Controle Total
✓	VMWARE:NATIVECLUSTER: Exibir
	vRealize Orchestrator: Publicar e Cancelar Publicação de Fluxos de Trabalho em Tenants
	vRealize Orchestrator: Registrar e Cancelar Registro de Servidores do vRealize Orchestrator
	vRealize Orchestrator: Exibir Servidores vRealize Orchestrator Registrados
	Servidor vSphere: Gerenciar
	Servidor vSphere: Gerenciar Proxy
	Servidor do vSphere: Gerenciar Configuração do Proxy
	Servidor vSphere: Exibir

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	✓	✓	✓		
	Catálogo: Alterar proprietário	✓				
	Catálogo: Criar/excluir um catálogo	✓	✓			
	Catálogo: Editar Propriedades	✓	✓			
	Catálogo: Publicar	✓	✓			
	Catálogo: Compartilhamento	✓	✓			
	Catálogo: Publicar e Assinar VCSP	✓	✓			
	Catálogo: Exibir ACL	✓	✓			
	Catálogo: Exibir Catálogos Particulares e Compartilhados	✓	✓	✓		
	Catálogo: Exibir Catálogos Publicados	✓				
	Biblioteca de Certificados: Gerenciar	✓				
	Biblioteca de Certificados: Exibir	✓				
	Entidade personalizada: Exibir todas as instâncias de entidades personalizadas da organização	✓				
	Entidade personalizada: Exibir instância de entidade personalizada	✓				
	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	✓				
	Disco Nomeado do vDC de Organização: Alterar Proprietário	✓	✓			
	Disco Nomeado do vDC de Organização: Criar	✓	✓	✓		
	Disco Nomeado do vDC de Organização: Excluir	✓	✓	✓		
	Disco Nomeado do vDC de Organização: Editar Propriedades	✓	✓	✓		
	Disco Nomeado do vDC de Organização: Exibir Status de Criptografia	✓		✓		
	Disco Nomeado do vDC de Organização: Exibir Propriedades	✓	✓	✓	✓	

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Rede do vDC de Organização: Editar Propriedades	✓				
	Rede do vDC de Organização: Exibir	✓		✓		
	Política de Armazenamento do vDC de Organização: Exibir Recursos	✓				
	Perfil de Armazenamento do vDC de Organização: Definir Padrão	✓				
	vDC de Organização: Editar ACL	✓				
	vDC de organização: Gerenciar Firewall	✓				
	vDC de Organização: Edição Simples	✓				
	vDC de Organização: Exibição do Usuário	✓	✓			
	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 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	✓				

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	Organização: Exibir	✓	✓	✓		
	Organização: Exibir métricas	✓				
✓	Recursos de Política de Cotas: Exibir	✓				
	Função: Criar, Editar, Excluir ou Copiar	✓				
	Biblioteca de Serviços: Exibir bibliotecas de serviços	✓				
✓	SSL: Testar Conexão	✓	✓			
	Plug-ins de UI: Exibir	✓	✓	✓	✓	
✓ (Disponível na versão 10.2.1 e posteriores)	Truststore: Gerenciar	✓				
✓ (Disponível na versão 10.2.1 e posteriores)	Truststore: Exibir	✓				
	Plug-ins de UI: Exibir	✓	✓	✓	✓	
	Modelo/Mídia de vApp: Copiar	✓	✓	✓		
	Modelo/Mídia de vApp: Criar/Carregar	✓	✓			
	Modelo/Mídia de vApp: Editar	✓	✓	✓		
	Modelo/Mídia de vApp: Exibir	✓	✓	✓	✓	
	Modelo de vApp: Adicionar à Minha Nuvem	✓	✓	✓	✓	
	Modelo de vApp: Alterar Proprietário	✓	✓			
	Modelo de vApp: Baixar	✓	✓			
	vApp: Alterar Proprietário	✓				
	vApp: Copiar	✓	✓	✓	✓	
	vApp: Criar/Reconfigurar	✓	✓	✓		

Novidades nesta versão	Nome do direito	Administrador da organização	Autor do catálogo	Autor de vApp	Usuário de vApp	Somente acesso ao console
	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	✓		✓	✓	
	vApp: Opções de Inicialização de VM	✓	✓	✓		
	vApp: Metadados da VM para o vCenter	✓	✓	✓		
✓	Grupo de VDCs: Configurar	✓				
✓	Grupo de VDCs: Configurar Log	✓				
✓	Grupo de VDCs: Exibir	✓				
	Modelo de VDC: Instanciar	✓				
	Modelo de VDC: Exibir	✓				

Gerenciamento dos pacotes de direitos

Como administrador do sistema, você pode criar pacotes de direitos e publicá-los em uma ou mais organizações em sua nuvem. Você pode editar e excluir pacotes de direitos existentes. Você pode cancelar a publicação de pacotes de direitos de organizações na sua nuvem.

Criar um pacote de direitos

Você pode agrupar um conjunto de direitos como um pacote de direitos que pode ser publicado em uma ou mais organizações em seu sistema.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Clique em **Adicionar**.
- 4 Digite um nome e, opcionalmente, uma descrição para o novo pacote de direitos.
- 5 Selecione os direitos que você deseja associar a este pacote.

Os direitos são agrupados em categorias e subcategorias para exibir ou gerenciar o acesso ao objeto ao qual eles estão relacionados.

Você pode selecionar os direitos individualmente, pelo modo de exibição ou gerenciamento por subcategoria ou pelo modo de exibição ou gerenciamento globalmente.

Categoria	Descrição
Controle de Acesso	Contém direitos para exibir e gerenciar organizações, direitos, funções e usuários.
Administração	Contém direitos para exibir e gerenciar a configuração geral e multissite.
Calcular	Contém direitos para exibir e gerenciar VDCs de organização e de provedor, vApps, modelos de VDC de organização e monitoramento de VM.
Extensões	Contém direitos para exibir e gerenciar plug-ins e extensões do VMware Cloud Director.
Infraestrutura	Contém direitos para exibir e gerenciar recursos do vSphere.
Bibliotecas	Contém direitos para exibir e gerenciar catálogos e itens de catálogos.
Rede	Contém direitos para exibir e gerenciar recursos de rede.

- 6 Clique em **Salvar**.

Próximo passo

Você pode publicar o pacote de direitos recém-criado para uma ou mais organizações em seu sistema. Consulte [Publicar ou cancelar a publicação de um pacote de direitos](#).

Clonar um pacote de direitos

Você pode usar um pacote de direitos existente como um modelo para a criação de um novo pacote.

Pré-requisitos

Verifique se você tem os direitos para adicionar novas funções a VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Selecione o pacote de direitos que você deseja clonar e clique em **Clonar**.
- 4 Na janela **Clonar Pacote de Direitos**, insira um nome e uma descrição para o pacote clonado.
- 5 (Opcional) Para editar os direitos clonados, ative a opção **Modificar Direitos Seleccionados** e selecione ou desmarque os direitos que você deseja alterar para a função clonada.
- 6 Clique em **Salvar**.

Publicar ou cancelar a publicação de um pacote de direitos

Você pode publicar um pacote de direitos em uma ou mais organizações do seu sistema. Depois de publicar um pacote de direitos para uma organização, os direitos nesse pacote tornam-se parte do conjunto de direitos da organização.

Direitos de organização podem abranger vários pacotes de direitos, mas os administradores e usuários da organização visualizam um conjunto simples de direitos que eles podem usar para criar e modificar funções.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Selecione o botão de opção ao lado do pacote de destino e clique em **Publicar**.

4 Para publicar o pacote:

- a Selecione **Publicar em Tenants**.
- b Selecione as organizações para a qual você deseja publicar a função.
 - Se você quiser publicar o pacote para todas as organizações existentes e recém-criadas no seu sistema, selecione **Publicar para Todos os Tenants**.
 - Se você deseja publicar o pacote para organizações específicas no seu sistema, selecione essas organizações individualmente.

5 Para cancelar a publicação do pacote:

- Se quiser cancelar a publicação do pacote de todas as organizações do sistema, desmarque a opção **Publicar para Tenants**.
- Se quiser cancelar a publicação do pacote de organizações específicas no seu sistema, desmarque **Publicar para Todos os Tenants** e desmarque as organizações individualmente.

6 Clique em **Salvar**.

Resultados

Os direitos no pacote publicado estão disponíveis nas organizações selecionadas e podem ser usados em funções nessas organizações.

Os direitos na função não publicada são removidos das organizações selecionadas e não podem ser usados em funções nessas organizações.

Exibir e editar um pacote de direitos

Você pode exibir os direitos que estão incluídos em um pacote de direitos. Você pode modificar o nome, a descrição e os direitos de um pacote.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Clique no nome do pacote de destino.

Você pode exibir os direitos que estão associados ao pacote por meio da expansão das categorias de direitos.
- 4 Edite o pacote e clique em **Manter**.

Resultados

Se você tiver modificado os direitos do pacote, o novo conjunto de direitos será aplicado a todas as organizações nas quais esse pacote de direitos é publicado.

Excluir um pacote de direitos

Você pode remover um pacote de direitos que você não usa mais em suas organizações.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Selecione o botão de seleção ao lado do pacote de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Gerenciamento das funções do tenant global

Como administrador do sistema, você pode criar funções do tenant global e publicá-las em uma ou mais organizações em sua nuvem. Você pode editar e excluir funções do tenant global existentes. Você pode cancelar a publicação de funções do tenant global de organizações individuais em sua nuvem.

Após a instalação e configuração inicial do VMware Cloud Director, o sistema contém um conjunto de tenants globais predefinidos que são publicados em todas as organizações. Consulte [Funções predefinidas e seus direitos](#).

Criar uma função de tenant global

Você pode criar uma função de tenant global que possa publicar em uma ou mais organizações em seu sistema.

Após a instalação e a configuração iniciais do VMware Cloud Director, o sistema contém funções de tenant global predefinidas que são publicadas em todas as organizações. Para obter informações sobre as funções predefinidas, consulte [Funções predefinidas e seus direitos](#).

Você pode adicionar funções globais personalizadas ao seu sistema.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Funções Globais**.
- 3 Clique em **Adicionar**.
- 4 Insira um nome e, opcionalmente, uma descrição para a nova função.
- 5 Selecione os direitos que você deseja associar à função.

Os direitos são agrupados em categorias e subcategorias para exibir ou gerenciar o acesso ao objeto ao qual eles estão relacionados.

Você pode selecionar os direitos individualmente, pelo modo de exibição ou gerenciamento por subcategoria ou pelo modo de exibição ou gerenciamento globalmente.

Categoria	Descrição
Controle de Acesso	Contém direitos para exibir e gerenciar organizações, direitos, funções e usuários.
Administração	Contém direitos para exibir e gerenciar a configuração geral e multissite.
Calcular	Contém direitos para exibir e gerenciar VDCs de organização e de provedor, vApps, modelos de VDC de organização e monitoramento de VM.
Extensões	Contém direitos para exibir e gerenciar plug-ins e extensões do VMware Cloud Director.
Infraestrutura	Contém direitos para exibir e gerenciar recursos do vSphere.
Bibliotecas	Contém direitos para exibir e gerenciar catálogos e itens de catálogos.
Rede	Contém direitos para exibir e gerenciar recursos de rede.

6 Clique em **Manter**.

Resultados

Durante a criação, o novo tenant global direito está disponível somente para a organização de Provedor do VMware Cloud Director.

Próximo passo

Você pode publicar a função recém-criada em uma ou mais organizações no seu sistema. Consulte [Publicar ou cancelar a publicação de uma função de tenant global](#).

Clonar uma função de tenant global

Você pode usar uma função de tenant global existente como modelo para a criação de uma nova função.

Pré-requisitos

Verifique se você tem os direitos para adicionar novas funções a VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Funções Globais**.
- 3 Selecione a função que você deseja clonar e clique em **Clonar**.
- 4 Na janela **Clonar Função Global**, insira um nome e uma descrição para a função clonada.
- 5 (Opcional) Para editar os direitos clonados, ative a opção **Modificar Direitos Seleccionados** e selecione ou desmarque os direitos que você deseja alterar para a função clonada.

6 Clique em **Salvar**.

Publicar ou cancelar a publicação de uma função de tenant global

Você pode publicar uma função de tenant global em uma ou mais organizações do seu sistema. Depois de publicar uma função para uma organização, essa função se torna parte do conjunto de funções de tenant da organização.

Pré-requisitos

Se quiser cancelar a publicação de uma função de tenant global de uma organização, certifique-se de que nenhum usuário esteja atribuído com essa função na organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Funções Globais**.
- 3 Selecione o botão de opção ao lado da função de destino e clique em **Publicar**.
- 4 Para publicar a função:
 - a Selecione **Publicar em Tenants**.
 - b Selecione as organizações para a qual você deseja publicar a função.
 - Se você quiser publicar a função para todas as organizações existentes e recém-criadas no seu sistema, selecione **Publicar para Todos os Tenants**.
 - Se você quiser publicar a função em organizações específicas no seu sistema, selecione essas organizações individualmente.
- 5 Para cancelar a publicação da função:
 - Se quiser cancelar a publicação da função de todas as organizações do sistema, desmarque a opção **Publicar para Tenants**.
 - Se quiser cancelar a publicação da função de organizações específicas no seu sistema, desmarque **Publicar para Todos os Tenants** e desmarque as organizações individualmente.

6 Clique em **Salvar**.

Resultados

A função publicada está disponível em organizações selecionadas e pode ser atribuída aos usuários nessas organizações. Os administradores da organização não podem editar funções de tenant global publicadas em suas organizações.

A função cuja publicação é cancelada é removida das organizações selecionadas e não pode ser atribuída aos usuários nessas organizações.

Visualizar e edite uma função de tenant global

Você pode visualizar os direitos que estão incluídos em uma função de tenant global. Você pode modificar o nome, a descrição e os direitos de uma função de tenant global.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Funções Globais**.
- 3 Clique no nome da função de destino.

Você pode exibir os direitos que estão associados à função por meio da expansão das categorias de direitos.

- 4 Para modificar o nome, a descrição ou os direitos da função, clique em **Editar**.
- 5 Edite a função e clique em **Manter**.

Resultados

Se você modificou os direitos da função, o novo conjunto de direitos será aplicado aos usuários em todas as organizações atribuídas a essa função.

Excluir uma função de tenant global

Você pode remover uma função de tenant global que não é mais usada em suas organizações.

Pré-requisitos

A função de tenant global que você deseja excluir não deve ser atribuída a nenhum usuário em todas as organizações.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Funções Globais**.
- 3 Selecione o botão de opção próximo à função de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Gerenciamento das funções do provedor

Você pode criar e gerenciar funções na sua organização de provedor do VMware Cloud Director.

Para obter informações sobre como gerenciar funções do tenant, consulte o *Guia do Portal de Tenants do VMware Cloud Director*.

Criar uma função de provedor

Você pode criar uma função na sua organização de Provedor do VMware Cloud Director.

Após a instalação e a configuração iniciais do VMware Cloud Director, o sistema contém funções predefinidas são locais para a organização de Provedor e globais para todas as organizações. Para obter informações sobre as funções predefinidas, consulte [Funções predefinidas e seus direitos](#).

Você pode adicionar funções de provedor personalizadas à sua organização de provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Funções**.
- 3 Clique em **Novo**.
- 4 Insira um nome e, opcionalmente, uma descrição para a nova função.
- 5 Selecione os direitos que você deseja associar à função.

Os direitos são agrupados em categorias e subcategorias para exibir ou gerenciar o acesso ao objeto ao qual eles estão relacionados.

Você pode selecionar os direitos individualmente, pelo modo de exibição ou gerenciamento por subcategoria ou pelo modo de exibição ou gerenciamento globalmente.

Categoria	Descrição
Controle de Acesso	Contém direitos para exibir e gerenciar organizações, direitos, funções e usuários.
Administração	Contém direitos para exibir e gerenciar a configuração geral e multissite.
Calcular	Contém direitos para exibir e gerenciar VDCs de organização e de provedor, vApps, modelos de VDC de organização e monitoramento de VM.
Extensões	Contém direitos para exibir e gerenciar plug-ins e extensões do VMware Cloud Director.
Infraestrutura	Contém direitos para exibir e gerenciar recursos do vSphere.
Bibliotecas	Contém direitos para exibir e gerenciar catálogos e itens de catálogos.
Rede	Contém direitos para exibir e gerenciar recursos de rede.

- 6 Clique em **Salvar**.

Resultados

A função recém-criada está disponível para atribuir a usuários na sua organização de Provedor.

Clonar uma função de provedor

Você pode usar uma função de provedor existente como modelo para a criação de uma nova função.

Pré-requisitos

Verifique se você tem os direitos para adicionar novas funções a VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Funções**.
- 3 Selecione a função que você deseja clonar e clique em **Clonar**.
- 4 Na janela **Clonar Função**, insira um nome e uma descrição para a função clonada.
- 5 (Opcional) Para editar os direitos clonados, ative a opção **Modificar Direitos Seleccionados** e selecione ou desmarque os direitos que você deseja alterar para a função clonada.
- 6 Clique em **Salvar**.

Exibir ou editar uma função de provedor

Você pode exibir os direitos que estão incluídos em uma função que é local para sua organização de Provedor do VMware Cloud Director. Você pode modificar o nome, a descrição e os direitos de uma função.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Funções**.
- 3 Clique no nome da função de destino.

Você pode exibir os direitos que estão associados à função por meio da expansão das categorias de direitos.
- 4 Para modificar o nome, a descrição ou os direitos da função, clique em **Editar**.
- 5 Edite a função e clique em **Salvar**.

Resultados

Se você modificou os direitos da função, o novo conjunto de direitos será aplicado aos usuários atribuídos a essa função.

Excluir uma função de provedor

Você pode remover uma função que não usa mais na sua organização de Provedor do VMware Cloud Director.

Pré-requisitos

A função que você deseja excluir não deve ser atribuída a nenhum usuário.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Funções**.
- 3 Selecione o botão de opção próximo à função de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Gerenciamento de grupos e usuários de provedor

Você pode adicionar e importar grupos e usuários para a sua organização de provedor do VMware Cloud Director.

Para obter informações sobre como gerenciar grupos e usuários da organização, consulte o *Guia do Portal de Tenants do VMware Cloud Director*.

Gerenciamento de usuários do provedor

Você pode gerenciar usuários na organização do seu provedor usando o Service Provider Admin Portal.

Para obter informações sobre como gerenciar usuários do tenant nas organizações, consulte o *Guia do Portal de Tenants do VMware Cloud Director*.

Criar um usuário do provedor

Você pode criar um usuário na sua organização de Provedor do VMware Cloud Director.

Durante a instalação e a configuração iniciais do VMware Cloud Director, você cria uma conta de **administrador do sistema**. Após a configuração inicial, você pode criar outros administradores e usuários para a organização de Provedor.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3 Clique em **Novo**.
- 4 Insira um nome de usuário e senha para o novo usuário.
A senha deve conter pelo menos seis caracteres.
- 5 Selecione se deseja ativar o usuário na criação.
- 6 No menu suspenso **Funções disponíveis**, selecione uma função para o usuário.

A lista de funções disponíveis compreende as funções globais e as funções que são locais para a organização do seu sistema.

7 (Opcional) Insira as informações de contato para o usuário.

Você pode inserir o nome completo, o endereço de e-mail, o número de telefone e a ID de mensagem instantânea.

8 (Opcional) Defina as cotas para o usuário.

- a Você pode definir um limite das máquinas virtuais de propriedade do usuário ou selecionar **Ilimitado**.
- b Você pode definir um limite das máquinas virtuais em execução de propriedade do usuário ou selecionar **Ilimitado**.

Importar usuários de provedor

Você pode importar usuários para a organização do seu provedor do VMware Cloud Director de um provedor de identidade LDAP ou SAML configurado anteriormente.

Pré-requisitos

[Configurar uma conexão de LDAP do sistema](#) ou [Configurar seu sistema para usar um provedor de identidade SAML](#).

Procedimentos

- 1** Na barra de navegação superior, selecione **Administração**.
- 2** No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3** Clique em **Importar Usuários**.
- 4** No menu suspenso **Origem**, selecione o tipo de provedor de identidade.

Pode ser **LDAP** ou **SAML**.

Se você tiver configurado apenas um provedor de identidade, essa opção será codificada.

- 5** Especifique os usuários.

Opção	Descrição
LDAP	<ul style="list-style-type: none"> a Insira um nome parcial ou completo de um usuário e clique em Pesquisar. b Nos resultados da pesquisa, selecione os usuários que você deseja importar. c No menu suspenso Atribuir Função, selecione uma função para os usuários importados.
SAML	<ul style="list-style-type: none"> a Digite os nomes dos usuários que você deseja importar no formato de identificador de nome suportado pelo provedor de identidade SAML. Use uma nova linha para cada nome de usuário. b No menu suspenso Atribuir Função, selecione uma função para os usuários importados.

- 6** Clique em **Salvar**.

Resultados

Você pode ver os usuários importados na lista de usuários.

Editar um usuário de provedor

Você pode alterar a senha, a função, as informações de contato e as cotas de um usuário na sua organização de Provedor. Você não pode alterar o nome de usuário.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3 Clique no botão de seleção ao lado do nome do usuário de destino e clique em **Editar**.
- 4 Edite os detalhes do usuário e clique em **Salvar**.

Ativar ou desativar um usuário do provedor

Depois que você desativar um usuário, ele não poderá fazer login no VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3 Clique no botão de seleção ao lado do nome do usuário de destino e clique em **Desativar** ou **Ativar**.
- 4 Se desativar um usuário, clique em **OK** para confirmar.

Excluir um usuário de provedor

Você pode remover um usuário da sua organização de Provedor do VMware Cloud Director excluindo a conta de usuário.

Para excluir um usuário bloqueado que perdeu o acesso ao sistema porque seu grupo LDAP foi excluído, use a API do VMware Cloud Director.

Pré-requisitos

Desative o usuário que você deseja excluir. Consulte [Ativar ou desativar um usuário do provedor](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3 Clique no botão de seleção ao lado do nome do usuário de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Desbloquear um usuário do provedor

Se você habilitou o bloqueio de conta nas configurações do sistema de política de senha, os usuários poderão bloquear suas contas após um determinado número de tentativas de logon inválidas. Mesmo que o bloqueio seja definido com um intervalo de bloqueio de conta, você pode desbloquear uma conta de usuário sem aguardar a expiração do bloqueio.

Para obter informações sobre como configurar a política de bloqueio de conta, consulte [Configurar a política de senha](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Usuários**.
- 3 Clique no botão de opção ao lado do nome do usuário de destino e clique em **Desbloquear**.

Gerenciamento de grupos de provedor

Você pode importar, editar e excluir grupos da sua organização de provedor usando o Service Provider Admin Portal.

Para obter informações sobre como gerenciar grupos nas organizações, consulte o *Guia do Portal de Tenants do VMware Cloud Director*.

Importar um grupo de provedor

Você pode importar grupos para a organização do seu provedor do VMware Cloud Director de um provedor de identidade LDAP ou SAML configurado anteriormente.

Pré-requisitos

[Configurar uma conexão de LDAP do sistema](#) ou [Configurar seu sistema para usar um provedor de identidade SAML](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Grupos**.
- 3 Clique em **Importar Grupos**.
- 4 No menu suspenso **Origem**, selecione o tipo de provedor de identidade.

Pode ser **LDAP** ou **SAML**.

Se você tiver configurado apenas um provedor de identidade, essa opção será codificada.

5 Especifique os usuários.

Opção	Descrição
LDAP	<ol style="list-style-type: none"> Insira um nome parcial ou completo de um grupo e clique em Pesquisar. Nos resultados da pesquisa, selecione os grupos que você deseja importar. No menu suspenso Atribuir Função, selecione uma função para os usuários nos grupos importados.
SAML	<ol style="list-style-type: none"> Digite os nomes dos grupos que você deseja importar no formato de identificador de nome suportado pelo provedor de identidade SAML. Use uma nova linha para cada nome de grupo. No menu suspenso Atribuir Função, selecione uma função para os usuários nos grupos importados.

6 Clique em **Salvar**.

Editar um grupo de provedores

Você pode editar a descrição e alterar a função dos membros de um grupo que você importou anteriormente para a sua organização de Provedor do VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Grupos**.
- 3 Clique no botão de seleção ao lado do nome do grupo de destino e clique em **Editar**.
- 4 Edite os detalhes do grupo e clique em **Salvar**.

Excluir um grupo de provedores

Você pode remover um grupo da sua organização de Provedor do VMware Cloud Director.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Provedor**, selecione **Grupos**.
- 3 Clique no botão de seleção ao lado do nome do grupo de destino e clique em **Excluir**.
- 4 Para confirmar, clique em **OK**.

Gerenciamento de configurações do sistema

11

Um administrador do sistema do VMware Cloud Director pode controlar as configurações de todo o sistema relacionadas a LDAP, notificação por e-mail, licenciamento e preferências gerais do sistema.

Este capítulo inclui os seguintes tópicos:

- [Modificar as configurações gerais do sistema](#)
- [Configurações gerais do sistema](#)
- [Ativar o modo FIPS nas células do grupo de servidores](#)
- [Definir as configurações de e-mail do sistema](#)
- [Alterar a licença do VMware Cloud Director](#)
- [Definir as configurações de sincronização de catálogo](#)
- [Criar um painel de avisos](#)
- [Configurar e monitorar tarefas de bloqueio e notificações](#)
- [Configurar endereços públicos](#)
- [Gerenciamento de provedores de identidade](#)
- [Gerenciamento de certificados](#)
- [Gerenciando plug-ins](#)
- [Personalizando os portais do VMware Cloud Director](#)
- [Configurar a política de senha](#)
- [Configurar os serviços do vSphere](#)

Modificar as configurações gerais do sistema

O VMware Cloud Director inclui configurações gerais do sistema relacionadas a logs de atividades, rede, tempos limite de sessão, certificados, limites da organização, limites de operação e assim por diante. As configurações padrão são apropriadas para muitos ambientes, mas você pode modificar as configurações para atender às suas necessidades.

Para obter uma lista das propriedades que você pode modificar, consulte [Configurações gerais do sistema](#).

Observação Para obter informações sobre como alterar a data, hora ou o fuso horário do dispositivo do VMware Cloud Director, consulte <https://kb.vmware.com/kb/59674>.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Geral**.
- 3 Clique em **Editar** para a seção que você deseja modificar, edite as propriedades e clique em **Salvar**.

Configurações gerais do sistema

O VMware Cloud Director inclui configurações gerais do sistema que você pode modificar para atender às suas necessidades.

Tabela 11-1. Configurações gerais do sistema

Nome	Categoria	Descrição
Activity log history to keep	Log de atividade	Número de dias do histórico de logs a ser mantido antes de excluí-lo. Insira 0 para nunca para excluir logs.
Activity log history shown	Log de atividade	Número de dias do histórico de logs a ser exibido. Para mostrar todas as atividades, insira 0.
Display debug information	Log de atividade	Ative essa configuração para exibir as informações de depuração no log de tarefa do VMware Cloud Director.
IP address release timeout	Rede	Número de segundos para manter endereços IP lançados em espera antes de torná-los disponíveis para alocação novamente. Essa configuração padrão é de 2 horas (7200 segundos) para permitir que as entradas antigas expirem a partir das tabelas ARP de cliente.
Allow Overlapping External Networks	Rede	Para adicionar redes externas que são executadas no mesmo segmento de rede, marque a caixa de seleção. Ative essa configuração somente se você estiver usando métodos não baseados em VLAN para isolar suas redes externas.
Allow FIPS mode	Rede	Permite a ativação do modo FIPS nos Gateways de Borda. Requer a instalação do NSX 6.3 ou posterior. Consulte o Modo FIPS na documentação do <i>VMware NSX for vSphere</i> .
Default syslog server settings for networks	Rede	Insira os endereços IP para até dois servidores de Syslog para uso em redes. Essa configuração não se refere aos servidores de Syslog usados por células de nuvem.

Tabela 11-1. Configurações gerais do sistema (continuação)

Nome	Categoria	Descrição
Provider Locale	Localização	Selecione uma localidade para a atividade do provedor, incluindo entradas de log, alertas de e-mail e assim por diante.
Idle session timeout	Tempos limite	Quantidade de tempo que o aplicativo do VMware Cloud Director permanece ativo sem interação com o usuário.
Maximum session timeout	Tempos limite	Quantidade máxima de tempo que o aplicativo do VMware Cloud Director permanece ativo.
Host refresh frequency	Tempos limite	Com que frequência o VMware Cloud Director verifica se os seus hosts ESXi estão acessíveis ou inacessíveis.
Host hung timeout	Tempos limite	Selecione a quantidade de tempo a aguardar antes de marcar um host como parado.
Transfer session timeout	Tempos limite	Quantidade de tempo a aguardar antes da falha de uma tarefa de carregamento pausada ou cancelada, por exemplo, carregar mídia ou carregar modelo vApp. Esse tempo limite não afeta as tarefas de carregamento que estão em andamento.
Enable upload quarantine with a timeout of __ seconds	Tempos limite	Selecione a caixa de seleção e insira um número de tempo limite que represente a quantidade de tempo para quarentena de arquivos carregados.
Verify vCenter and vSphere SSO certificates	Certificados	VMware Cloud Director sempre verifica os certificados. Quando habilitado, verifica os nomes de host nos certificados do vCenter Server.
Verify NSX Manager certificates	Certificados	VMware Cloud Director sempre verifica os certificados. Quando habilitado, o VMware Cloud Director verifica os nomes de host nos certificados do NSX Manager.
Edit Organization Limits	Limites do VDC de Organização	Insira o número máximo de centros de dados virtuais de organização por organização ou selecione Ilimitado .
Number of resource intensive operations running per user	Limites operacionais	Insira o número máximo de operações simultâneas que fazem uso intenso de recursos por usuário ou selecione Ilimitado .
Number of resource intensive operations to be queued per user (in addition to running)	Limites operacionais	Insira o número máximo de operações enfileiradas que fazem uso intenso de recursos por usuário ou selecione Ilimitado .
Number of resource intensive operations running per organization	Limites operacionais	Insira o número máximo de operações simultâneas que fazem uso intenso de recursos por organização ou selecione Ilimitado .
Number of resource intensive operations to be queued per organization	Limites operacionais	Insira o número máximo de operações enfileiradas que fazem uso intenso de recursos por organização ou selecione Ilimitado .
Provide default vApp names	Outros	Marque a caixa de seleção para configurar o VMware Cloud Director para fornecer nomes padrão a novos vApps.

Tabela 11-1. Configurações gerais do sistema (continuação)

Nome	Categoria	Descrição
Make Allocation pool Org VDCs elastic	Outros	Marque a caixa de seleção para ativar o pool de alocações elástico, tornando elásticos todos os centros de dados virtuais de organização do pool de alocações. Antes de desmarcar essa opção, certifique-se de que todas as máquinas virtuais para cada centro de dados virtual da organização tenham migrado para um único cluster.
VM discovery enabled	Outros	Por padrão, cada VDC de organização descobre automaticamente VMs do vCenter que foram criadas em qualquer pool de recursos que suporta o VDC. Desmarque para desativar essa configuração para todos os VDCs no sistema.

Ativar o modo FIPS nas células do grupo de servidores

Você pode configurar o VMware Cloud Director 10.2.2 e versões posteriores no Linux para usar módulos criptográficos validados para FIPS 140-2 e executar no modo compatível com FIPS.

O Federal Information Processing Standard (FIPS) 140-2 é um padrão federal dos EUA e do Canadá que especifica requisitos de segurança para módulos criptográficos. O Programa de Validação de Módulos Criptográficos (CMVP) do NIST valida os módulos criptográficos em conformidade com os padrões FIPS 140-2.

O objetivo do suporte ao FIPS do VMware Cloud Director é facilitar as atividades de conformidade e a segurança em vários ambientes regulamentados. Para saber mais sobre o suporte para FIPS 140-2 em produtos da VMware, consulte <https://www.vmware.com/security/certifications/fips.html>.

No VMware Cloud Director, a criptografia validada para FIPS está desativada por padrão. Ao ativar o modo FIPS, você configura o VMware Cloud Director para usar módulos criptográficos validados para FIPS 140-2 e executados no modo compatível com FIPS.

Observação Ativar o modo FIPS também permite a pesquisa inversa de nomes de host.

Importante Quando você ativa o modo FIPS, a integração ao vRealize Orchestrator não funciona.

No VMware Cloud Director 10.2.2, quando você ativa o modo FIPS, não é possível criptografar asserções SAML. Quando não está no modo FIPS, não há restrição quanto à criptografia de asserções.

O VMware Cloud Director usa os seguintes módulos criptográficos validados para FIPS 140-2:

- BC-FJA (Bouncy Castle FIPS Java API) da VMware, versão 1.0.2.1: [Certificado #3673](#)
- Módulo de objeto OpenSSL FIPS da VMware, versão 2.0.20-vmw: [Certificado #3857](#)

O VMware Cloud Director está em um pacote com a ferramenta de gerenciamento de células (CMT). No entanto, a ferramenta de gerenciamento de células não é compatível com FIPS.

Para obter informações sobre como ativar o modo FIPS no dispositivo VMware Cloud Director, consulte [Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director](#).

Pré-requisitos

- Verifique se os certificados têm o bit `KeyCertSign` com asserção usando o uso do OpenSSL. O modo FIPS apenas poderá funcionar se os certificados SSL do VMware Cloud Director tiver o `KeyCertSign` com asserção.

```
openssl crl2pkcs7 -nocrl -certfile certificates.pem | openssl pkcs7 -print_certs -text -noout
```

Se os certificados não incluírem a extensão, especifique o bit `KeyCertSign` ao criar um armazenamento de chaves de certificados SSL.

- Instale e ative o conjunto de utilitários `rng-tools`. Consulte <https://wiki.archlinux.org/index.php/Rng-tools>.
- Se a coleta de métricas estiver ativada, verifique se os certificados Cassandra seguem o padrão de certificado X.509 v3 e incluem todas as extensões necessárias. Você deve configurar o Cassandra com os mesmos conjunto de codificações usados pelo VMware Cloud Director. Para obter informações sobre as codificações SSL permitidas, consulte [Gerenciando a lista de codificações SSL permitidas](#).
- Cancele o registro do VMware Cloud Director no vCenter Lookup Service. Consulte [Configurar os serviços do vSphere](#).

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **SSL**.
- 3 Clique em **Ativar**.
- 4 Confirme se o seu ambiente atende a todos os pré-requisitos para ativar o modo FIPS.
Se o seu ambiente não atender a todos os pré-requisitos antes de iniciar a configuração do modo FIPS, é possível que o VMware Cloud Director se torne inacessível.
- 5 Para confirmar que você deseja iniciar o processo, clique em **Ativar**.
Quando a configuração terminar, o VMware Cloud Director exibirá uma mensagem para reiniciar as células da nuvem.
- 6 Depois que o VMware Cloud Director exibir uma mensagem para reiniciar suas células de nuvem, reinicie todas as células no grupo de servidores do VMware Cloud Director.

Próximo passo

- Desative o modo FIPS clicando em **Desativar** e, depois que o VMware Cloud Director indicar que a configuração está pronta, reinicie as células.
- Você pode visualizar o status FIPS das células VMware Cloud Director ativas usando o comando da CMT `fips-mode`. Consulte [Visualizar o status FIPS de todas as células ativas](#) no *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Definir as configurações de e-mail do sistema

Você pode editar as configurações de e-mail do sistema, incluindo a definição das configurações do servidor SMTP e as configurações de notificação do VMware Cloud Director.

O VMware Cloud Director requer um servidor SMTP para enviar notificações de usuário e e-mails de alerta do sistema para usuários do sistema.

O VMware Cloud Director envia os e-mails de alerta do sistema quando ele tem informações importantes para relatar. Por exemplo, o VMware Cloud Director envia um alerta quando o espaço de um datastore está se tornando insuficiente. Você pode configurar o VMware Cloud Director para enviar alertas de e-mail a todos os administradores de sistema ou a uma lista específica de endereços de e-mail.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **E-mail** e clique em **Editar**.
- 3 Insira o nome de host DNS ou o endereço IP do servidor de e-mail SMTP.
- 4 Insira o número da porta do servidor SMTP.
- 5 (Opcional) Se o servidor SMTP exigir um nome de usuário, ative a opção **Exige autenticação** e insira o nome de usuário e a senha da conta SMTP.
- 6 Selecione a guia **Configurações de notificação**.
- 7 Insira um endereço de e-mail a ser exibido como remetente para os e-mails do VMware Cloud Director.

O VMware Cloud Director usa o endereço de e-mail do remetente para enviar alertas de expiração de tempo de execução e de locação de armazenamento.

- 8 (Opcional) Insira o texto do prefixo do assunto.
- 9 Selecione os destinatários das notificações.

Por padrão, somente os administradores da organização recebem as notificações SMTP.

- 10 Clique em **Salvar**.

11 (Opcional) Teste as configurações SMTP.

- a Clique em **Testar**.
- b Se você tiver ativado a opção **Exige autenticação**, insira a senha do servidor SMTP.
- c Insira um endereço de e-mail de destino e clique em **Testar**.

Alterar a licença do VMware Cloud Director

O VMware Cloud Director requer uma licença válida, especificada como um número de série, para ser executado. Você pode modificar as informações de licenciamento inseridas durante a configuração inicial do VMware Cloud Director.

O número de série de produto do VMware Cloud Director não é o mesmo que a chave de licença do vCenter Server. Você pode obter um número de série do VMware Cloud Director no Portal de Licenças da VMware.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, selecione **Licença** e clique em **Editar**.
- 3 Insira um novo número de série e clique em **Salvar**.

Definir as configurações de sincronização de catálogo

Você pode editar as configurações de sincronização de catálogo para todas as organizações e catálogos, incluindo a taxa de atualização das assinaturas de catálogo.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **Catálogo**.
- 3 Clique em **Editar**.
- 4 Ative a sincronização de catálogos.
- 5 Defina as horas de início e de término da sincronização.
- 6 Defina o intervalo de sincronização.

O intervalo de sincronização é a taxa de atualização das assinaturas de catálogos.

- 7 Clique em **Salvar**.

Próximo passo

Para obter informações sobre como configurar a otimização da sincronização de catálogos, consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Criar um painel de avisos

Você pode criar notificações que são exibidas na parte superior das páginas da interface de usuário no VMware Cloud Director Service Provider Admin Portal e no Tenant Portal. As mensagens podem ser exibidas para os administradores do sistema, os usuários em uma organização ou os usuários em todas as organizações.

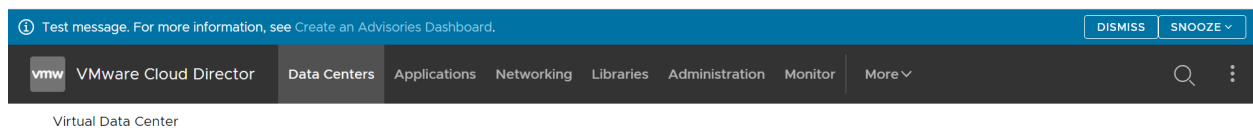
Não é possível editar avisos depois de criá-los.

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 visualizar todos os avisos na guia **Avisos**. No entanto, eles são exibidos para o grupo de usuários selecionado apenas durante o período selecionado.
- 6 Selecione se você deseja que a notificação seja exibida somente para os administradores do sistema, para todos os usuários dentro da organização ou entre as organizações.
- 7 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.

Configurar e monitorar tarefas de bloqueio e notificações

Você pode usar tarefas de bloqueio e notificações para configurar o VMware Cloud Director para enviar mensagens AMQP disparadas por certos eventos.

Algumas dessas mensagens são apenas notificações que o evento ocorreu. Outras mensagens publicam informações em um endpoint AMQP designado, indicando que uma ação solicitada foi bloqueada e está pendente por um aplicativo cliente associado a esse endpoint. Essas mensagens são conhecidas como tarefas de bloqueio.

Um **administrador do sistema** pode configurar um conjunto de tarefas de bloqueio em todo o sistema que estão sujeitas a ações de programação por um cliente de AMQP.

Configurar um agente AMQP

Se você quiser que o VMware Cloud Director envie mensagens AMQP disparadas por determinados eventos, deverá configurar um agente AMQP. É possível usar as mensagens AMQP para automatizar o tratamento de uma solicitação de usuário subjacente.

Procedimentos

1 Na barra de navegação superior, selecione **Administração**.

2 Em **Configurações**, selecione **Extensibilidade**.

A guia **Agente AMQP** é aberta.

3 Clique no botão **Editar** da seção **Agente AMQP**.

4 Insira o nome de host DNS ou o endereço IP do host AMQP.

O nome de domínio completo do host do servidor RabbitMQ, por exemplo *amqp.example.com*.

5 Insira a porta AMQP.

A porta padrão na qual o agente ouve mensagens é 5672.

6 Insira o intercâmbio.

7 Insira o vHost.

O padrão é /.

8 Insira o prefixo.

- 9 (Opcional) Para usar o SSL, ative a opção **Usar SSL** e selecione uma das opções de certificado.

Por padrão, o serviço AMQP do VMware Cloud Director envia mensagens não criptografadas. Você pode configurar o serviço AMQP para criptografar essas mensagens usando o SSL. Você também pode configurar o serviço para verificar o certificado do agente usando o armazenamento confiável JCEKS padrão do Java Runtime Environment na célula do VMware Cloud Director, normalmente em `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Opção	Descrição
Aceitar todos os certificados	O registro de CN do campo do proprietário do certificado deve corresponder ao nome do host do agente AMQP. Para usar certificados que não correspondem ao nome do host do agente, ative o botão Aceitar todos os certificados .
Certificado SSL	Carregue o certificado SSL.
Armazenamento de Chaves de SSL (JCEKS)	Carregue o armazenamento de chaves SSL e insira a senha do armazenamento de chaves.

- 10 Insira um nome de usuário e senha para se conectar ao host AMQP.
- 11 Clique em **Salvar**.
- 12 (Opcional) Para testar as configurações, clique no botão **Testar** na seção **Agente AMQP** e forneça a senha.
- 13 (Opcional) Para publicar eventos de auditoria no agente AMQP, clique no botão **Editar** na seção **Notificações AMQP sem bloqueios** e ative a opção **Habilitar notificações**.

Definir as configurações da tarefa de bloqueio

É possível configurar certas operações como tarefas de bloqueio. Essas operações serão suspensas até que um **administrador do sistema** atue sobre elas ou até a expiração de um timer pré-configurado. Você pode especificar as configurações de tempo limite e as ações padrão para tarefas de bloqueio. As configurações se aplicam a todas as organizações na instalação.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 Em **Configurações**, selecione **Extensibilidade**.
- 3 Selecione a guia **Tarefas de Bloqueio**.

- 4 Para editar o tempo limite de extensão padrão e a ação de tempo limite padrão, clique no botão **Editar** na seção **Geral**.

- a Edite o **Tempo limite da tarefa de bloqueio padrão**.
- b Edite a **Ação de Tempo Limite Padrão**.

A **Ação de Tempo Limite Padrão** é a ação após a expiração de um **Tempo limite de tarefa de bloqueio padrão**.

- c Clique em **Salvar**.
- 5 Para editar a lista de operações, consideradas como tarefas de bloqueio, clique no botão **Editar** da seção **Operações**.
 - a Marque ou desmarque operações na lista de tarefas de bloqueio.
 - b Clique em **Salvar**.

Monitorar tarefas bloqueadas

Você pode monitorar as tarefas bloqueadas atuais ou cancelar, causar a falha ou retomar manualmente as tarefas antes da expiração do temporizador pré-configurado.

Pré-requisitos

Definir as configurações da tarefa de bloqueio

Procedimentos

- 1 Na barra de navegação superior, em **Monitorar**, selecione **Tarefas de Bloqueio**.
A guia exibe uma lista das tarefas bloqueadas atuais.
- 2 Selecione a tarefa que você deseja editar manualmente.
- 3 Decida entre cancelar, causar a falha ou retomar a tarefa e clique no botão correspondente.
- 4 Insira uma mensagem e clique em **Salvar**.

A mensagem aparece nos detalhes da tarefa.

Configurar endereços públicos

Para atender aos requisitos de balanceador de carga ou de proxy, você pode alterar os endereços da Web do endpoint padrão para o Portal da Web do VMware Cloud Director, a API do VMware Cloud Director e o proxy do console.

Os endereços públicos são endereços da Web expostos aos clientes do VMware Cloud Director. Os padrões para esses endereços são especificados durante a instalação. Se necessário, você pode atualizar os endereços.

Se o VMware Cloud Director consistir em uma única célula, o instalador criará endpoints públicos que normalmente fornecem acesso suficiente para clientes de API e da Web. As instalações e implantações que incluem várias células normalmente colocam um balanceador de carga entre as células e os clientes. Os clientes acessam o sistema no endereço do balanceador de carga. O balanceador de carga distribui as solicitações do cliente entre as células disponíveis. Outras configurações de rede que incluem um proxy ou colocar as células em uma zona desmilitarizada também exigem endpoints personalizados. Os detalhes da URL do endpoint são específicos da sua configuração de rede.

Os endpoints para o VMware Cloud Director Tenant Portal e o Console Web do VMware Cloud Director exigem certificados SSL, de preferência assinados. Ao instalar ou implantar o VMware Cloud Director, você deve fornecer o nome do caminho para esses certificados. Se você personalizar qualquer um desses endpoints após a instalação ou implantação, talvez seja necessário instalar novos certificados que correspondam aos detalhes do endpoint, como `hostname` e `subject alternative name`.

Para o dispositivo VMware Cloud Director, você deve configurar o endereço de proxy do console público do VMware Cloud Director, pois o dispositivo usa um único endereço IP com porta personalizada 8443 para o serviço de proxy do console. Consulte [Etapa 6](#).

Pré-requisitos

Verifique se você está conectado como **administrador do sistema**. Somente um **administrador do sistema** pode personalizar os endpoints públicos.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Endereços Públicos**.
- 3 Para personalizar os endpoints públicos, clique em **Editar**.
- 4 Para personalizar as URLs do VMware Cloud Director, edite os endpoints do **Portal da Web**.
 - a Insira uma URL pública personalizada do VMware Cloud Director para conexões HTTP (não seguras).
 - b Insira a URL pública personalizada do VMware Cloud Director para conexões HTTPS (seguras) e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

A cadeia de certificados deve corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias `consoleproxy`. Não há suporte para a terminação SSL das conexões de proxy do console em um balanceador de carga. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato `PEM` sem uma chave privada.

5 (Opcional) Para personalizar as URLs da REST API e do OpenAPI do Cloud Director, desative a opção **Usar Configurações do Portal da Web.**

- a Insira uma URL base HTTP personalizada.

Por exemplo, se você definir a URL base HTTP como **http://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em `http://vcloud.example.com/api` e poderá acessar o OpenAPI do VMware Cloud Director em `http://vcloud.example.com/cloudapi`.

- b Insira uma URL de base da REST API de HTTPS e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

Por exemplo, se você definir a URL base da API REST HTTPS como **https://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em `https://vcloud.example.com/api` e o OpenAPI do VMware Cloud Director em `https://vcloud.example.com/cloudapi`.

A cadeia de certificados deverá corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias `http`, ou ao certificado VIP do balanceador de carga se for usada uma terminação SSL. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato PEM sem uma chave privada.

6 Insira um endereço de proxy personalizado do console público do VMware Cloud Director.

- Personalize o endereço de proxy do console público do dispositivo VMware Cloud Director.

Esse endereço é o nome de domínio completo (FQDN) do dispositivo do VMware Cloud Director `eth0` NIC, especificado por FQDN ou por endereço IP, com a porta personalizada 8443 para o serviço de proxy do console.

- Personalize o endereço de proxy do console público do VMware Cloud Director no Linux.

Esse endereço é o nome de domínio totalmente qualificado (FQDN) do servidor do VMware Cloud Director ou do balanceador de carga com o número da porta. A porta padrão é 443.

Por exemplo, para uma instância do VMware Cloud Director Appliance com FQDN `vcloud.example.com`, insira **vcloud.exemplo.com:8443**.

O VMware Cloud Director usa o endereço de proxy do console ao abrir uma janela de console remoto em uma VM.

7 Clique em **Salvar.**

Gerenciamento de provedores de identidade

Você pode integrar sua nuvem a um provedor de identidade externo e importar usuários e grupos para sua organização. Você pode configurar uma conexão de servidor LDAP em um nível de

sistema ou de organização. Você pode configurar uma integração de SAML em um nível de organização.

Gerenciamento de conexões LDAP

Como administrador do sistema, você pode configurar sua organização de sistema do VMware Cloud Director e qualquer outra organização no sistema para usar um servidor LDAP como fonte de usuários e grupos. As organizações podem usar a conexão LDAP do sistema ou uma conexão LDAP privada.

A partir da versão 10.1, o VMware Cloud Director está se movendo para uma área de armazenamento centralizada e ciente do tenant para o gerenciamento de certificados. Dessa forma, o VMware Cloud Director centraliza todos os certificados em um local para que os **administradores de sistema** e os **administradores de organização** possam visualizar, auditar e gerenciar todos os certificados em uso por vários componentes no sistema. Você pode usar a API do VMware Cloud Director para adicionar, atualizar ou remover certificados da nova área de armazenamento com reconhecimento de tenant. Consulte *Referência de esquemas de API do VMware Cloud Director*.

Ao adicionar ou editar um novo endpoint de servidor LDAP, a interface de usuário do VMware Cloud Director investiga esse endpoint para qualquer certificado que esteja apresentando. O VMware Cloud Director adiciona a uma área de armazenamento de certificado centralizada qualquer certificado que você decidir confiar.

Configurar uma conexão de LDAP do sistema

Para fornecer VMware Cloud Director e suas organizações com acesso compartilhado para usuários e grupos, você pode configurar uma conexão LDAP em um nível de sistema.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Provedores de Identidade**, clique em **LDAP**.

As configurações de LDAP atuais são exibidas.

Próximo passo

[Configurar, teste e sincronizar uma conexão LDAP](#).

Configurar uma conexão LDAP da organização

Você pode configurar uma organização para usar a conexão LDAP do sistema como uma fonte compartilhada de usuários e grupos. Você pode configurar uma organização para usar uma conexão LDAP separada como uma fonte privada de usuários e grupos.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **Organizações**.

- 3 Clique no nome da organização de destino.

Você será redirecionado para o Portal de Tenant do VMware Cloud Director da organização.

- 4 Na barra de navegação superior, selecione **Administração**.
- 5 No painel esquerdo, em **Provedores de Identidade**, clique em **LDAP**.

As configurações de LDAP atuais são exibidas.

- 6 Na guia **Opções de LDAP**, clique em **Editar**.
- 7 Configure a fonte LDAP de usuários e grupos para esta 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 VCD	A organização usa a conexão LDAP do sistema VMware Cloud Director que você configurou anteriormente. Consulte Configurar uma conexão de LDAP do sistema .
Serviço LDAP personalizado	A organização usa um servidor LDAP privado como uma fonte de usuários e grupos da organização. Clique na guia LDAP Personalizado e 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>.

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, DC=example,DC=com.</p> <p>Para se conectar a um nó na estrutura de árvore do domínio, insira o nome distinto desse nó, por exemplo, OU=ServiceDirector,DC=example,DC=com.</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 Active Directory ou OpenLDAP .
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 Carregar e importe um certificado SSL do LDAP ou selecione Aceitar todos os certificados .
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.

Configurar seu sistema para usar um provedor de identidade SAML

Se você quiser importar usuários e grupos de um provedor de identidade SAML para a organização do sistema, deverá configurar a organização do sistema com esse provedor de identidade SAML. Os usuários importados podem fazer login na organização do sistema com as credenciais estabelecidas no provedor de identidade SAML.

Para configurar VMware Cloud Director com um provedor de identidade SAML, você estabelece uma confiança mútua trocando metadados do provedor de serviços SAML e do provedor de identidade.

Quando um usuário importado tenta fazer login, o sistema extrai os seguintes atributos do token SAML, se disponível, e os usa para interpretar as partes correspondentes de informações sobre o usuário.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (esse atributo é configurável)

Informações de grupo são usadas se o usuário não é importado diretamente, mas espera-se que faça login em virtude da associação em grupos importados. Um usuário pode pertencer a vários grupos, portanto, pode ter várias funções durante uma sessão.

Se um usuário ou grupo importado for atribuído à 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 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 direitos para executar nenhuma atividade.

Dica Se você precisar fazer login como um usuário local, poderá usar a URL base que configurou, como `https://vcloud.example.com/tenant/tenant_name/login`.

Pré-requisitos

- Verifique se você tem acesso a um provedor de identidade em conformidade com o SAML 2.0.
- Obtenha um arquivo XML com os seguintes metadados do provedor de identidade SAML.
 - 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 SAML.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em Provedores de Identidade, clique em **SAML** e clique em **Editar**.
As configurações do SAML atual são exibidas.

- 3 Na guia **Provedor de Serviços**, baixe os metadados do provedor de serviço SAML do VMware Cloud Director.
 - a Insira uma ID de Entidade para a organização do sistema.

A ID da Entidade identifica exclusivamente a organização do seu sistema para o seu Provedor de Identidade.
 - b Examine a data de expiração do certificado e, se expirar em breve, gere novamente o certificado clicando em **Regenerar**.

O certificado está incluído nos metadados SAML e é usado para assinatura e criptografia. Uma ou ambas podem ser necessárias, dependendo de como a relação de confiança é estabelecida entre a organização e o IDP SAML.
 - c Clique no link de **Metadados**.

O link é semelhante a `https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd`.

Seu navegador baixa os metadados do provedor de serviços SAML, um arquivo XML que você deve fornecer ao seu provedor de identidade.
- 4 Na guia **Provedor de Identidade**, carregue os metadados SAML que você recebeu anteriormente do seu provedor de identidade.
 - a Selecione **Usar Provedor de Identidade SAML**.
 - b Clique no ícone **Procurar** e carregue o arquivo ou copie e cole seu conteúdo na caixa de texto **XML de Metadados**.
- 5 Clique em **Salvar**.

Gerenciamento de certificados

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.

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](#).

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.

Você deve gerenciar as bibliotecas de certificados separadamente para cada site.

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](#).

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.

Gerenciando plug-ins

Os plug-ins do VMware Cloud Director estendem as funções do Service Provider Admin Portal e do VMware Cloud Director Tenant Portal. Você pode carregar, desativar e excluir plug-ins do Service Provider Admin Portal. Você pode publicar um plug-in no provedor de serviços e organizações individuais.

Alguns plug-ins são instalados como parte do VMware Cloud Director.

Extensão CPOM

Fornece a capacidade de exibir e gerenciar os proxies e as instâncias dedicadas do vCenter Server usando o VMware Cloud Director Tenant Portal.

Personalizar portal

Fornece a capacidade de personalizar o VMware Cloud Director Service Provider Admin Portal e o VMware Cloud Director Tenant Portal.

Disponibilidade do vCloud

O plug-in do VMware vCloud® Availability™ fornece a capacidade de acessar o vCloud Availability Portal diretamente na interface do usuário do VMware Cloud Director. Para obter mais informações, consulte a [documentação do vCloud Availability](#).

Carregar um plug-in

Você pode carregar plug-ins adicionais no VMware Cloud Director Service Provider Admin Portal para uso pelo provedor de serviços e pelas organizações na nuvem.

Pré-requisitos

Baixe o arquivo de instalação do plug-in.

Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Personalizar Portal**.
- 2 Clique em **Carregar**.
- 3 Clique em **Selecionar arquivo do plug-in**, navegue até o arquivo de instalação de destino e clique em **Abrir**.
- 4 Clique em **Avançar**.
- 5 Selecione o escopo para este plug-in.

Opção	Descrição
Provedores de Serviço	A função de plug-in fica disponível no VMware Cloud Director Service Provider Admin Portal.
Tenants	A função de plug-in fica disponível no VMware Cloud Director Service Provider Admin Portal das organizações que você seleciona.

- 6 Se você tiver definido o escopo do plug-in nos tenants, selecione as organizações para as quais deseja publicar esse plug-in.
- 7 Revise a página **Revisar e Concluir** e clique em **Concluir**.

Ativar ou desativar um plug-in

Para impedir que todas as organizações usem um plug-in, você pode desativar esse plug-in.

Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Personalizar Portal**.
- 2 Marque a caixa de seleção ao lado dos nomes dos plug-ins de destino e clique em **Ativar** ou **Desativar**.

Excluir um plug-in

Você pode remover um ou mais plug-ins do VMware Cloud Director Service Provider Admin Portal.

Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Personalizar Portal**.
- 2 Marque as caixas de seleção ao lado dos nomes dos plug-ins que você deseja remover e clique em **Excluir**.
- 3 Para confirmar, clique em **Salvar**.

Publicar ou cancelar a publicação de um plug-in de uma organização

Você pode modificar o conjunto de organizações que podem usar a função fornecida por um plug-in.

Você pode modificar o conjunto de organizações para vários plug-ins.

Procedimentos

- 1 Na barra de navegação superior, selecione **Mais > Personalizar Portal**.
- 2 Marque as caixas de seleção ao lado dos nomes dos plug-ins de destino e clique em **Publicar**.
- 3 Selecione o escopo para este plug-in.

Opção	Descrição
Provedores de Serviço	A função de plug-in fica disponível no VMware Cloud Director Service Provider Admin Portal.
Tenants	A função de plug-in fica disponível no VMware Cloud Director Service Provider Admin Portal das organizações que você seleciona.

- 4 Se você tiver definido o escopo do plug-in nos tenants, selecione as organizações para as quais deseja publicar esse plug-in.
- 5 Clique em **Salvar**.

Personalizando os portais do VMware Cloud Director

Para corresponder aos padrões de identidade visual da sua empresa e criar uma experiência de nuvem totalmente personalizada, você pode definir o logotipo e o tema para o VMware Cloud Director Service Provider Admin Portal e para o VMware Cloud Director Tenant Portal de cada organização. Além disso, pode modificar e adicionar links personalizados aos dois menus na parte superior direita nos portais do VMware Cloud Director.

Observação Para personalizar seus atributos e links de identidade visual, você deve usar os métodos de OpenAPI de vCloud de `branding`. Consulte *Introdução à OpenAPI do VMware Cloud Director* em <https://code.vmware.com>.

Identidade visual do portal

Como parte da instalação, o VMware Cloud Director contém dois temas: padrão e escuro. Você pode criar, gerenciar e aplicar temas personalizados. Também pode alterar o nome do portal, o logotipo e o ícone do navegador. Além disso, o título do navegador adota o nome do portal que você definiu.

Você define os atributos de identidade visual em um nível do sistema, para que personalize o VMware Cloud Director Service Provider Admin Portal. O VMware Cloud Director Tenant Portal de cada organização adota os atributos de identidade visual do sistema, a menos que você tenha configurado atributos de identidade visual para o tenant específico.

Para um determinado tenant, você pode substituir seletivamente qualquer combinação do nome do portal, cor do plano de fundo, logotipo, ícone, tema e links personalizados. Qualquer valor que você não definir usará o valor padrão do sistema correspondente.

Observação Por padrão, a identidade visual do tenant individual não é exibida fora de uma sessão conectada. A identidade visual individual do tenant não aparece nas páginas de login e logoff, para que os tenants não possam descobrir a existência de outros. Você pode habilitar a identidade visual fora das sessões conectadas usando a ferramenta de gerenciamento de célula:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

Para obter informações sobre como usar a ferramenta de gerenciamento de célula, consulte o *Guia de instalação, configuração e upgrade do VMware Cloud Director*.

Links personalizados

Os links personalizados são um componente da identidade visual do portal. Há dois tipos de links personalizados:

- Os itens de menu `override` substituem os links existentes dos itens de menu **Ajuda**, **Sobre** e **Fazer Download do VMRC**. Por padrão, **Fazer Download do VMRC** redireciona os usuários para <https://my.vmware.com> para baixar o VMRC, que exige que os usuários tenham contas registradas para download. Ao substituir esse link, você pode realocar o instalador do VMRC para o seu próprio servidor.
- Os itens de menu `link` são novos links que você adiciona ao item de menu **Fazer Logout** no canto superior direito do portal. Os novos links personalizados aparecem na ordem fornecida na chamada à API.

Você pode organizar esses links personalizados usando os itens de menu `section` e `separator`. Um item de menu `section` adiciona um cabeçalho ao menu; um item de menu `separator` adiciona uma linha ao menu.

Os links personalizados permitem variáveis personalizadas que você pode usar para passar informações de identificação para outros aplicativos na forma de parâmetros de consulta.

O VMware Cloud Director oferece suporte às seguintes variáveis personalizadas no valor `url` para um link personalizado:

Tabela 11-2. Variáveis personalizadas para links personalizados

Variável	Descrição
<code>\${TENANT_NAME}</code>	Nome da organização
<code>\${TENANT_ID}</code>	ID da organização
<code>\${SESSION_TOKEN}</code>	x-vcloud-authorization token

Por exemplo,

```
url: https://host:port/tenant/${TENANT_NAME}/vdc
```

no VMware Cloud Director Tenant Portal do myorg da organização é convertido em:

```
url: https://host:port/tenant/myorg/vdc
```

Configurar a política de senha

Para impedir que um usuário faça login no VMware Cloud Director após um determinado número de tentativas com falha, você pode ativar o bloqueio da conta.

As alterações na política de bloqueio de conta do sistema se aplicam a todas as novas organizações. As organizações criadas antes da alteração da política de bloqueio de conta devem ser alteradas no nível da organização.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Política de Senha**.
- 3 Clique em **Editar**.
- 4 Para ativar o bloqueio de conta, ative o botão de alternância **Bloqueio de conta**.
- 5 Selecione o número aceitável de logins inválidos antes de bloquear uma conta.
- 6 Selecione o intervalo de bloqueio.
- 7 Para habilitar o bloqueio de conta do **administrador do sistema**, ative o botão de alternância **A conta do Administrador do Sistema pode ser bloqueada**.
- 8 Clique em **Salvar**.

Configurar os serviços do vSphere

Você pode configurar e ativar o VMware Cloud Director para usar o vCenter Single Sign-On, de forma que o provedor de identidade do vSphere autentique os administradores do sistema.

O vCenter Lookup Service contém informações de topologia sobre a infraestrutura do vSphere, permitindo que os componentes do vSphere conectem-se uns aos outros com segurança.

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **Serviços do vSphere**.
- 3 Configure os serviços do vSphere.
 - Para registrar o VMware Cloud Director no vCenter Lookup Service, clique em **Registrar**.

- Para cancelar o registro do VMware Cloud Director no vCenter Lookup Service, clique em **Cancelar Registro**.
- 4 Insira a URL do vCenter Lookup Service, por exemplo, `https://hostname:443/lookupservice/sdk`.
 - 5 Insira o nome de usuário e a senha de um usuário do vCenter Single Sign-On com privilégios administrativos, por exemplo, o usuário `administrator@your_domain_name`.

Resultados

Se você tiver registrado o VMware Cloud Director no vCenter Lookup Service, os **administradores do sistema** deverão fazer login no VMware Cloud Director com suas credenciais do vCenter Single Sign-On.

Monitorando o VMware Cloud Director

12

Os administradores do sistema podem monitorar operações concluídas e em andamento, e exibir informações de uso de recursos no centro de dados virtual do provedor, no centro de dados virtual da organização e no nível do datastore.

Começando com a versão 9.1, o VMware Cloud Director não é compatível com o VMware vCenter Chargeback Manager. Consulte as [Matrizes de interoperabilidade entre produtos VMware](#).

Este capítulo inclui os seguintes tópicos:

- [Relatórios de custos e VMware Cloud Director](#)
- [Visualizar informações de uso para um centro de dados virtual do provedor](#)

Relatórios de custos e VMware Cloud Director

Você pode usar o VMware vRealize Operations Tenant App para o VMware Cloud Director configurar um sistema de relatório de custos para o VMware Cloud Director.

O VMware vRealize Operations Tenant App apresenta recursos de medição que permitem aos provedores de serviços fornecerem sua base de clientes com serviços de chargeback.

O VMware vRealize Operations Tenant App também é um aplicativo voltado para o tenant que fornece aos administradores de tenant visibilidade do seu ambiente e dos dados de faturamento.

Para obter informações sobre compatibilidade entre o VMware Cloud Director e o VMware vRealize Operations Tenant App, consulte as *Matrizes de interoperabilidade de produtos VMware* em http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Você pode baixar o VMware vRealize Operations Tenant App em <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director>.

Para obter informações sobre como usar o VMware vRealize Operations Tenant App, consulte *Usando o Aplicativo de Tenant do vRealize Operations para VMware Cloud Director como um Provedor de Serviços* e *Usando o Aplicativo de Tenant do vRealize Operations para VMware Cloud Director como um Tenant*.

Visualizar informações de uso para um centro de dados virtual do provedor

Os centros de dados virtuais do provedor oferecem recursos de processamento, memória e armazenamento aos centros de dados virtuais da organização. É possível monitorar o uso dos recursos do centro de dados virtual do provedor para que você possa decidir adicionar mais recursos.

Procedimentos

- 1 Na barra de navegação superior, selecione **Recursos** e clique em **Recursos de Nuvem**.
- 2 No painel esquerdo, selecione **VDCs do Provedor** e clique no nome do centro de dados virtual de provedor de destino.
- 3 Clique na guia **Configurar > Métricas**.
- 4 Para obter detalhes sobre cada parâmetro, clique em cada ícone de informação.

O modo de exibição de conteúdo Bibliotecas no VMware Cloud Director Service Provider Admin Portal fornece uma interface para a integração com o vRealize Orchestrator. Os fluxos de trabalho do vRealize Orchestrator estão disponíveis como catálogo de serviços que os administradores do provedor de serviços podem publicar para os tenants ou outros provedores de serviços, e dessa forma estender o conjunto de funcionalidades e recursos de gerenciamento que oferecem.

Este capítulo inclui os seguintes tópicos:

- [Integração do vRealize Orchestrator ao VMware Cloud Director](#)
- [Criar uma categoria de serviço](#)
- [Editar uma categoria de serviço](#)
- [Importar um serviço](#)
- [Procurar um serviço](#)
- [Executar um serviço](#)
- [Alterar uma categoria de serviço](#)
- [Cancelar o registro de um serviço](#)
- [Publicar um serviço](#)

Integração do vRealize Orchestrator ao VMware Cloud Director

Você integra o vRealize Orchestrator ao VMware Cloud Director por meio do VMware Cloud Director Service Provider Admin Portal.

A integração do vRealize Orchestrator ao VMware Cloud Director estende a funcionalidade base do VMware Cloud Director, permitindo que os administradores de provedor de serviços desenvolvam tarefas de automação complexas por meio da orquestração do fluxo de trabalho e da utilização de plug-ins de terceiros.

Através do VMware Cloud Director Service Provider Admin Portal, os administradores do provedor de serviços são capazes de exibir, importar e executar fluxos de trabalho de instâncias do servidor do vRealize Orchestrator registradas.

No VMware Cloud Director Service Provider Admin Portal, os fluxos de trabalho do vRealize Orchestrator podem ser publicados em provedores de serviços ou tenants, permitindo o controle de acesso rápido e a execução dos serviços personalizados e internos.

O vRealize Orchestrator tem uma biblioteca de fluxo de trabalho extensa que contém tarefas predefinidas projetadas para resolver desafios específicos e realizar tarefas administrativas comuns. Os plug-ins de terceiros também estão disponíveis no [VMware Solution Exchange](#).

Registrar uma instância do vRealize Orchestrator no VMware Cloud Director

Para aproveitar a orquestração de fluxos de trabalho e a automação de tarefas pelo vRealize Orchestrator no VMware Cloud Director, você pode registrar uma instância do vRealize Orchestrator no VMware Cloud Director Service Provider Admin Portal.

Pré-requisitos

- Implante e configure uma instância de servidor do vRealize Orchestrator. Para obter mais informações, consulte *Instalando e configurando o VMware vRealize Orchestrator* na documentação do vRealize Orchestrator.
- Configure o vRealize Orchestrator para usar o vSphere como um provedor de autenticação.
- Certifique-se de que o VMware Cloud Director esteja registrado no serviço de pesquisa do mesmo Controlador de Serviços de Plataforma que o vCenter Single Sign-On usado pelo vRealize Orchestrator para autenticação.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**
 - a No painel esquerdo, selecione **Gerenciamento de Serviços**.
É exibida uma lista de servidores vRealize Orchestrator registrados.
- 2 Para registrar um novo servidor vRealize Orchestrator, clique em **Adicionar**.
É exibida a caixa de diálogo **Registrar o vRealize Orchestrator**.
- 3 Insira os seguintes valores.

Opção	Descrição
Nome	Nome da instância do vRealize Orchestrator registrada.
Descrição	Descrição da instância do servidor do vRealize Orchestrator registrada.
Nome de host	O nome de domínio totalmente qualificado e a porta do servidor vRealize Orchestrator. O valor da porta HTTPS padrão é 443. Observação O VMware Cloud Director se conecta à interface de API do vRealize Orchestrator.
Nome de usuário	Uma conta de usuário que é membro do grupo de administradores do vRealize Orchestrator.

Opção	Descrição
Senha	A senha para a conta de administrador do vRealize Orchestrator.
Âncora de Confiança	O certificado SSL do servidor do vRealize Orchestrator em um formato PEM. Clique no ícone de upload para localizar e selecionar o arquivo .pem.

- 4 Clique em **OK** para concluir o registro.

O servidor do vRealize Orchestrator está registrado no VMware Cloud Director.

Criar uma categoria de serviço

Você pode organizar os serviços em categorias de serviço.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**
 - a No painel esquerdo, selecione **Gerenciamento de Serviços**.
 - b Navegue até a guia **Categorias de Serviço**.

É exibida uma lista de categorias de servidor existentes.

- 2 Para criar uma nova categoria de serviço, clique em **Adicionar**.

A caixa de diálogo **Nova Categoria de Serviço** é exibida.

- 3 Insira os seguintes valores.


Opção	Descrição
Nome	Nome da categoria de serviço.
Ícone	Importe o ícone exibido para a categoria de serviço.
Descrição	Breve descrição da categoria de serviço.

Editar uma categoria de serviço

Você pode editar as categorias de serviço existentes.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**
 - a No painel esquerdo, selecione **Gerenciamento de Serviços**.
 - b Navegue até a guia **Categorias de Serviço**.

É exibida uma lista de categorias de servidor existentes.
- 2 Use a barra de lista () no lado esquerdo de uma categoria de serviço selecionada e clique em **Editar**.

3 Edite os seguintes valores.

Opção	Descrição
Nome	Nome da categoria de serviço.
Ícone	Importe o ícone exibido para a categoria de serviço.
Descrição	Breve descrição da categoria de serviço.

Importar um serviço

Você pode importar serviços da biblioteca de fluxo de trabalho de uma instância do vRealize Orchestrator que está registrada com o VMware Cloud Director.

Pré-requisitos

- Registre uma instância do vRealize Orchestrator. Consulte [Registrar uma instância do vRealize Orchestrator no VMware Cloud Director](#).
- Crie uma categoria de serviço. Consulte [Criar uma categoria de serviço](#).

Procedimentos

1 Na barra de navegação superior, selecione **Bibliotecas**.

a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

2 Para importar um novo serviço, clique no botão **Importar**.

3 Siga as etapas do Assistente de **Importação**.

Opção	Descrição
Importar para biblioteca de destino	Selecione a categoria de serviço para a qual deseja importar o serviço.
Selecionar fonte	Selecione a instância do vRealize Orchestrator da qual deseja importar fluxos de trabalho.
Selecionar fluxos de trabalho	Expand a exibição de árvore hierárquica para selecionar um ou vários fluxos de trabalho para importação.
Revisão	Revise os detalhes e clique em Concluído para concluir a importação.

Os fluxos de trabalho importados aparecem na exibição de cartões da **Biblioteca de Serviço**.

Procurar um serviço

Você pode procurar um serviço pelo seu nome ou pela categoria de serviço à qual ele pertence.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

- 2 Na caixa de texto **Pesquisa** no topo da página, insira uma palavra ou um caractere do nome do serviço ou da categoria de serviço que você deseja localizar.

- 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 fluxos de trabalho do vRealize Orchestrator como serviços importados.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

- 2 Para executar um serviço, no cartão do serviço selecionado, clique em **Executar**.

O assistente de **Executar um serviço** é exibido.

- 3 Preencha os parâmetros de entrada do serviço necessários e clique em **Concluir**.

Resultados

Você pode monitorar o status da execução no modo de exibição de **Tarefas recentes**. Para obter mais informações, consulte [Exibir tarefas](#).

Observação Quando você inicia um fluxo de trabalho do vRealize Orchestrator como serviço do VMware Cloud Director, VMware Cloud Director alguns parâmetros personalizados são adicionados ao contexto de execução do fluxo de trabalho.

Propriedade personalizada	Descrição
_vcd_orgName	Nome da organização à qual pertence o usuário que executa o serviço.
_vcd_orgId	ID da organização à qual pertence o usuário que executa o serviço.
_vcd_username	Nome do usuário que executa o serviço.
_vcd_isAdmin	Tem valor <code>True</code> se o usuário que executa o serviço é administrador .
_vdc_isAdmin	Obsoleto. Tem valor <code>True</code> se o usuário que executa o serviço é administrador .
_vdc_username	Obsoleto. Nome do usuário que executa o serviço.
_vcd_sessionToken	Token de autenticação que você recebeu após a autenticação bem-sucedida no VMware Cloud Director
_vcd_apiEndpoint	Endpoint da API REST do VMware Cloud Director

Alterar uma categoria de serviço

Você pode alterar a categoria à qual um serviço pertence.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

- 2 No cartão do serviço selecionado, selecione **Gerenciar > Alterar Categoria**.

A caixa de diálogo **Alterar Categoria** é aberta.

- 3 Selecione a categoria na qual deseja colocar o serviço e clique em **Salvar**.

Cancelar o registro de um serviço

Você pode remover o acesso a um serviço para provedores de serviço e locatários, cancelando o registro desse serviço.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

- 2 No cartão do serviço selecionado, selecione **Gerenciar > Cancelar Registro do Fluxo de Trabalho**.

A caixa de diálogo **Cancelar Registro do Fluxo de Trabalho** é aberta.

- 3 Para remover o serviço da biblioteca de serviços, clique em **Excluir**.

Publicar um serviço

Você pode controlar o acesso do provedor de serviços e do tenant aos serviços publicando esses serviços.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Biblioteca de Serviço**.

Os serviços disponíveis são exibidos em um modo de exibição de cartão de doze itens por página, classificados por nomes em ordem alfabética. Cada placa indica que o item é um fluxo de trabalho do vRealize Orchestrator e mostra o nome do serviço e uma marca que corresponde à categoria de serviço, na qual o fluxo de trabalho é importado.

- 2 No cartão do serviço selecionado, selecione **Gerenciar > Publicar Fluxo de Trabalho**.

É exibida a caixa de diálogo **Publicar Fluxo de Trabalho**.

- 3 Para publicar para provedores de serviços, selecione **Publicar para Provedores de Serviços** e clique em **Salvar**.

- 4 Para publicar para uma organização de tenant específica, selecione o botão **Publicar para Tenants**.

- a É exibida uma lista com organizações de tenant disponíveis. Selecione a organização de tenant para a qual publicar o fluxo de trabalho e clique em **Salvar**.

- 5 Para publicar para todas as organizações de tenant, selecione **Publicar para Todos os Tenants** e clique em **Salvar**.

Gerenciamento de entidades definidas

14

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.

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:** ao criar um tipo de RDE, você cria um pacote de direitos para o tipo. Para fornecer acesso a operações específicas, você deve atribuir direitos desse pacote a outras funções. Cada pacote tem 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.

Os **administradores do sistema** com o direito **Exibir ACL Geral** podem exibir as ACLs atribuídas a uma entidade definida específica usando a API de `accessControls`. Para obter referência da API do VMware Cloud Director, consulte code.vmware.com.

Os **administradores do sistema** com o direito **Gerenciar ACL Geral** podem criar, modificar e remover ACLs específicas usando a API de `accessControls`.

Tabela 14-1. Direitos e entradas da ACL para operações da RDE

Operação da entidade	Opção	Descrição
Leitura	Direito Exibição do Administrador: TYPE	Os usuários com esse direito podem ver todas as RDEs desse tipo dentro de uma organização.
	Direito Exibir: TYPE e entrada da ACL >= Exibir	Os usuários com esse direito e uma ACL de nível de leitura podem exibir RDEs desse tipo.
Modificar	Direito Controle Total do Administrador: TYPE	Os usuários com esse direito podem criar, exibir, modificar e excluir RDEs desse tipo em todas as organizações.
	Direito Editar: TYPE e entrada da ACL >= Alterar	Os usuários com esse direito e a ACL de nível de modificação podem criar, exibir e modificar RDEs desse tipo.
Excluir	Direito Controle Total do Administrador: TYPE	Os usuários com esse direito podem criar, exibir, modificar e excluir RDEs desse tipo em todas as organizações.
	Direito Controle Total: TYPE e entrada da ACL = Controle Total	Os usuários com esse direito e a ACL de nível de controle total podem criar, exibir, modificar e excluir RDEs desse tipo.

Você pode usar a API ou a interface de usuário do VMware Cloud Director para publicar o pacote de direitos em todas as organizações que você deseja gerenciar as entidades desse tipo. Depois de publicar o pacote de direitos, você pode atribuir direitos do pacote a funções na organização.

Você pode usar a API do VMware Cloud Director para editar a tabela da ACL.

Este capítulo inclui os seguintes tópicos:

- [Compartilhamento de entidades definidas](#)
- [Gerenciamento de entidades personalizadas](#)

Compartilhamento de entidades definidas

Você pode conceder acesso às Runtime Defined Entities (RDEs) compartilhando-as com outros administradores de sistema ou tenants.

Compartilhando as entidades definidas com outro usuário

- 1 Se você quiser conceder acesso a entidades definidas para tenants, publique o pacote de direitos do tipo de entidade definida em uma organização de tenant. Por exemplo, para a criação e o gerenciamento de clusters do Tanzu Kubernetes, você deve publicar o pacote de direitos **vmware:tkgcluster Entitlement**. Consulte [Publicar ou cancelar a publicação de um pacote de direitos](#).

Se você quiser compartilhar a entidade definida com um **administrador do sistema**, pule essa etapa.

- 2 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.

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.

- 3 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.

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.

Você também pode usar chamadas à API REST para revogar acesso ou para exibir quem tem acesso à entidade. Consulte a documentação da REST API do VMware Cloud Director em code.vmware.com.

Compartilhando direitos de administrador para entidades definidas

- 1 Se você quiser conceder acesso a entidades definidas para tenants, publique o pacote de direitos do tipo de entidade definida em uma organização de tenant. Por exemplo, para a criação e o gerenciamento de clusters do Tanzu Kubernetes, você deve publicar o pacote de direitos **vmware:tkgcluster Entitlement**. Consulte [Publicar ou cancelar a publicação de um pacote de direitos](#).

Se você quiser compartilhar a entidade definida com um **administrador do sistema**, pule essa etapa.

- 2 Atribua o direito **Exibição do Administrador: TYPE** ou **Controle Total do Administrador: TYPE** do pacote para as funções de usuário que você deseja ter o nível específico de acesso à entidade definida.

Por exemplo, se você quiser que os usuários com essa função visualizem todos os clusters do Tanzu Kubernetes na organização, deverá adicionar o direito **Exibição do Administrador: Tanzu Kubernetes Guest Cluster** à função. Se você quiser que os usuários com essa função criem, exibam, modifiquem e excluam clusters do Tanzu Kubernetes em todas as organizações, adicione o direito **Controle Total do Administrador: Tanzu Kubernetes Guest Cluster** à função do usuário.

Os usuários com o direito **Controle Total do Administrador: Tanzu Kubernetes Guest Cluster** podem conceder acesso à ACL para qualquer entidade VMWARE:TKGCLUSTER.

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.

Gerenciamento 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. Quando um provedor de serviços publica definições de uma entidade personalizada para qualquer outro provedor de serviços, ou para um ou mais tenants, os usuários do VMware Cloud Director podem obter, gerenciar e alterar esses tipos de acordo com suas necessidades. Ao executar serviços, os usuários do provedor de serviços e os usuários da organização podem instanciar entidades personalizadas e aplicar ações sobre as instâncias dos objetos.

Procurar uma entidade personalizada

Você pode procurar uma entidade personalizada por seu nome.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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. Você não pode alterar o tipo da entidade ou o tipo de objeto do vRealize Orchestrator ao qual a entidade está vinculada. Estas 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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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**.

Abre uma nova caixa de diálogo.

- 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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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**.

Etapa	
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. Observação Se você tiver mais de um servidor do vRealize Orchestrator, deverá criar uma definição de entidade personalizada para cada um deles separadamente.
Tipo	Clique no ícone de lista de exibição para navegar pelos tipos de objeto disponíveis do vRealize Orchestrator agrupados por plug-ins. Por exemplo, SSH > Host . Se você souber o nome do tipo, poderá inseri-lo diretamente na caixa de texto. Por exemplo, <code>SSH:Host</code> .
Revisão	Revise os detalhes que você especificou e clique em Concluído 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.

Procedimentos


- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.
 - a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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**.
Abre uma nova caixa de diálogo.
- 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 Biblioteca de Serviços .
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	Análise os detalhes que você especificou e clique em Concluído 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 entidade personalizada

Você pode remover um fluxo de trabalho do vRealize Orchestrator na lista de ações associadas.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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**.

Abre uma nova caixa de diálogo.

- 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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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**.

Abre uma nova caixa de diálogo.

- 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.

Procedimentos

- 1 Na barra de navegação superior, selecione **Bibliotecas**.

- a No painel esquerdo, selecione **Definições de Entidades Personalizadas**.

A lista de entidades personalizadas aparece em uma exibição de cartão de 12 itens por página, ordenados 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.