

Uso e gerenciamento do vRealize Automation Cloud Assembly

Dezembro de 2022
vRealize Automation 8.7

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 © 2022 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

1 O que é o Cloud Assembly 8

Como funciona o Cloud Assembly 9

2 Tutoriais 12

Implantando uma máquina virtual 14

Configurando e testando a infraestrutura e as implantações do vSphere 21

Configurando e provisionando uma carga de trabalho de produção 39

Usando tags para gerenciar recursos do vSphere 46

Adicionando um modelo de nuvem ao catálogo do Service Broker com um formulário de solicitação personalizado 57

Integrando e gerenciando recursos do vSphere 69

Infraestrutura e implantações em várias nuvens 79

Parte 1: Configurar a infraestrutura de exemplo 79

Parte 2: Criar o projeto de exemplo 86

Parte 3: Projetar e implantar o exemplo de modelo de nuvem 87

Configurando o VMware Cloud on AWS 105

Configurar um fluxo de trabalho básico do VMware Cloud on AWS 105

Configurar uma rede isolada no VMware Cloud on AWS 119

Configurando uma integração de IPAM externo para Infoblox 124

Adicionar atributos extensíveis necessários no aplicativo Infoblox antes de implantar o pacote de download 126

Baixar e implantar um pacote de provedor de IPAM externo 127

Criar um ambiente em execução para um ponto de integração de IPAM 129

Adicionar uma integração de IPAM externo para Infoblox 131

Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente 134

Definir e implantar um modelo de nuvem que usa uma atribuição de intervalo de provedor de IPAM externo 137

Uso de propriedades específicas do Infoblox para integrações de IPAM em modelos de nuvem 140

Controlar a coleta de dados de rede usando filtros Infoblox 144

3 Como configurar o Cloud Assembly para sua organização 147

Quais são as funções de usuário do vRealize Automation 147

Funções de usuário de serviço e organização 150

Personalizar funções de usuário 173

Casos de uso: Como funções de usuário podem me ajudar a controlar o acesso 177

Função integrada de Administrador de Infraestrutura 199

Como adicionar contas de nuvem 201

| | |
|---|-----|
| Credenciais necessárias para trabalhar com contas de nuvem | 201 |
| Criar uma conta de nuvem do Microsoft Azure | 220 |
| Criar uma conta de nuvem do Amazon Web Services | 225 |
| Criar uma conta de nuvem do Google Cloud Platform | 226 |
| Criar uma conta de nuvem do vCenter | 228 |
| Criar uma conta de nuvem do NSX-V | 230 |
| Criar uma conta de nuvem do NSX-T | 231 |
| Criar uma conta de nuvem do VMware Cloud on AWS | 235 |
| Criar uma conta de nuvem do VMware Cloud Foundation | 237 |
| Criar uma conta de nuvem do VMware Cloud Director no vRealize Automation | 238 |
| Integração com outros aplicativos | 244 |
| Como usar a integração com o GitLab e o GitHub | 245 |
| Como configurar uma integração externa de IPAM | 251 |
| Como fazer upgrade para um pacote de integração de IPAM externo mais recente | 253 |
| Configurar a integração do My VMware no Cloud Assembly | 254 |
| Configurar uma integração do vRealize Orchestrator no Cloud Assembly | 255 |
| Como trabalhar com o Kubernetes no Cloud Assembly | 260 |
| O que é o gerenciamento de configuração no Cloud Assembly | 288 |
| Criar uma integração com o SaltStack Config | 303 |
| Como criar uma integração do Active Directory no Cloud Assembly | 308 |
| Configurar uma integração do VMware SDDC Manager | 311 |
| Integrando com o vRealize Operations Manager | 312 |
| O que são planos de integração | 329 |
| Máquinas selecionadas integradas como uma implantação única | 331 |
| Configuração avançada | 334 |
| Como configurar um servidor proxy de Internet | 334 |
| O que posso fazer com o mapeamento do NSX-T para vários vCenters | 337 |
| O que acontecerá se eu remover uma associação de conta de nuvem do NSX | 338 |
| Como usar o SDK de IPAM para criar um pacote de integração de IPAM externo específico do provedor | 339 |
| Usando o vRealize Automation com a Azure VMware Solution | 340 |
| Usando o vRealize Automation com o Google Cloud VMware Engine | 341 |
| Usando o vRealize Automation com a Oracle Cloud VMware Solution | 341 |
| Usando o vRealize Automation com o VMware Cloud on Dell EMC | 342 |

4 Como compilar a infraestrutura de recursos 343

| | |
|---|-----|
| Como adicionar zonas de nuvem | 343 |
| Saiba mais sobre as zonas de nuvem | 344 |
| Como adicionar mapeamentos de tipo | 347 |
| Saiba mais sobre os mapeamentos de tipo | 348 |
| Como adicionar mapeamentos de imagem | 348 |
| Saiba mais sobre mapeamentos de imagem | 349 |

| | |
|--|-----|
| Como adicionar perfis de rede | 355 |
| Saiba mais sobre perfis de rede | 355 |
| Usando configurações de rede | 362 |
| Usando configurações de grupos de segurança | 367 |
| Usando configurações de balanceador de carga | 368 |
| Como configurar um perfil de rede para oferecer suporte a uma rede sob demanda para uma integração de IPAM externa | 369 |
| Como configurar um perfil de rede para oferecer suporte a uma rede existente para uma integração de IPAM externa | 373 |
| Como adicionar perfis de armazenamento | 373 |
| Saiba mais sobre perfis de armazenamento | 374 |
| Como uso cartões de preços | 378 |
| Como criar cartões de preços para o vSphere e o VMC | 380 |
| Como usar tags | 385 |
| Criação de uma estratégia de marcação | 388 |
| Como usar tags de capacidade no Cloud Assembly | 389 |
| Como usar tags de restrição no Cloud Assembly | 391 |
| Tags padrão | 393 |
| Como o Cloud Assembly processa tags | 394 |
| Como configurar uma estrutura de marcação simples | 394 |
| Como trabalhar com recursos | 396 |
| Recursos de processamento | 397 |
| Recursos de rede | 397 |
| Recursos de segurança | 400 |
| Recursos de armazenamento | 403 |
| Saiba mais sobre recursos | 403 |
| Configurando recursos de tenant de vários provedores com o vRealize Automation | 426 |
| Como criar uma zona privada virtual para o vRealize Automation | 426 |
| Gerenciar a configuração da Zona Privada Virtual para tenants do vRealize Automation | 430 |
| Criar mapeamento global de tipo e imagem para tenants do vRealize Automation | 431 |
| Configurar mapeamentos de tipo e imagem específicos do tenant para vRealize Automation | 435 |
| Criar assinaturas de extensibilidade para provedores ou tenants | 436 |
| Como trabalhar com zonas privadas virtuais legadas em versões mais recentes do vRealize Automation | 437 |

5 Como adicionar e gerenciar projetos 439

| | |
|--|-----|
| Como adicionar um projeto para a minha equipe de desenvolvimento | 439 |
| Saiba mais sobre projetos | 442 |
| Usando tags de projeto e propriedades personalizadas | 442 |
| Usando políticas de posicionamento em nível de projeto | 444 |
| Quais são os custos do projeto | 449 |
| Como os projetos funcionam no momento da implantação | 449 |

| | | |
|----------|---|------------|
| 6 | Como projetar suas implantações | 451 |
| | Primeiros passos com designs | 453 |
| | Ajuda para complementação de código | 456 |
| | Associações e dependências | 458 |
| | Controle de versão de modelos | 460 |
| | Entrada do usuário em solicitações | 462 |
| | Ações do vRealize Orchestrator como entradas | 469 |
| | Grupos de propriedades | 473 |
| | Grupos de propriedades de entrada | 474 |
| | Grupos de propriedades constantes | 485 |
| | Saiba mais sobre grupos de propriedades | 488 |
| | Sinalizadores de recursos para solicitações | 489 |
| | Expressões | 492 |
| | Sintaxe de expressões | 495 |
| | Propriedades secretas | 502 |
| | Acesso remoto | 503 |
| | Posicionamento de discos SCSI | 507 |
| | Inicialização de máquinas | 510 |
| | Especificações de personalização do vSphere | 511 |
| | Comandos de configuração | 512 |
| | Endereços IP estáticos do vSphere | 514 |
| | Implantação atrasada | 520 |
| | Personalização de guests do Windows | 521 |
| | Clusters de máquina e disco | 525 |
| | Nomenclatura personalizada para recursos implantados | 527 |
| | Recurso do SaltStack Config | 530 |
| | Configurações do Terraform | 537 |
| | Preparando um ambiente de tempo de execução do Terraform | 537 |
| | Preparando para configurações do Terraform | 544 |
| | Projetando para configurações do Terraform | 546 |
| | Saiba mais sobre as configurações do Terraform | 551 |
| | Tipos de recursos personalizados | 554 |
| | Como criar um modelo de nuvem que adiciona usuários ao Active Directory | 558 |
| | Como criar um modelo de nuvem que inclui SSH | 564 |
| | Preparando-se para o dia 2 | 568 |
| | Como usar entradas de modelo de nuvem para atualizações de dia 2 | 568 |
| | Como criar uma ação de recurso para aplicar o vMotion a uma máquina virtual | 570 |
| | Outros exemplos de código | 578 |
| | Modelo de nuvem revisável | 579 |
| | Exemplos de recursos do vSphere | 586 |
| | Núcleos por soquete e contagem de CPUs | 589 |

| | |
|--|-----|
| Redes, recursos de segurança e balanceadores de carga | 590 |
| Modelo de nuvem habilitado para Puppet com acesso de nome de usuário e senha | 620 |
| Esquema de propriedades de recursos | 630 |
| Propriedades especiais | 630 |
| Outras maneiras de criar modelos | 630 |
| Estendendo e automatizando ciclos de vida de aplicativos | 631 |
| Assinaturas de ação de extensibilidade | 632 |
| Assinaturas de fluxo de trabalho de extensibilidade | 660 |
| Saiba mais sobre assinaturas de extensibilidade | 667 |

7 Gerenciamento de implantações e recursos 682

| | |
|---|-----|
| Como gerenciar implantações | 682 |
| Como monitorar implantações | 686 |
| O que fazer se uma implantação do Cloud Assembly falhar | 688 |
| Como gerenciar o ciclo de vida de uma implantação concluída | 691 |
| Quais ações posso executar nas implantações | 696 |
| Gerenciando recursos | 711 |
| Como trabalhar com recursos individuais | 715 |
| Como trabalhar com máquinas descobertas | 717 |

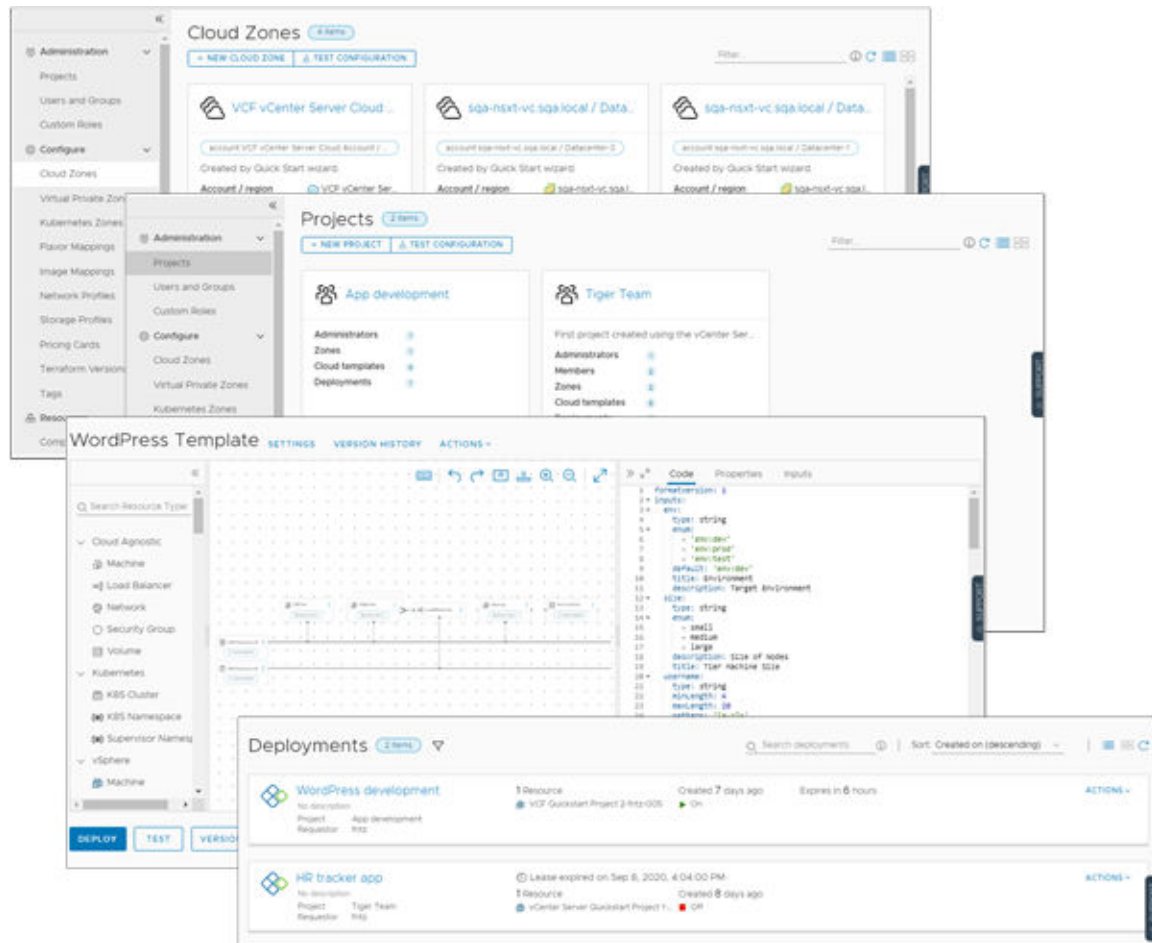
O que é o Cloud Assembly

1

Você usa o vRealize Automation Cloud Assembly para se conectar aos seus provedores de nuvem pública e privada, para poder implantar máquinas, aplicativos e serviços criados para esses recursos. Você e suas equipes desenvolvem modelos de nuvem como código em um ambiente que suporta um fluxo de trabalho iterativo, do desenvolvimento até o teste para produção. No momento do provisionamento, é possível implantar em uma variedade de fornecedores de nuvem. O serviço é uma estrutura gerenciada da VMware baseada em SaaS e NaaS.

Uma visão geral do Cloud Assembly inclui as seguintes funções básicas.

- A guia Recursos mostra o status atual dos seus recursos provisionados, descobertos, integrados e outros. É possível acessar os detalhes dos recursos e as ações de dia 2 que você usa para gerenciá-los.
- A guia Projetar é a página inicial de desenvolvimento. Use a tela e o editor YAML para desenvolver e, em seguida, implantar máquinas e aplicativos.
- A guia Infraestrutura é onde você adiciona e organiza os recursos e usuários do fornecedor de nuvem. Essa guia também fornece informações sobre modelos de nuvem implantados.
- A guia Extensibilidade é onde é possível estender e automatizar seus ciclos de vida do aplicativo. É possível assinar eventos que são usados para disparar ações de extensibilidade ou fluxos de trabalho do vRealize Orchestrator.
- "A guia Alertas fornece notificações sobre capacidade, desempenho e disponibilidade para seus recursos de infraestrutura." Você deve configurar uma integração com o vRealize Operations Manager para ver e usar os alertas.
- A guia Gerenciamento de Tenants mostra os diferentes tenants que você configurou se você é um provedor de serviços e permite alocar ou desalocar zonas privadas virtuais.



Este capítulo inclui os seguintes tópicos:

- [Como funciona o Cloud Assembly](#)

Como funciona o Cloud Assembly

O Cloud Assembly é um serviço de desenvolvimento e implantação de modelo de nuvem. Você e suas equipes usam o serviço para implantar máquinas, aplicativos e serviços em seus recursos de fornecedor de nuvem.

Como administrador do Cloud Assembly, geralmente chamado de administrador da nuvem, você configura a infraestrutura de provisionamento e cria os projetos que agrupam usuários e recursos.

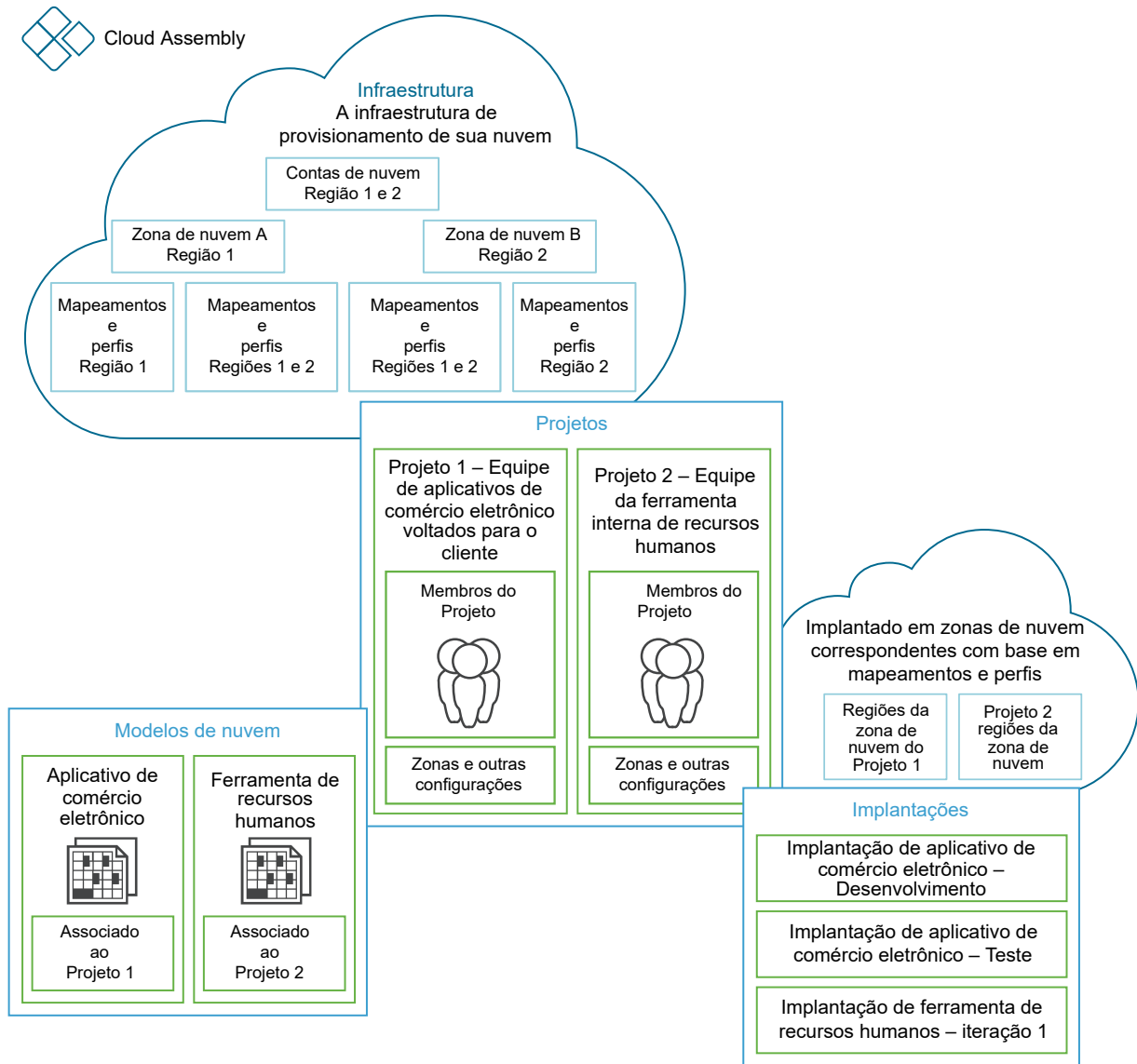
- Adicione suas contas de fornecedor de nuvem. Consulte [Como adicionar contas de nuvem ao Cloud Assembly](#).
- Determine quais regiões ou repositórios de dados são as zonas de nuvem que deseja que seus desenvolvedores implantem. Consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).
- Crie políticas que definem as zonas de nuvem. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).

- Crie projetos que agrupem os desenvolvedores com as zonas de nuvem. Consulte [Usando tags de projeto e propriedades personalizadas do Cloud Assembly](#) .

Como desenvolvedor de modelo de nuvem, você é membro de um ou mais projetos. Crie e implante modelos nas zonas de nuvem associadas a um dos seus projetos.

- Desenvolva modelos de nuvem para projetos usando a tela de design. Consulte [Primeiros passos com designs do Cloud Assembly](#).
- Implante seus modelos de nuvem para projetar zonas de nuvem com base em políticas e restrições.
- Gerencie suas implantações, incluindo a exclusão de aplicativos não utilizados. Consulte [Como gerenciar implantações do Cloud Assembly](#).

Bem-vindo ao Cloud Assembly. Para ver um exemplo de como definir a infraestrutura, depois, criar e implantar um modelo de nuvem, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).



Tutoriais do Cloud Assembly

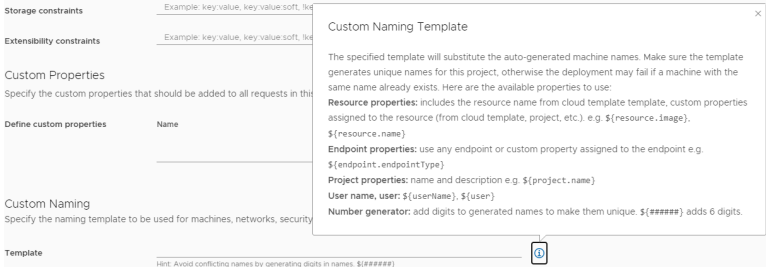
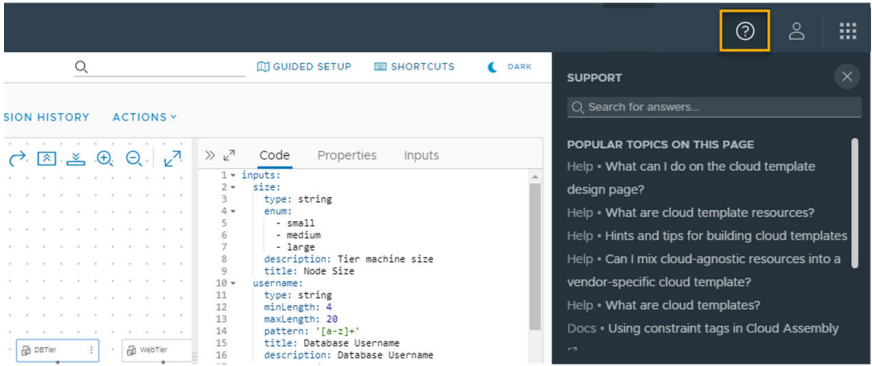
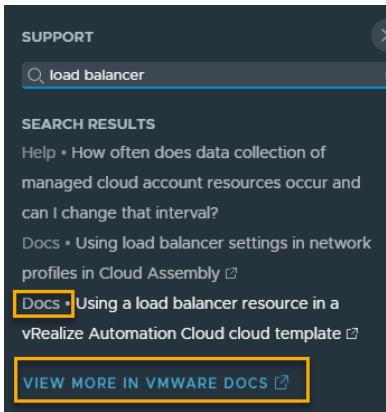
2

Os tutoriais mostram como realizar tarefas comuns que ajudam você a se tornar proficiente no Cloud Assembly.

Antes de começar, lembre-se de que, além das etapas nos tutoriais, há informações adicionais neste guia. São fornecidos links para tópicos relevantes.

Como acessar a assistência ao usuário

Igualmente importante, a assistência ao usuário é fornecida em todo o aplicativo. A assistência ao usuário ajuda você a compreender recursos e fornece informações que ajudam a tomar decisões sobre como preencher caixas de texto. A documentação externa fornece maior profundidade, além de amostras de código e casos de uso.

| Tipo de assistência | Como acessar a assistência | Exemplo |
|--|---|--|
| Ajuda de sinalização em nível de campo | Clique no ícone Informações (i) ao lado de um campo. |  |
| Ajuda do painel de suporte contextual | Clique no ícone de ajuda (?) ao lado do seu nome e organização. |  |
| Acessar a documentação externa | Clique em um título de artigo com o rótulo Docs ou clique em Exibir Mais no VMware Docs . |  |

Este capítulo inclui os seguintes tópicos:

- Tutorial: Implantando uma máquina virtual no Cloud Assembly
- Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly
- Tutorial: configurando o Cloud Assembly para provisionar uma carga de trabalho de produção
- Tutorial: Usando tags no Cloud Assembly para gerenciar recursos do vSphere
- Tutorial: Adicionando um modelo de nuvem do Cloud Assembly ao catálogo do Service Broker com um formulário de solicitação personalizado
- Tutorial: integrando e gerenciando recursos do vSphere no vRealize Automation

- [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#)
- [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#)
- [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#)

Tutorial: Implantando uma máquina virtual no Cloud Assembly

Como administrador do Cloud Assembly, é possível implantar uma máquina virtual simples que não exige que você saiba como criar um modelo de nuvem. Se você não tem experiência no Cloud Assembly, este tutorial o orienta pelo processo de configuração, pela criação da máquina virtual e mostra onde gerenciar a máquina implantada.

Esse método é uma maneira fácil de implantar rapidamente uma máquina com base em modelos de imagem, tipos de dimensionamento, armazenamento e redes definidos pelo provedor de nuvem. Trata-se de um teste rápido da sua conta e projetos de nuvem.

Você pode criar uma máquina virtual para qualquer um dos provedores de serviços de nuvem a seguir.

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- vCenter Server
- VMware Cloud on AWS

A Google Cloud Platform é o exemplo neste tutorial.

Antes de começar

- Verifique se você tem a função Administrador do Cloud Assembly. Consulte [Funções de usuário de serviço e organização no vRealize Automation](#). Se você não tem essa função de usuário, não vê a opção de criar uma VM.

Etapa 1: Adicionar uma conta de nuvem

As contas de nuvem fornecem as credenciais que o Cloud Assembly usa para conexão com o provedor de nuvem.

- 1 Selecione **Infraestrutura > Conexões > Contas da Nuvem**.
- 2 Clique em **Adicionar Conta de Nuvem** e selecione o tipo de conta.

Pode aceder aos detalhes da configuração utilizando os seguintes links.

- [Criar uma conta de nuvem do Amazon Web Services no vRealize Automation](#)

- Criar uma conta de nuvem do Google Cloud Platform no vRealize Automation
- Criar uma conta de nuvem do Microsoft Azure no vRealize Automation
- Criar uma conta de nuvem do vCenter no vRealize Automation
- Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation

Depois que você adicionar a conta de nuvem, o Cloud Assembly coletará informações de recursos da conta do provedor de nuvem de destino que serão usadas posteriormente para implantar uma máquina virtual.

Etapa 2: Criar um projeto

O projeto associa os usuários e as zonas de nuvem da conta.

Neste tutorial, o nome do projeto é Criar Projeto de VM. Este projeto é um projeto de demonstração que inclui zonas de nuvem para todas as plataformas compatíveis.

- 1 Selecione **Infraestrutura > Administração > Projetos**.
- 2 Clique em **Novo Projeto**.
- 3 Digite um nome.

Neste tutorial, o nome é **Criar Projeto de VM**.

- 4 Se você deseja que outra pessoa use esse projeto, clique na guia **Usuários** e adicione usuários ao projeto.
- 5 Clique na guia **Provisionamento** e em **Adicionar Zona** para adicionar pelo menos uma zona de nuvem às contas de nuvem nas quais você está implantando.

Lembre-se de que este é um projeto de demonstração que inclui uma zona de nuvem para cada plataforma de fornecedor de nuvem compatível.

Create VM Project DELETE

Summary Users **Provisioning** Kubernetes Provisioning Integrations

Zones
Specify the zones that can be used when users provision deployments in this project. ⓘ

+ADD ZONE × REMOVE

| <input type="checkbox"/> | Name | Status | Description | Priority | Instances | Memory Limit (MB) | CPU Limit | Storage Limit (GB) | Capability Tags |
|--------------------------|----------------------------------|--------|-------------|----------|-----------|-------------------|-----------|--------------------|-----------------|
| <input type="checkbox"/> | dsadsa-vsphere / SDDC-Datacenter | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |
| <input type="checkbox"/> | yingzhi-GCP / us-east1 | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |
| <input type="checkbox"/> | AWS / af-south-1 | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |
| <input type="checkbox"/> | vc65 / Datacenter | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |
| <input type="checkbox"/> | Azure Test / West US | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |

1 - 5 of 5 zones

- 6 Clique em **Criar**.

Etapa 3: crie e implante uma máquina virtual

- 1 Selecione **Recursos > Recursos > Máquinas Virtuais** e clique em **Nova VM**.
- 2 Defina as configurações necessárias na página Geral do assistente e clique em **Seguinte**.

Este tutorial usa a Google Cloud Platform como a conta de nuvem na qual você deseja implantar a máquina virtual.

General Location and basic information.

Select the project, cloud zone, and other basic information for your virtual machine.

Name * Google Cloud Create VM
Enter a name for your machine. A suffix or naming policy may also be applied during provisioning

Project * Create VM Project
Select a project with access to your desired cloud zone

Cloud zone * yingzhi-GCP / us-east1
Select the cloud zone where you want to provision this machine

Tags Enter a new tag
Tags are added to the machine when provisioned

NEXT CANCEL

Lembre-se de que esses valores são apenas amostras. Seus valores devem ser específicos para o seu ambiente.

Tabela 2-1. Valores de amostra para a primeira página do assistente

| Configuração | Valor de amostra |
|---------------|--------------------------|
| Nome | Criar VM do Google Cloud |
| Projeto | Criar Projeto de VM |
| Zona de nuvem | yingzhi-GCP/us-east1 |

- 3 Selecione a imagem e o tipo usados para criar a máquina virtual.

Os valores disponíveis são coletados da zona de nuvem de destino. "A imagem é o sistema operacional, e o tipo é as opções de tamanho definidas." Alguns tipos de provedor de destino exigem que você especifique a CPU e a memória. Esse destino exige que você selecione uma das opções definidas.

4 Clique em **Seguinte**.

Para implantar apenas a máquina, clique em **Criar**. Para este tutorial, clique em **Seguinte** para adicionar o armazenamento e a rede opcionais a essa máquina virtual.

5 Para adicionar um novo disco, clique em **Adicionar disco rígido** e digite **Nome** e **Tamanho**.

6 Clique em **Seguinte**.

7 Para adicionar um adaptador de rede, clique em **Adicionar adaptador de rede**.

8 Selecione nos resultados da pesquisa.

9 Clique em **Criar**.

Seu modo de exibição alterna para a página Implantações para que você possa monitorar o progresso da implantação.

Etapa 4: gerenciar a nova máquina virtual como uma implantação

Quando o processo de implantação for concluído com êxito, você poderá começar a gerenciar a implantação.

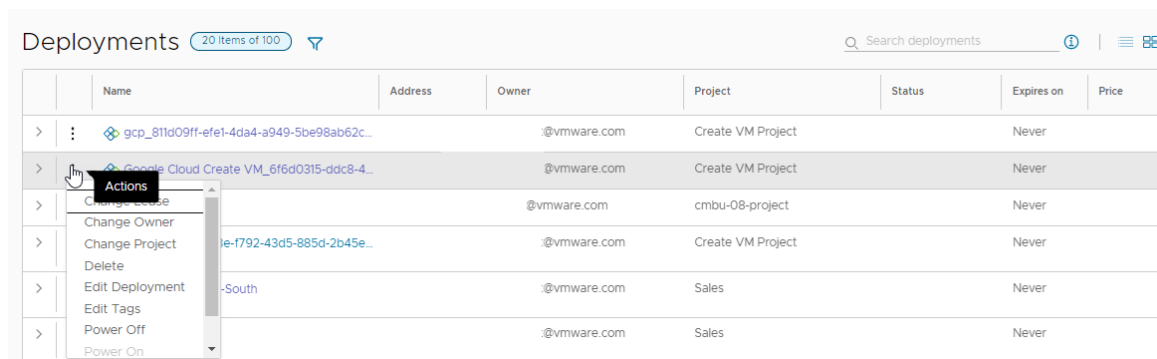
Para obter mais informações sobre como gerenciar suas implantações, consulte [Como gerenciar implantações do Cloud Assembly](#).

Para ver uma lista de todas as ações de dia 2 possíveis em todos os tipos de recursos, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

1 Selecione **Recursos > Implantações** e localize sua máquina virtual.

Neste tutorial, o nome da implantação é Criar VM do Google Cloud.

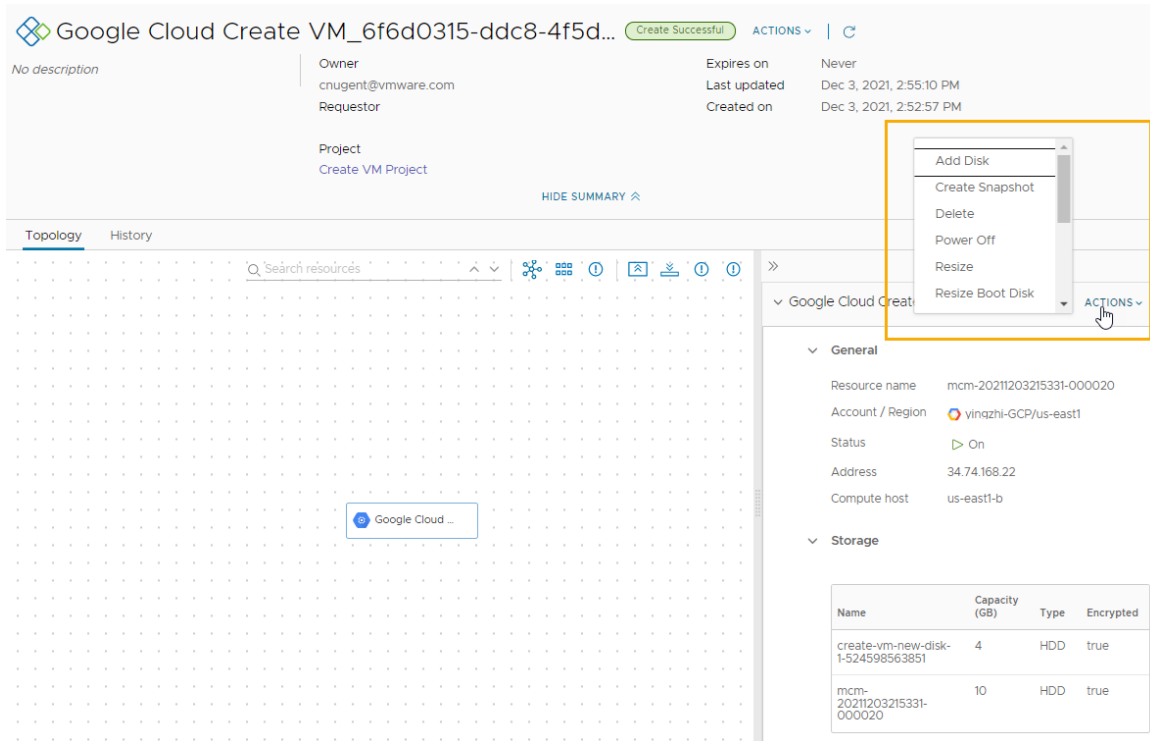
2 "Executar uma ação permitida no nível de implantação na implantação a partir desse modo de exibição, clique nas reticências verticais e selecione a ação."



3 Para saber mais sobre a implantação, incluindo a topologia, clique no nome da implantação.

Observe que a topologia dessa implantação é simples. Implantações mais complexas também fornecem a topologia completa que pode incluir máquinas, balanceadores de carga, conexões de rede e outros componentes.

Você também pode visualizar o histórico da implantação, que é um log de todas as ações nos componentes da implantação, e executar as ações permitidas no nível da máquina.



Etapa 5: gerenciar a nova máquina virtual como um recurso

"Ao gerenciar a máquina virtual como uma implantação, você também pode gerenciá-la junto com os outros recursos." Os recursos podem incluir máquinas virtuais implantadas, descobertas e integradas, volumes de armazenamento e recursos de rede e segurança.

Os recursos descobertos são aqueles coletados da instância de nuvem. Você pode gerenciar os recursos descobertos com um conjunto limitado de ações de dia 2, como ligar e desligar. Para obter mais informações sobre como trabalhar com recursos descobertos, consulte [Como trabalhar com o recursos descobertos no Cloud Assembly](#).

Os recursos integrados são recursos descobertos que você colocou em um gerenciamento completo. Eles podem ser gerenciados com as opções de ação de dia 2 mais avançadas. Para obter mais informações sobre como integrar recursos descobertos, consulte [O que são planos de integração no Cloud Assembly](#).

À medida que você trabalha com essa máquina implantada, ela fica elegível para mais ações de dia 2. A disponibilidade das ações depende do estado da máquina e das ações de dia 2 que você tem permissão para executar.

- 1 Selecione **Recursos > Recursos > Máquinas Virtuais**.
- 2 Localize a máquina.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

| Name | Deployment | VM State | Account / Region | Address | Project | Origin | Tags |
|--------------------------|------------------------------|----------|--|-----------------|-------------------|------------|------|
| vm-administrator-VLDX... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-N6CE... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | 192.167.211.142 | | Discovered | - |
| mcm-20211203215331-0... | Google Cloud Create VM_6f... | ▶ On | yingzhi-GCP / us-east1 | 34.74.168.22 | Create VM Proj... | Deployed | - |

- 3 Para executar uma ação no nível da máquina permitida na máquina a partir desse modo de exibição, clique nas reticências verticais e selecione a ação.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

| Name | Deployment | VM State | Account / Region | Address | Project | Origin | Tags |
|--------------------------|------------------------------|----------|--|-----------------|-------------------|------------|------|
| vm-administrator-VLDX... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-N6CE... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | 192.167.211.142 | | Discovered | - |
| mcm-20211203215331-0... | Google Cloud Create VM_6f... | ▶ On | yingzhi-GCP / us-east1 | 34.74.168.22 | Create VM Proj... | Deployed | - |
| vm-administrator-Q628... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BBJM... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-7RQZ... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BONL... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-2M3... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BSKX... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-X4FT... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-GLA... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-757X... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| e2e-a8n-mcm545178-18... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| mcm-20211203165342-... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| TimWin7-LinkedClone-... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |

- 4 Para revisar os detalhes dos recursos da máquina, clique no nome da máquina.

Os detalhes úteis neste exemplo incluem o armazenamento, a rede e as propriedades personalizadas.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

| Name | Deployment | VM State | Account / Region | Address | Project | Origin | Tags |
|--------------------------|------------------------------|----------|--|-----------------|-------------------|------------|------|
| vm-administrator-VLDX... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-N6CE... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | 192.167.211.142 | | Discovered | - |
| mcm-20211203215331-0... | Google Cloud Create VM_6f... | ▶ On | yingzhi-GCP / us-east1 | 34.74.168.22 | Create VM Proj... | Deployed | - |
| vm-administrator-Q628... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BBJM... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-7RQZ... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BONL... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-2M3... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-BSKX... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-X4FT... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-GLA... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-757X... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| e2e-a8n-mcm545178-18... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| mcm-20211203165342-... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| Load-Balancer-NSX-Uni... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| TimWin7-LinkedClone-... | | ▶ On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |

Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly

Se você é iniciante com o vRealize Automation ou apenas precisa de um curso de recapitulação, este tutorial o orientará pelo processo de configuração do Cloud Assembly. Você adicionará endpoints de conta do vSphere de nuvem, definirá a infraestrutura, adicionará usuários a projetos e, em seguida, projetará e implantará uma carga de trabalho usando VMware Cloud Templates com base em tipos de recursos do vSphere, aprendendo o processo ao longo do caminho.

Embora este tutorial seja apenas o começo, você está no caminho certo para fornecer automação de autoatendimento e desenvolvimento interativo que funcionam em várias nuvens públicas e privadas. Este tutorial se concentra no VMware vCenter Server e no NSX-T. Depois de concluir esse fluxo de trabalho, você poderá aplicar o que aprendeu para adicionar mais tipos de contas de nuvem e distribuir modelos de nuvem mais sofisticados.

À medida que você avança pelas etapas, forneceremos exemplos de dados. Substitua esses exemplos por valores que funcionam melhor no seu ambiente.

Execute todas as etapas deste tutorial no Cloud Assembly.

Esse processo de configuração é a base da sua experiência de desenvolvimento no Cloud Assembly. Ao criar sua infraestrutura e amadurecer suas habilidades de desenvolvimento de modelos de nuvem, você repetirá e expandirá esse fluxo de trabalho.

O que fazer primeiro

- Verifique se você tem a função Administrador do Cloud Assembly. Consulte [Funções de usuário de serviço e organização no vRealize Automation](#).
- Se você não tiver usado os assistentes de Início Rápido do VMware vCenter Server ou do VMware Cloud Foundation no console do vRealize Automation, poderá fazer isso agora.

Esses fluxos de trabalho orientados por assistente incluem a maioria das configurações neste tutorial, mas não todas.

Este tutorial é uma experiência prática que amplia seu conhecimento sobre como planejar uma infraestrutura operacional e implantar uma carga de trabalho.

Consulte [Como configurar o Cloud Assembly](#) no *Guia de Introdução*.

- Se você ainda não tiver usado a configuração guiada que está disponível no Cloud Assembly, poderá fazer isso agora. A configuração guiada orienta você pela maioria dos procedimentos realizados neste tutorial, mas não todos. Para abrir a configuração guiada, clique em **Configuração Guiada** no lado direito da barra de guias.
- Certifique-se de ter credenciais do vCenter Server e do NSX. Para obter mais informações sobre as permissões que as credenciais devem ter, consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#). Se você planeja adicionar mais usuários a projetos, verifique se eles são membros do serviço Cloud Assembly.

Etapa 1: Adicionar as contas de nuvem do vCenter Server e do NSX

As contas de nuvem fornecem as credenciais que o vRealize Automation utiliza para se conectar ao vCenter Server e ao servidor NSX associado.

1 Adicione a conta de nuvem do vCenter Server.

A conta de nuvem do vCenter Server fornece as credenciais do vCenter que o Cloud Assembly utiliza para descobrir recursos e implantar modelos de nuvem.

Para obter mais informações sobre contas de nuvem do vCenter Server, consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).

- a Selecione **Infraestrutura > Conexões > Contas da Nuvem**.
- b Clique em **Adicionar Conta de Nuvem** e selecione **vCenter**.
- c Insira os valores.

New Cloud Account

Name * vCenter Server Account

Description

vCenter Server Credentials

vCenter IP address / FQDN * sc2vc05.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

VALIDATE ✓ Credentials validated successfully. ✕

Configuration

Allow provisioning to these datacenters * ☒ wld01-DC

☒ Create a cloud zone for the selected datacenters

NSX cloud account

Capabilities

Capability tags ⓘ

ADD **CANCEL**

Lembre-se de que esses valores são apenas exemplos. Seus valores serão específicos para o seu ambiente.

| Configuração | Valor de amostra |
|-----------------------------|------------------------------------|
| Nome | Conta do vCenter Server |
| Endereço IP/FQDN do vCenter | your-dev-vcenter.company.com |
| Nome de Usuário e Senha | vCenterCredentials@yourCompany.com |

- d Para verificar as credenciais, clique em **Validar**.
 - e Para **Permitir o provisionamento para esses datacenters**, selecione um ou mais centros de dados.
 - f Ignore a conta de nuvem do NSX. Vamos configurar isso mais tarde, vinculando a conta do vCenter Server à conta de nuvem do NSX.
 - g Clique em **Adicionar**.
- 2 Adicione uma conta de nuvem do NSX associada.

A conta de nuvem do NSX-T fornece as credenciais do NSX-T que o Cloud Assembly utiliza para descobrir recursos de rede e implantar redes com modelos de nuvem.

Para obter mais informações sobre contas de nuvem do NSX-T, consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).

- a Selecione **Infraestrutura > Conexões > Contas da Nuvem**.
- b Clique em **Adicionar Conta de Nuvem** e selecione NSX-T ou NSX-V. Este tutorial usa **NSX-T**.
- c Insira os valores.

New Cloud Account

Name * NSX-T Account

Description

NSX-T Credentials

NSX-T IP address / FQDN * sc2vc05-vip-nsx-mgmt.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

NSX mode Policy ⓘ

VALIDATE ✔ Credentials validated successfully. ✕

Associations

vCenter cloud accounts + ADD ✕ REMOVE

| <input type="checkbox"/> | Name | Status | Identifier | Type |
|--------------------------|------------------------|--------|--------------------|---------|
| <input type="checkbox"/> | vCenter Server Account | ✔ OK | sc2vc05.cmbu.local | vCenter |

1 - 1 of 1 cloud accounts

Capabilities

Capability tags Enter capability tags ⓘ

ADD CANCEL

Esses valores são apenas exemplos. Seus valores serão específicos para o seu ambiente.

| Configuração | Valor de amostra |
|-----------------------------|--|
| Nome | Conta do NSX-T |
| Endereço IP/FQDN do vCenter | your-dev-NSX-vcenter.company.com |
| Nome de Usuário e Senha | NSXCredentials@yourCompany.com |
| Modo NSX | <p>Não sabe o que selecionar?</p> <p>Esta é uma grande oportunidade de usar a ajuda no produto. Clique no ícone de informações à direita do campo. Observe que a ajuda em nível de campo inclui informações que podem ajudar você a configurar a opção.</p> <p>Neste exemplo, selecione Política.</p> |

- d Para verificar as credenciais, clique em **Validar**.
 - e Para associar a conta do vCenter Cloud que você criou na etapa anterior, clique em **Adicionar** e, em seguida, selecione a **Conta do vCenter**.
- Essa associação de conta de nuvem do vCenter garante a segurança da rede.
- f Na página da conta de nuvem do NSX, clique em **Adicionar**.

Etapa 2: Definir os recursos de processamento da zona de nuvem


As zonas de nuvem são grupos de recursos de processamento em uma conta/região que, em seguida, são disponibilizados para projetos. Os membros do projeto implantam modelos de nuvem usando os recursos nas zonas de nuvem atribuídas. Se quiser ter um controle mais granular sobre onde os modelos de nuvem do projeto são implantados, você pode criar várias zonas de nuvem com diferentes recursos de processamento.

Contas/regiões são como os fornecedores de nuvem vinculam recursos a regiões ou repositórios de dados isolados. A conta indica o tipo de conta de nuvem e a região indica a região ou o repositório de dados. O vCenter Server usa repositórios de dados, e os recursos de provisionamento são os clusters e os pools de recursos selecionados.

Para este tutorial, você deve garantir que as zonas de nuvem incluam os recursos que oferecem suporte às metas da equipe de desenvolvimento do projeto e seus requisitos de orçamento e gerenciamento.

Para obter mais informações sobre zonas de nuvem, consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).

- 1 Selecione **Infraestrutura > Configurar > Zonas de Nuvem**.
- 2 Clique na zona de nuvem que foi adicionada à sua instância do vCenter Server e insira os valores.


vCenter Account Cloud Zone
DELETE

Summary
Compute
Projects

A cloud zone defines a set of compute resources that can be used for provisioning.

Account / region *

vCenter Account / wld01-DC

Name *

vCenter Account Cloud Zone

Description

Placement policy *

DEFAULT

Folder

Select folder

Capabilities

Capability tags are effectively applied to all compute resources in this cloud zone, but only in the context of this cloud zone.

Capability tags

Enter capability tags

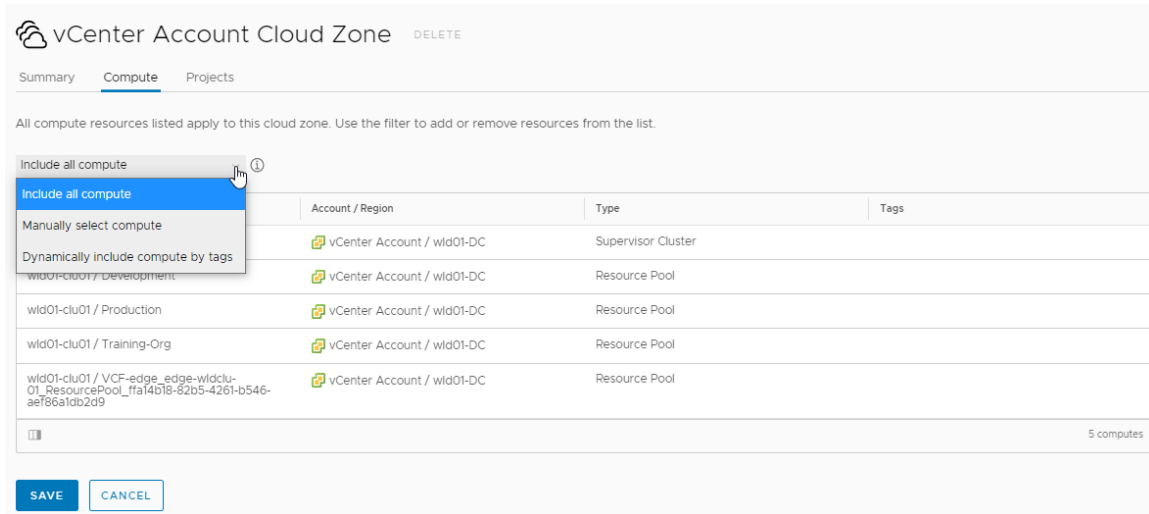
SAVE

CANCEL

| Configuração | Valor de amostra |
|--------------|---|
| Conta/região | Nome do centro de dados/conta do vCenter |
| Nome | Zona de nuvem do vCenter Server Esse valor não pode ser alterado após a criação. Se quiser configurar um centro de dados diferente para um vCenter Server diferente, você deverá criar uma nova zona de nuvem na qual possa selecionar a conta/região. |
| Descrição | Todos os recursos de processamento do vCenter Server para desenvolvimento. |
| Política | Padrão Não se esqueça de consultar a ajuda se tiver dúvidas sobre um valor de campo. |

Lembre-se de que todos os valores são apenas exemplos. Suas especificações de zona serão específicas para o seu ambiente.

- Clique na guia **Processamento** e verifique se os recursos de processamento estão presentes. Se você precisar excluir um, alterne para **Selecionar manualmente o processamento** e adicione apenas aqueles que você deseja incluir na zona de nuvem.



- 4 Clique em **Salvar**.
- 5 Repita o processo para todas as zonas de nuvem adicionais, mas você deve garantir nomes de zona exclusivos.

Etapa 3: Configurar os possíveis recursos que estão disponíveis para a conta/região

Você adicionou a conta/região à zona de nuvem. Agora, defina os possíveis tamanhos de máquina (mapeamentos de tipo), mapeamentos de imagem, perfis de rede e perfis de armazenamento para a conta de nuvem. As definições de mapeamento e perfil são avaliadas para uma correspondência quando você implanta um modelo de nuvem, garantindo que a carga de trabalho inclua o tamanho de máquina (tipo), a imagem, as redes e o armazenamento apropriados.

- 1 Configure os mapeamentos de tipo para a conta/regiões.

Às vezes, tipos são chamados de estimativas de tamanho. Dependendo de como o modelo de nuvem está configurado, o mapeamento de tipos aplicado determina o número de CPUs e memória.

Para obter mais informações sobre mapeamentos de tipos, consulte [Saiba mais sobre mapeamentos de tipo no vRealize Automation](#).

- a Selecione **Infraestrutura > Configurar > Mapeamentos de Tipo**.
- b Clique em **Novo Mapeamento de Tipo** e insira valores que definem máquinas pequenas, médias e grandes.

Lembre-se de que estes são valores de amostra. Você deve selecionar contas/regiões relevantes e definir o dimensionamento.

small DELETE

Allows you to define flavors by name in a cloud-agnostic way. ⓘ

Flavor name * small

Configuration *

| Account / Region | Value |
|----------------------------|-------|
| vCenter Account / wld01-DC | 2 |
| | 1 |

GB ▾ +

| Configuração | Valor de amostra |
|------------------|----------------------------------|
| Nome do tipo | small |
| Conta/região | Centro de dados/conta do vCenter |
| Valor da CPU | 2 |
| Valor de memória | 1 GB |

- c Clique em **Criar**.
- d Para criar tamanhos adicionais, configure mapeamentos de tipo médios e grandes para a conta/região.

| Configuração | Valor de amostra |
|------------------|----------------------------------|
| Nome do tipo | medium |
| Conta/região | Centro de dados/conta do vCenter |
| Valor da CPU | 4 |
| Valor de memória | 2 GB |
| Nome do tipo | large |
| Conta/região | Centro de dados/conta do vCenter |
| Valor da CPU | 8 |
| Valor de memória | 4 GB |

- 2 Configure os mapeamentos de imagem para a conta/região.

As imagens são o sistema operacional das máquinas no modelo de nuvem. Quando você estiver trabalhando com imagens do vCenter Server, selecione modelos do vCenter.

Para obter mais informações sobre mapeamentos de imagens, consulte [Saiba mais sobre mapeamentos de imagem no vRealize Automation](#).

- a Selecione **Infraestrutura > Configurar > Mapeamentos de Imagens**.
- b Clique em **Novo Mapeamento de Imagem** e procure as imagens para a conta/região.
Lembre-se de que estes são valores de amostra. Você deve selecionar imagens relevantes que foram descobertas na sua conta/região.

| Configuração | Valor de amostra |
|----------------|------------------|
| Nome da imagem | centos |
| Conta/região | Conta do vCenter |
| Imagem | centos7 |

- c Clique em **Criar**.
 - d Repita o processo para criar mapeamentos de imagem adicionais. Por exemplo, um mapeamento do Ubuntu para a conta/região.
- 3 Configure perfis de rede.
- Perfis de rede definem as redes e as configurações de rede que estão disponíveis para uma conta/região. Os perfis devem oferecer suporte aos ambientes de implantação de destino.
- Essa tarefa fornece as informações de configuração mínimas para o sucesso. Se quiser mais informações sobre perfis de rede, comece com [Saiba mais sobre perfis de rede no vRealize Automation](#).
- a Selecione **Infraestrutura > Configurar > Perfil de Rede**.
 - b Clique em **Novo Perfil de Rede** e crie um perfil para a conta/região Centro de Dados/Conta do vCenter.

Network Profile
DELETE

[Summary](#)
[Networks](#)
[Network Policies](#)
[Load Balancers](#)
[Security Groups](#)

A network profile defines a group of networks and network settings used when machines are provisioned.

Account / region vCenter Account / wld01-DC

Name * Network Profile

Description Networks for development teams.

Capabilities
Capability tags listed here are matched to constraint tags in the cloud template.

Capability tags ⓘ

| Configuração | Valor de amostra |
|--------------|--|
| Conta/região | Centro de dados/conta do vCenter |
| Nome | Perfil de Rede |
| Descrição | Redes para equipes de desenvolvimento. |

- c Clique na guia **Redes** e clique em **Adicionar Rede**.

Network Profile
DELETE

[Summary](#)
[Networks](#)
[Network Policies](#)
[Load Balancers](#)
[Security Groups](#)

Networks listed here are used when provisioning to existing, on-demand, or public networks. ⓘ

[+ ADD NETWORK](#)
[TAGS](#)
[MANAGE IP RANGES](#)
[REMOVE](#)

| <input type="checkbox"/> | Name | Account / Region | Zone | Network Domain | CIDR | Support Public IP | Default for Zone | Origin | Tags |
|--------------------------|---|------------------|------|--|-----------------|-------------------|------------------|------------|--|
| <input type="checkbox"/> | DevProject-004 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 192.168.1.64/27 | -- | -- | Deployed | |
| <input type="checkbox"/> | External-mcm13/3520-150877845350 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 172.16.1.64/28 | -- | -- | Discovered | |
| <input type="checkbox"/> | seg-domain-c8e2a5390e-2772-43f5-9eaa-eddc05e35996-vmware-system-nsx-0 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 10.244.0.0/28 | -- | -- | Discovered | external_id.8... ncp/project_u... ncp/cluster.d... ncp/version.1... ncp/project.v... |

1 - 3 of 3 networks

- d Selecione as redes do NSX que você deseja disponibilizar para a equipe de desenvolvimento de aplicativos.

Neste exemplo, tínhamos uma rede do NSX-T chamada DevProject-004.

- e Clique na guia **Políticas de Rede** e crie uma política.

| Configuração | Valor de amostra |
|-----------------------------|------------------|
| Política de isolamento | Nenhum |
| Roteador lógico de camada 0 | Tier-0-router |
| Edge cluster | EdgeCluster |

f Clique em **Criar**.

4 Configure perfis de armazenamento.

Perfis de armazenamento definem os discos para uma conta/região. Os perfis devem oferecer suporte aos ambientes de implantação de destino.

Se quiser mais informações sobre perfis de armazenamento, consulte [Saiba mais sobre perfis de armazenamento no vRealize Automation](#).

a Selecione **Infraestrutura > Configurar > Perfil de Armazenamento**.

b Clique em **Novo Perfil de Armazenamento** e crie um perfil para a conta/região vCenter Server/Centro de Dados.

A menos que especificado na tabela, mantenha os valores padrão.

Storage Profile

Account / region

vCenter Account / wld01-DC

Name *

Storage Profile

Description

Disk type *

☒ Standard disk
☐ First class disk (FCD)

Storage policy

Datastore default

Datastore / cluster

Q wld01-sc2vc05-wld01-clu01-vsan01

Provisioning type

Unspecified

Shares

Unspecified

Limit IOPS

Disk mode

Dependent

☐ Supports encryption
☒ Preferred storage for this region

Capability tags

Enter capability tags

SAVE

CANCEL

| Configuração | Valor de amostra |
|---|--|
| Conta/região | Centro de dados/conta do vCenter |
| Nome | Perfil de Armazenamento |
| Repositório de dados/cluster | Selecione um repositório de dados com capacidade suficiente e que possa ser acessado por todos os hosts. |
| Armazenamento preferencial para esta região | Marque a caixa de seleção. |

c Clique em **Criar**.

Etapa 4: Criar um projeto

É aqui que você realmente começa a pensar sobre as metas do projeto.

- Quais usuários precisam de acesso aos recursos de processamento para poderem criar e implantar um modelo de nuvem de aplicativo? Para obter mais informações sobre o que as diferentes funções do projeto podem ver e fazer, consulte [Funções de usuário de serviço e organização no vRealize Automation](#).
- Os membros do projeto criarão aplicativos que vão desde o desenvolvimento até a produção? Quais são os recursos necessários?
- Que zonas de nuvem são necessárias? Que prioridades e limites devem ser colocados em cada zona para o projeto?

Para este tutorial, vamos oferecer suporte à equipe de Desenvolvimento à medida que eles criam e estendem um aplicativo de software interno.

Essa tarefa fornece as informações de configuração mínimas para o sucesso. Se quiser mais informações sobre projetos, comece com [Saiba mais sobre projetos do Cloud Assembly](#).

- 1 Selecione **Infraestrutura > Administração > Projetos**.
- 2 Clique em **Novo Projeto** e insira o nome **Projeto de Desenvolvimento**.
- 3 Clique na guia **Usuários** e depois clique em **Adicionar Usuários**.

Não é necessário adicionar usuários no momento. Mas, se quiser que outros usuários trabalhem com modelos de nuvem, eles deverão ser membros do projeto.

- 4 Insira endereços de e-mail para adicionar usuários como membros do projeto ou administradores, dependendo de quais permissões você deseja que cada pessoa tenha.

- 5 Clique em **Provisionamento** e depois em **Adicionar Zonas > Zona da Nuvem**.
- 6 Adicione as zonas de nuvem nas quais os usuários podem implantar.

Você também pode definir limites de recursos para a zona de nuvem no projeto. No futuro, será possível definir limites diferentes para outros projetos.

| Configuração da zona de nuvem do projeto | Valor de amostra |
|--|-----------------------------------|
| Zona de Nuvem | Zona de nuvem da conta do vCenter |
| Prioridade de provisionamento | 1 |
| Limite de instâncias | 5 |

- 7 Adicione outras zonas de nuvem ao projeto.
- 8 Clique em **Criar**.

- 9 Para verificar se o projeto foi adicionado à zona de nuvem, selecione **Infraestrutura > Configurar > Zonas de Nuvem** e abra o cartão de zona de nuvem da Zona da conta do vCenter para poder examinar a guia **Projetos**. Você verá o Projeto de Desenvolvimento.

Etapa 5: Projetar e implantar um modelo de nuvem básico

Você cria e implanta o modelo de nuvem para garantir que sua infraestrutura esteja configurada corretamente para oferecer suporte ao modelo. Mais tarde, você poderá desenvolver o modelo à medida que cria um aplicativo que atenda às necessidades do seu projeto.

A melhor maneira de criar um modelo de nuvem é fazer isso componente por componente, verificando se ele é implementado entre cada alteração. Este tutorial começa com uma máquina simples e, em seguida, adiciona mais recursos iterativamente.

Os exemplos neste procedimento usam o editor de código YAML. Essa é uma maneira mais fácil de fornecer trechos de código para você. No entanto, se preferir usar uma interface de usuário baseada em caixa de diálogo, clique em **Entradas**.

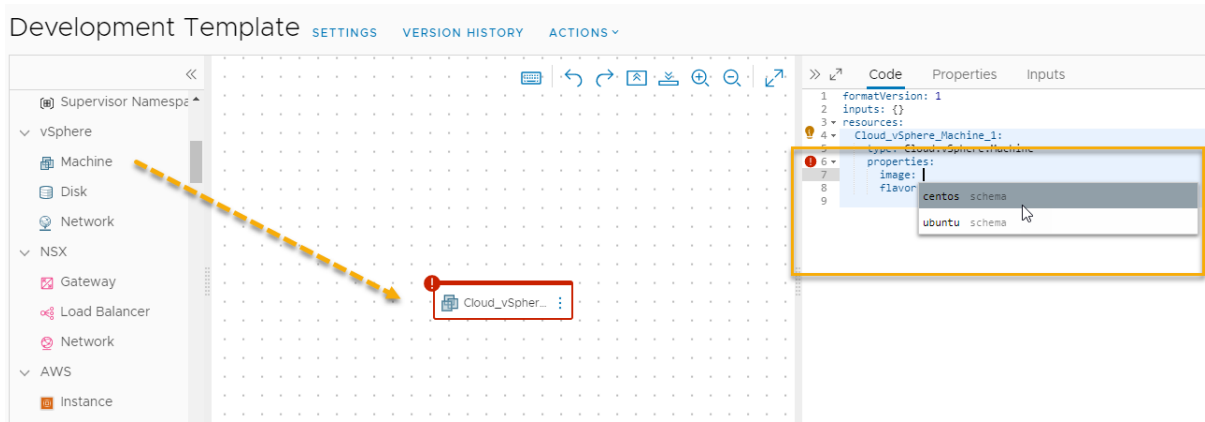
Você pode fazer muito mais com modelos de nuvem além do que é fornecido neste tutorial. Se quiser mais informações, comece com [Capítulo 6 Como projetar suas implantações do Cloud Assembly](#).

Este tutorial usa tipos de recursos do vSphere e NSX. Esses tipos de recursos podem ser implantados apenas em endpoints da conta de nuvem do vCenter Server. Você também pode usar os tipos de recursos independentes de nuvem para criar modelos de nuvem que podem ser implantados em qualquer endpoint. Para obter um exemplo de como configurar a infraestrutura e projetar o modelo para qualquer endpoint, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).



Para obter um vídeo que ilustra as etapas básicas neste procedimento, consulte [Como projetar e implantar um modelo básico de nuvem](#).

- 1 Selecione **Design > Modelos de Nuvem**.
- 2 Selecione **Novo a partir de > Tela em Branco**.
- 3 Insira o **Nome Modelo de Desenvolvimento**, selecione o **Projeto Projeto de Desenvolvimento** e clique em **Criar**.
- 4 Adicione uma máquina do vSphere à tela de criação e depois teste-a e implante-a.



- a No painel de tipo de recurso, arraste uma **Máquina do vSphere** até a tela.

Observe que o painel **Código** mostra o YAML da máquina, com um valor vazio para a imagem e as propriedades predefinidas de CPU e memória. Você vai tornar esse modelo capaz de oferecer suporte ao dimensionamento flexível.

- b Para selecionar um valor de imagem, coloque o ponteiro entre as aspas simples para `image` e selecione **centos** na lista de imagens que você configurou.

Lembre-se de que estes são valores de amostra. Se não tiver configurado uma imagem centos, selecione uma imagem que você tenha configurado.

- c Crie uma linha abaixo da propriedade da imagem e insira ou selecione `flavor` e, em seguida, selecione `small` na lista.

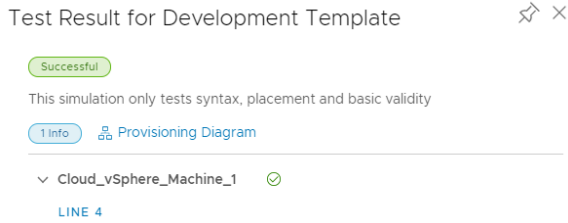
- d Exclua `cpuCount` e `totalMemory`.

Seu YAML deve ser semelhante a este exemplo.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
```

- e Clique em **Testar**.

O teste permite que você valide a sintaxe e o posicionamento do seu modelo de nuvem. Um teste bem-sucedido não significa que você possa implantar o modelo sem erros.



Se o teste falhar, clique em **Diagrama de Provisionamento** e procure os pontos de falha. Para obter mais informações sobre como usar o diagrama para solucionar problemas, consulte [Testar um modelo de nuvem básico](#).

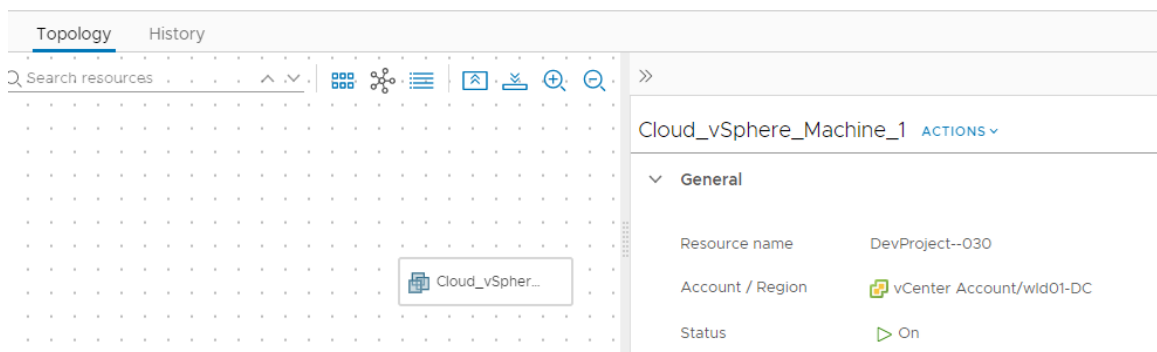
f Clique em **Implantar**.

g Insira **Nome da Implantação** como **DevTemplate - máquina** e clique em **Implantar**.

Você pode rastrear o progresso da implantação na página de detalhes da implantação DevTemplate ou na guia Implantações. Selecione **Recursos > Implantações**.

Se a implantação falhar, será possível solucionar o problema e revisar o modelo. Consulte [O que fazer se uma implantação do Cloud Assembly falhar](#).

Uma implantação bem-sucedida é semelhante a este exemplo na página Implantações.



5 Defina uma versão para o modelo e adicione uma rede.

O controle de versão de um modelo de nuvem é necessário para torná-lo disponível no catálogo do Service Broker, mas é útil ter uma versão íntegra para reverter durante o desenvolvimento.

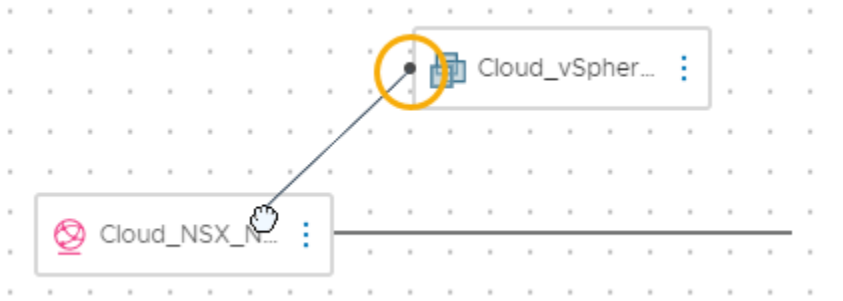
a Abra o modelo na tela de design.

b Clique em **Versão**, insira uma **Descrição** semelhante a **Máquina implantável simples** e clique em **Criar**.

c No painel de tipo de recurso, arraste um tipo de recurso **Rede do NSX** até a tela.

d Conecte a máquina à rede.

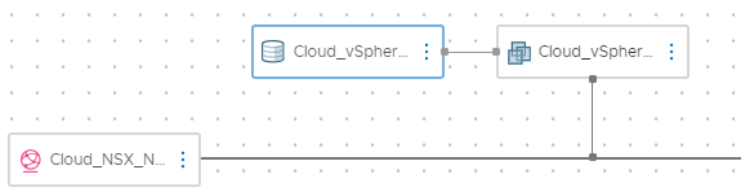
Clique no pequeno círculo no componente de máquina e arraste a conexão até a rede.



Observe que o YAML agora é semelhante a esse exemplo.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks: []
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Clique em **Testar** para validar o modelo.
 - f Clique em **Implantar**.
 - g Insira o nome **DevTemplate - máquina - rede** e clique em **Implantar**.
 - h Acompanhe o progresso e revise a implantação bem-sucedida.
- 6 Defina uma versão para o modelo e adicione um disco de dados.
- a Abra o modelo na tela de design.
 - b Defina uma versão para o modelo.
- Insira **Máquina com rede existente** como a descrição.
- c No painel tipo de recurso, arraste um tipo de recurso **Disco vSphere** até a tela.
 - d Conecte o disco à máquina.



Observe que o YAML agora é semelhante a esse exemplo.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Teste o modelo.
- f Implante o modelo usando o nome **DevTemplate - máquina - rede - armazenamento**.
- g Acompanhe o progresso e revise a implantação bem-sucedida.
- h Defina uma versão para o modelo.

Insira **Máquina com rede e disco de armazenamento existentes** como a descrição.

Essa versão final garante que você possa adicionar um modelo operacional ao Service Catalog.

Resultados do tutorial

Você concluiu o fluxo de trabalho que configurou o Cloud Assembly como um sistema de trabalho. Agora, você está familiarizado com os seguintes conceitos.

- Contas de nuvem são as credenciais que conectam o Cloud Assembly aos seus endpoints de fornecedor de nuvem.
- Zonas de nuvem são os recursos de processamento selecionados em contas/regiões que você então atribui a diferentes projetos com base nas necessidades desses projetos e nas suas metas de gerenciamento de custos.
- Recursos de infraestrutura são definições de recursos associados a contas/regiões que são usadas em modelos de nuvem.

- Projetos são como você concede aos usuários acesso às zonas de nuvem com base nas metas de desenvolvimento de aplicativos do projeto.
- Modelos de nuvem são as definições das suas cargas de trabalho de aplicativo que você desenvolve e implementa iterativamente.

Este tutorial é a base de sua experiência de desenvolvimento no Cloud Assembly. Você pode usar esse processo para criar sua infraestrutura e amadurecer suas habilidades de desenvolvimento de modelos de nuvem.

Tutorial: configurando o Cloud Assembly para provisionar uma carga de trabalho de produção

Como administrador de nuvem, você deseja automatizar o processo de implantação de um projeto para que, quando os designers de modelos de nuvem estiverem criando e implantando modelos, o Cloud Assembly faça o trabalho para você. Por exemplo, as cargas de trabalho são implantadas com um padrão de nomenclatura de máquina personalizado específico, as máquinas são adicionadas a uma unidade organizacional específica do Active Directory e intervalos de DNS e IP específicos são usados.

Ao automatizar o processo para as implantações de projetos, você pode gerenciar mais facilmente vários projetos em vários centros de dados e ambientes de nuvem.

Não é necessário concluir todas as tarefas fornecidas aqui. É possível misturar e combinar qualquer uma dessas tarefas, dependendo das suas metas de gerenciamento.

Antes de começar

Este tutorial exige que você tenha sua infraestrutura configurada e tenha implantado com êxito um modelo de nuvem com uma máquina e uma rede. Verifique se os seguintes itens já estão configurados no seu sistema.

- Você executou com êxito todas as etapas especificadas no tutorial de infraestrutura. Consulte [Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly](#).
- Você tem a função de Administrador do Cloud Assembly. Consulte [Funções de usuário de serviço e organização no vRealize Automation](#).

Personalizar os nomes de máquinas

O objetivo dessa tarefa é garantir que as máquinas implantadas para o Projeto de desenvolvimento sejam nomeadas com base no centro de custos do projeto, no tipo de recurso selecionado no momento da implantação e nos números incrementados para garantir a exclusividade. Por exemplo, DevProject-centos-021.

Você pode adaptar esse exemplo aos seus requisitos de nomenclatura.

Para obter mais informações sobre projetos, consulte [Capítulo 5 Como adicionar e gerenciar projetos do Cloud Assembly](#).



Para obter um vídeo que ilustra esse exemplo de nomenclatura personalizada, consulte [Como criar um modelo de nomenclatura personalizada para implantações](#).

- 1 Selecione **Infraestrutura > Projetos**.
- 2 Selecione um projeto existente ou crie um novo.
Para este tutorial, o nome do projeto é Projeto de desenvolvimento.
- 3 Clique em **Criar**.
- 4 Na página Projetos, clique no nome do projeto no bloco para poder configurar o projeto.
- 5 Clique na guia **Usuários** e adicione os usuários que são membros desse projeto.
- 6 Clique na guia **Provisionamento**.
 - a Na seção Zonas, clique em **Adicionar Zona** e adicione as zonas de nuvem possíveis nas quais as cargas de trabalho serão implantadas para esse projeto.
 - b Na seção Propriedades Personalizadas, adicione uma propriedade personalizada com o nome **costCenter** e o valor **DevProject**.

| Name | Value | Encrypted |
|------------|------------|--------------------------|
| costCenter | DevProject | <input type="checkbox"/> |

Custom Naming

Specify the naming template to be used for machines, networks, security groups and disks provisioned in this project.

Template:

Hint: Avoid conflicting names by generating digits in names. \${#####}

- c Na seção Nomenclatura Personalizada, adicione o seguinte modelo de nomenclatura.

```
${resource.costCenter}-${resource.installedOS}-${###}
```

O `${resource.installedOS}` é baseado no sistema operacional selecionado quando você implanta o modelo de nuvem.

- 7 Clique em **Salvar**.
- 8 Atualize o modelo de nuvem com um valor de entrada para o tipo de sistema operacional.
Valores de entrada são a maneira direta de personalizar o formulário de solicitação de implantação para usuários e simplificar o processo de desenvolvimento. Ao criar valores de entrada, você pode usar um único modelo de nuvem para implantar cargas de trabalho com configurações diferentes. Por exemplo, tamanho ou sistema operacional.

Este exemplo usa o Modelo de Desenvolvimento de um tutorial anterior. Consulte [Etapa 5: Projetar e implantar um modelo de nuvem básico](#).

- a Selecione **Design** e abra o Modelo de Desenvolvimento.
 - b No painel Código, atualize o YAML com as seguintes alterações.
 - Na seção **Inputs**, adicione **installedOS**.

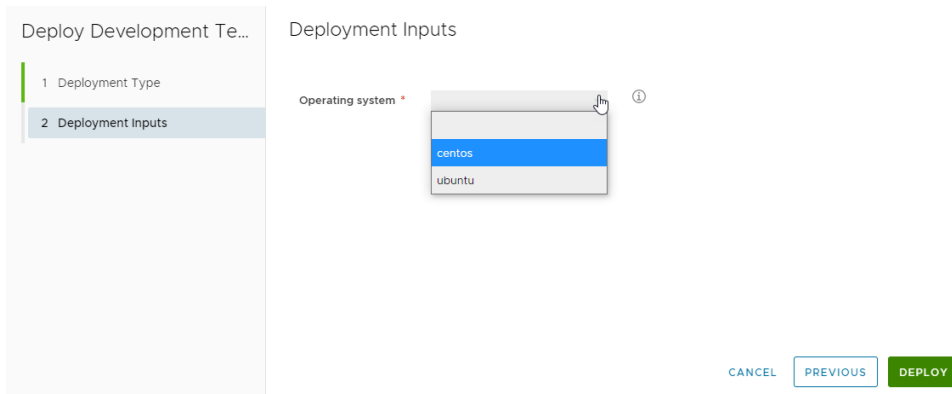
Na próxima etapa, você pode ver que a entrada `installedOS` também é usada para especificar a imagem. Quando você adiciona as cadeias de caracteres na seção `enum`, os valores, neste exemplo, são `centos` e `ubuntu` devem corresponder aos nomes de imagem que você definiu em **Infraestrutura > Configurar > Mapeamentos de Imagem**. Por exemplo, se o seu nome de mapeamento de imagem for CentOS em vez de CentOS, você deverá usar o CentOS na seção de entradas.

```
inputs:
  installedOS:
    type: string
    title: OS Type
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
```

- Na seção `Cloud_vSphere_Machine_1`, atualize o `image` para um parâmetro de entrada `installedOS` (`${input.installedOS}`) e adicione uma propriedade personalizada `installedOS` com o mesmo parâmetro de entrada.

```
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ${input.installedOS}
      installedOS: ${input.installedOS}
      flavor: small
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

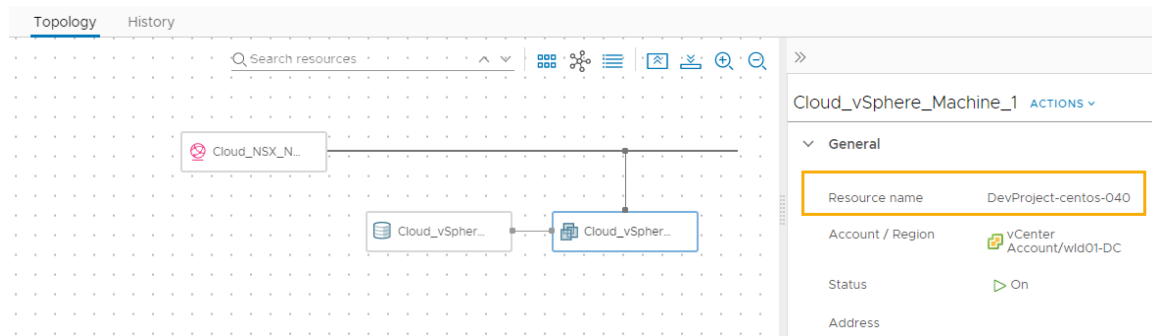
- Clique em **Implantar** e insira o nome **Teste de implantação de nome personalizado**.
- Clique em **Seguinte**.
- Selecione o sistema operacional **centos** no menu suspenso.



f Clique em **Implantar**.

9 Acompanhe o progresso e revise a implantação bem-sucedida.

O nome da máquina neste exemplo é DevProject-centos-026. Apenas como lembrete, este exemplo baseia-se no tutorial mencionado no início desta tarefa.



Criar registros de máquina do Active Directory

Ao provisionar uma carga de trabalho, você pode criar registros de máquina no Active Directory. Ao configurar o Cloud Assembly para realizar essa tarefa automaticamente para as implantações de um projeto, você alivia sua própria carga de trabalho como administrador de nuvem.

1 Adicione uma integração com o Active Directory.

a Selecione **Infraestrutura > Conexões > Integrações**.

Essas etapas abrangem a configuração básica do Active Directory que está relacionada a este tutorial de registros de máquinas do AD. Para obter mais informações sobre a integração com o Active Directory, consulte [Como criar uma integração do Active Directory no Cloud Assembly](#).

b Clique em **Adicionar Integração** e depois em **Active Directory**.

c Insira o nome que você está usando para essa integração.

d Insira o **Host/IP do LDAP** e as credenciais associadas.

e Insira o **DN Base**.

Neste tutorial, o exemplo é **ou=AppDev,dc=cmbu,dc=local**. AppDev é a UO principal da UO de computador que você adicionará ao projeto.

f Clique em **Adicionar**.

2 Adicione o projeto à integração.

3 Na integração com o Active Directory, clique na guia **Projetos** e depois em **Adicionar Projeto**.

Add Projects

Select a project and the OU it will be mapped to by adding its relative DN. The effective DN is created by appending the RDN to the integration base DN (**dc=cmbu,dc=local**).

a Selecione o projeto Desenvolvimento de aplicativo.

b Insira os DN's relativos. Por exemplo, **OU=AppDev-Computers**.

- c Deixe as opções Substituições e Ignorar desligadas.

Esse procedimento é focado na automatização do processo para um projeto. Não se trata de personalizações que você pode fazer em modelos.

- d Clique em **Adicionar**.

- 4 Para salvar as alterações na integração, clique em **Salvar**.

- 5 Implante um modelo de nuvem para o projeto e verifique se a máquina foi adicionada à UO correta do Active Directory.

Definir o intervalo de IP interno e o DNS de rede

Adicione ou atualize um perfil de rede para incluir seus servidores DNS e intervalos de IPs internos.

Você já deve ter criado uma conta de nuvem para o vSphere, o NSX-V ou o NSX-T. Consulte [Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly](#) ou [Como adicionar contas de nuvem ao Cloud Assembly](#).

- 1 Selecione **Infraestrutura > Configurar > Perfis de Rede**.
- 2 Selecione um perfil existente ou crie um.
- 3 Na guia **Resumo**, selecione uma **Conta/região** e insira um nome.
Para este tutorial, o nome do perfil de rede é Perfil de Rede.
- 4 Adicionar redes.
 - a Clique na guia **Redes**.
 - b Clique em **Adicionar Rede**.
 - c Adicione uma ou mais redes do NSX ou do vSphere.
 - d Clique em **Adicionar**.
- 5 Configure os servidores DNS.
 - a Na lista redes na guia **Redes**, clique no nome da rede.

Summary

Networks

Network Policies

Load Balancers

Security


Networks listed here are used when provisioning to existing, on-demand, or p

+ ADD NETWORK

TAGS

MANAGE IP RANGES

REMOVE

| <input type="checkbox"/> | Name ↑ | Account / Region | Zone | Network Domain | CIDR |
|--------------------------|-----------------|---|------|--|-----------------|
| <input type="checkbox"/> | DevProject--004 |  NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 192.168.1.64/27 |

- b Insira os endereços IP do servidor DNS que você deseja que essa rede utilize.

DevProject--004

DNS servers

192.168.1.22
192.168.1.23

DNS search domains

company.local

DNS Servers

Use a comma separated list or new lines.

- c Clique em **Salvar**.

- 6 Especifique o intervalo de IPs para a rede.

- a Na lista de redes, marque a caixa de seleção ao lado do nome da rede.

Network Profile **DELETE**

Summary **Networks** Network Policies Load Balancers Security Groups

Networks listed here are used when provisioning to existing, on-demand, or public networks. ⓘ

+ ADD NETWORK TAGS **MANAGE IP RANGES** REMOVE

| <input type="checkbox"/> | Name | Account / Region | Zone | Network Domain | CIDR | Su Pu |
|-------------------------------------|----------------------------------|------------------|------|--|-------------------|-------|
| <input type="checkbox"/> | External-mcm1343745-148168716643 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 172.16.12.64/28 | |
| <input type="checkbox"/> | NSX-mcm1376447-151082888186 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 192.168.100.32/28 | |
| <input checked="" type="checkbox"/> | NSX-mcm39835-146434698964 | NSX-T Account | | overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local | 192.168.1.0/27 | |

1

- b Clique em **Gerenciar Intervalos de IP**.

- c Na caixa de diálogo Gerenciar Intervalos de IP, clique em **Novo Intervalo de IP**.

New IP Range

| | |
|--------------------|--|
| Network * | NSX-mcm1376447-151082888186 |
| Source | <input checked="" type="radio"/> Internal <input type="radio"/> External |
| Name * | DevProject Range |
| Description | <div></div> |
| CIDR | 192.168.100.32/28 |
| Start IP address * | 192.168.100.34 |
| End IP address * | 192.168.100.46 |

d Digite um nome.

Por exemplo, **Intervalo de DevProject**.

e Para definir o intervalo, insira o **Endereço IP Inicial** e o **Endereço IP Final**.

f Clique em **Adicionar**.

g Adicione intervalos adicionais ou clique em **Fechar**.

- Adicione a zona de nuvem que contém a conta/região de rede associada que você configurou para o seu Projeto de desenvolvimento.
- Implante um modelo de nuvem para o projeto e verifique se a máquina está provisionada dentro de intervalo de IPs especificado.

Tutorial: Usando tags no Cloud Assembly para gerenciar recursos do vSphere

Tags são metadados poderosos que você pode associar a recursos e incluir em modelos. Você pode usar tags em uma variedade de cenários de gerenciamento, incluindo posicionamento de carga de trabalho e rotulagem de recursos.

Introdução rápida a tags

Esta seção é uma introdução simples a tags conforme elas se aplicam às etapas fornecidas. Para obter informações mais detalhadas sobre tags, consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).

- Tags de capacidade e restrição

Você pode usar tags para controlar implantações com base em capacidades de recursos. Por exemplo, como um administrador de nuvem, você deseja que os modelos de nuvem desenvolvidos iterativamente sejam implantados em um pool de recursos específico de desenvolvimento e os modelos dignos de produção para implantar em um pool de recursos diferente.

- Tags de capacidade são adicionadas a recursos, definindo suas capacidades.
- Tags de restrição são usadas em modelos de nuvem, definindo quais recursos você deseja que os recursos implantados consumam.
- Tags de rótulo

Para gerenciar recursos, você pode adicionar tags como rótulos ou descrições de objetos. As possibilidades de gerenciamento incluem melhores resultados de pesquisa de recursos, diferenciação entre objetos semelhantes, anotação de objetos com informações personalizadas, fornecimento de informações para sistemas de terceiros, criação de critérios de associação de agrupamento de segurança, garantia de consistência entre domínios SDDC vinculados.

Antes de começar

- Revise os recursos e o modelo de nuvem definido em [Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly](#). Os valores de amostra usados nesse tutorial são usados aqui.

Usando tags para gerenciar a posicionamento de carga de trabalho

Este exemplo simples usa tags de ambiente de desenvolvimento e produção para demonstrar como usar tags de capacidade e restrição. Primeiro, você adiciona tags de capacidade em recursos de processamento do pool de recursos do vCenter Server e, em seguida, inclui as tags no modelo de nuvem. O exemplo de modelo de nuvem demonstra como usar entradas para permitir que o usuário da implantação selecione se deseja implantá-la em um pool de recursos de desenvolvimento ou de produção.

Para obter um exemplo de como usar as mesmas tags para definir o posicionamento em um ambiente de várias nuvens, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).

- 1 Adicione tags de capacidade a pools de recursos.
 - a Selecione **Infraestrutura > Recursos > Processamento**.

- b Abra a zona da nuvem e clique em **Processamento**.

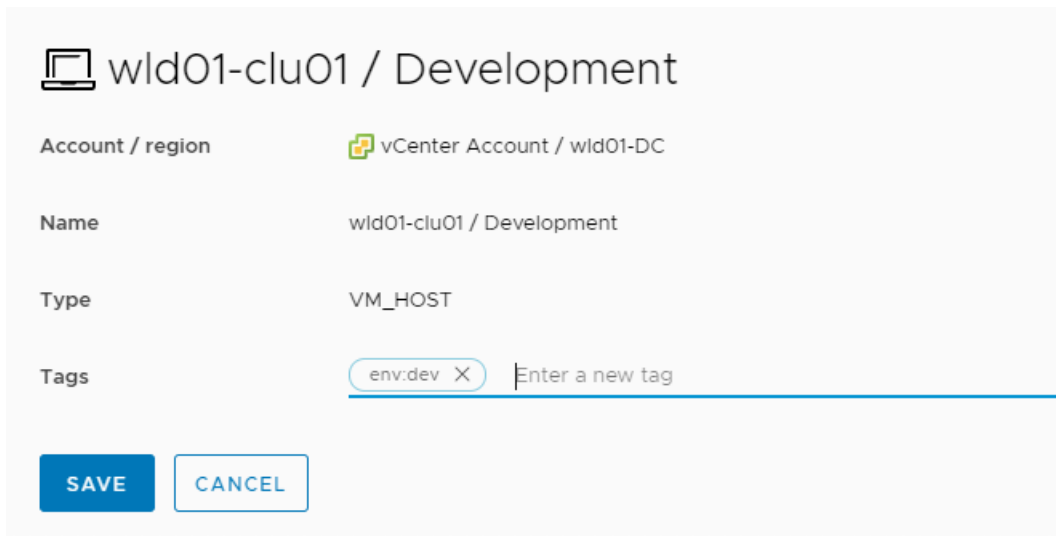


- c Localize e clique no pool de recursos no qual deseja implantar as cargas de trabalho de desenvolvimento.

Este tutorial usa os seguintes valores de amostra. Lembre-se de que esses valores são apenas exemplos. Seus valores serão específicos para o seu ambiente.

| Amostra de pool de recursos | Tag de amostra |
|-------------------------------|----------------|
| wld01-clu01 / Desenvolvimento | env:dev |
| wld01-clu01 / Produção | env:prod |

- d Adicione a tag **env:dev** e clique em **Salvar**.



- e Repita o processo para o pool de recursos em que deseja implantar cargas de trabalho de produção e adicione a tag **env:prod**.
- 2 Verifique se as tags de capacidade foram adicionadas aos pools de recursos na sua zona de nuvem.
- a Selecione **Infraestrutura > Configurar > Zonas de Nuvem**.
- b Abra a zona da nuvem associada ao projeto e clique em **Processamento**.

Neste exemplo, a zona da nuvem é Zona de nuvem da conta do vCenter e as tags foram adicionadas aos dois pools de recursos, wid01-clu01 / Desenvolvimento e wid01-clu01 / Produção.

| Name | Account / Region | Type | Tags |
|--|----------------------------|--------------------|----------|
| 10.176.152.27 | vCenter Account / wid01-DC | Host | |
| wid01-clu01 | vCenter Account / wid01-DC | Supervisor Cluster | |
| wid01-clu01 / Development | vCenter Account / wid01-DC | Resource Pool | env:dev |
| wid01-clu01 / Production | vCenter Account / wid01-DC | Resource Pool | env:prod |
| wid01-clu01 / Training-Org | vCenter Account / wid01-DC | Resource Pool | |
| wid01-clu01 / VCF-edge_edge-widclu-01_ResourcePool_ffa14b18-82b5-4261-b546-ae86a1db2d9 | vCenter Account / wid01-DC | Resource Pool | |

3 Adicione tags de restrição ao modelo de nuvem.

Tags de restrição são usadas para limitar onde o modelo é implantado.

- Selecione **Design > Modelos de Nuvem** e, em seguida, abra seu modelo.

Neste tutorial, o nome do modelo é Modelo de Desenvolvimento.

- Revise o YAML para o modelo no painel Código.

Esse YAML é o ponto de partida para este tutorial.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: medium
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- c Adicione a tag de restrição ao recurso `Cloud_vSphere_Machine_1` usando `${input.placement}` como uma variável.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: medium
    constraints:
      - tag: '${input.placement}'
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
```

- d Defina a variável de posicionamento na seção Entradas.

```
inputs:
  placement:
    type: string
    enum:
      - env:dev
      - env:prod
    default: env:dev
    title: Select Placement for Deployment
    description: Target Environment
```

- e Verifique se o YAML final é semelhante ao exemplo a seguir.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
    constraints:
      - tag: '${input.placement}'
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
```

```
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 5
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

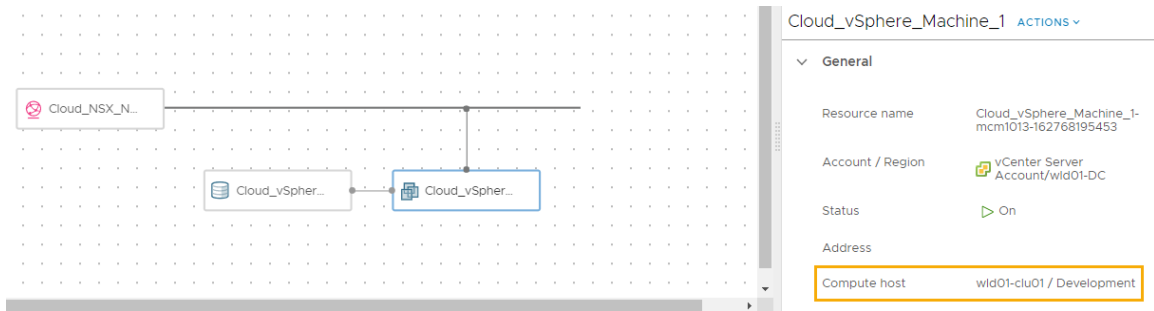
- f Para testar a variável de tag em relação aos recursos disponíveis, clique em **Testar** e selecione **env:dev**.



Repita o teste usando **env:prod**. Quando ambos os testes forem bem-sucedidos, confirme se o modelo funciona implantando-o.

- 4 Implante o modelo para testar o posicionamento da carga de trabalho.
 - a No designer de modelo de nuvem, clique em **Implantar**.
 - b Insira **Desenvolvimento de tags de implantação** como o **Nome de Implantação** e clique em **Próximo**.
 - c Selecione **env:dev** no menu suspenso **Selecionar Posicionamento para Implantação** e clique em **Implantar**.
- 5 Verifique se o modelo implantou os recursos no pool de recursos selecionado.
 - a Selecione **Recursos > Implantações** e localize a implantação Desenvolvimento de tags de implantação.
 - b Abra os detalhes de implantação e clique em **Topologia**.
 - c Clique na máquina vSphere e expanda as informações da máquina no painel direito.
 - d Na seção **Geral**, localize **Host de processamento** e verifique se o valor corresponde ao pool de recursos que corresponde à sua tag env:dev.

Neste exemplo, o valor é wid01-clu01 / Development, ilustrando que a carga de trabalho foi implantada para corrigir o pool de recursos com base na tag de restrição selecionada.



- e Repita o processo de implantação e dessa vez selecione **env:prod**.

Adicionando tags como rótulos que você pode usar no vCenter Server e no NSX-T

Você pode adicionar tags a implantações que podem ser usadas para gerenciar recursos.

Neste exemplo, você adiciona tags para identificar a máquina MySQL e a rede. Você também adiciona uma tag para identificar a rede da Web. Devido ao modo como as tags funcionam nas redes existentes em comparação com as redes sob demanda, você tem duas opções.

- Se você usar o perfil de rede existente usado na seção anterior, a tag NGINX:web não será adicionada aos objetos existentes no NSX-T. Portanto, você pode ignorar as etapas de verificação relacionadas a essa tag no NSX-T.
- Se você criar um perfil de rede sob demanda, poderá atualizar a rede no YAML para usar a rede roteada/sob demanda. A rede sob demanda é usada neste exemplo para que possamos demonstrar a tag NGINX:web no novo objeto no NSX-T.

O seguinte YAML é do exemplo anterior, com a diferença de que agora ele usa um networkType roteado sob demanda. Ele inclui as tags de restrição.

Este tutorial usa os seguintes valores de amostra. Lembre-se de que esses valores são apenas exemplos. Seus valores serão específicos para o seu ambiente.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
```



```

networks:
  - network: '${resource.Cloud_NSX_Network_1.id}'
attachedDisks:
  - source: '${resource.Cloud_vSphere_Disk_1.id}'
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 5
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: routed
  constraints:
    - tag: 'net:od'

```

- 1 Selecione **Design > Modelos de Nuvem** e, em seguida, abra seu modelo.
- 2 Nas propriedades Cloud_vSphere_Machine, adicione a seguinte tag.

```

tags:
  - key: db
    value: mysql

```

- 3 Adicione tags de NIC da VM.

```

tags:
  - key: db
    value: mysql

```

- 4 Adicione tags lógicas de switch/segmento NSX.

```

tags:
  - key: NGINX
    value: web

```

- 5 Verifique se o YAML é semelhante ao exemplo a seguir.

```

formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:

```

```

Cloud_vSphere_Machine_1:
  type: Cloud.vSphere.Machine
  properties:
    image: centos
    flavor: small
    constraints:
      - tag: '${input.placement}'
    tags:
      - key: db
        value: mysql
  networks:
    - network: '${resource.Cloud_NSX_Network_1.id}'
      tags:
        - key: db
          value: mysql
  attachedDisks:
    - source: '${resource.Cloud_vSphere_Disk_1.id}'
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 5
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: routed
    constraints:
      - tag: 'net:od'
    tags:
      - key: NGINX
        value: web

```

6 Implante o modelo.

Este exemplo usa o nome **Tags w do modelo de desenvolvimento**.

7 Para verificar as tags na implantação, abra a implantação e clique na guia **Topologia**.

- a Clique na máquina na topologia.
- b Expanda a seção **Geral** da máquina e localize o rótulo Tags.

O valor da tag é db:mysql.

- c Expanda a seção **Rede** e localize a coluna Tags da rede.

O valor da tag é db:mysql.

Development template w tags Create Successful ACTIONS |

No description

Owner: fritz
Requestor: fritz
Project: Development Project
Cloud Template: Development Template

Expires on: Never
Last updated: Mar 8, 2021, 4:31:01 PM
Created on: Mar 8, 2021, 4:09:14 PM

HIDE SUMMARY

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_vSphere...

Cloud_vSphere_Machine_1 ACTIONS

General

Resource name: Cloud_vSphere_Machine_1-mcm1019-163638575175
Account / Region: vCenter Server Account/wld01-DC
Status: On
Address:
Compute host: wld01-clu01 / Development
Tags: db.mysql

Storage

Network

| Index | Name | Address | Assignment Type | Security Groups | Tags |
|-------|----------------|---------|-----------------|-----------------|----------|
| 0 | DevProject-004 | | dynamic | | db.mysql |

Custom properties

- d Clique na rede na topologia e expanda a seção **Geral** para localizar o rótulo da tag.
O valor da tag é NGINX:web.

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_vSphere...

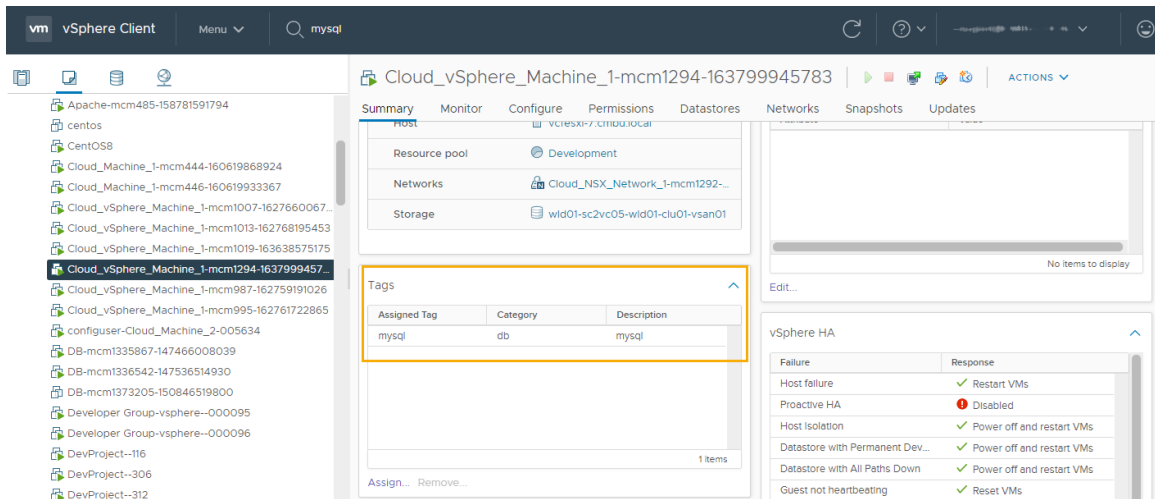
Cloud_NSX_Network_1 ACTIONS

General

Resource name: Cloud_NSX_Network_1-mcm1292-163799928607
Account: NSX-T Account
Network type: routed
CIDR: 192.168.150.0/28
Tags: NGINX:web

Custom properties

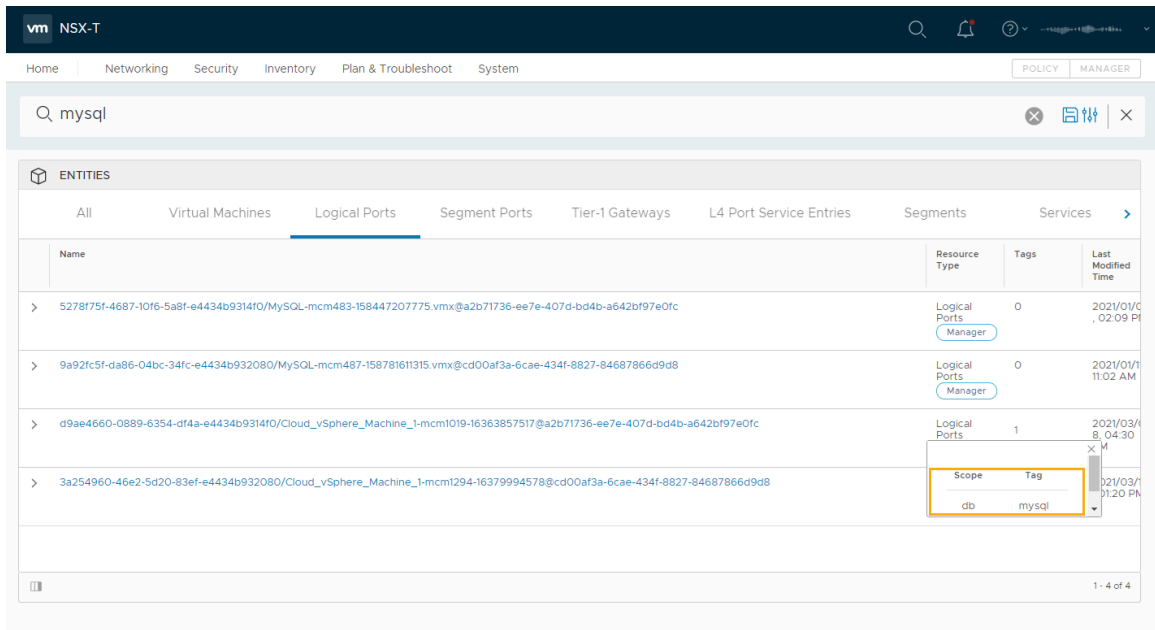
- 8 Para verificar as tags no vCenter Server, faça login na instância do vCenter Server onde essa carga de trabalho foi implantada.
- a Localize a máquina virtual e localize o painel Tags.



9 Para verificar as tags no NSX-T, faça login na instância do NSX-T onde essa rede está configurada.

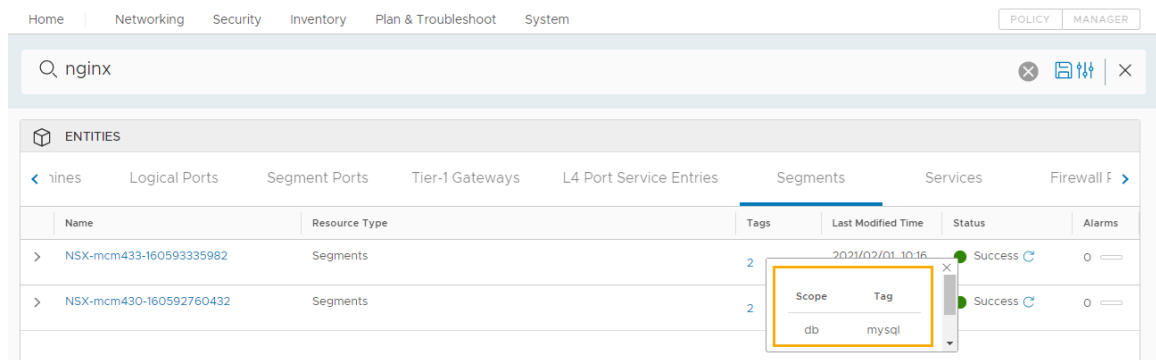
- Clique em **Política** no canto superior direito.
- Para localizar a tag `db:mysql` associada à NIC, procure **mysql**.
- Clique em **Portas Lógicas** e localize a máquina vSphere implantada.
- Clique no número na coluna Tags.

O Escopo e a Tag são `db` e `mysql`, respectivamente.



- Para localizar a tag `NGINX:web` associada ao segmento, procure a rede. Neste exemplo, o nome da rede é **Cloud_NSX_Network_1-mcm1292-163799928607**.
- Localize a linha Segmentos e clique no número na coluna de tags.

O Escopo e a Tag são NGINX e web, respectivamente.



Tutorial: Adicionando um modelo de nuvem do Cloud Assembly ao catálogo do Service Broker com um formulário de solicitação personalizado

Durante o desenvolvimento iterativo dos seus modelos de nuvem ou quando tiver um modelo final, você pode disponibilizar os modelos para os consumidores no catálogo de autoatendimento do Service Broker. Para melhorar ainda mais a experiência do usuário, é possível criar um formulário de solicitação personalizado. Esse formulário personalizado é mais eficiente do que as opções de entrada de modelo simples.

O que fazer primeiro

- Verifique se você tem a infraestrutura compatível com o seu modelo. Se não tiver, comece com [Tutorial: configurando e testando a infraestrutura e as implantações do vSphere no Cloud Assembly](#) e continue com os outros tutoriais.
- Verifique se você marcou alguns pools de recursos como `env:dev` e `env:prod`. Para obter mais informações, consulte [Tutorial: Usando tags no Cloud Assembly para gerenciar recursos do vSphere](#).
- Certifique-se de ter um modelo de nuvem implantável, semelhante ao modelo de nuvem abaixo. Este tutorial começa com o modelo a seguir.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating System
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    enum:
      - 'env:dev'
```

```

    - 'env:prod'
  default: 'env:dev'
  title: Select Placement for Deployment
  description: Target Environment
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: '${input.installedOS}'
      installedOS: '${input.installedOS}'
      flavor: small
    constraints:
      - tag: '${input.placement}'
    tags:
      - key: db
        value: mysql
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
        tags:
          - key: db
            value: mysql
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
    tags:
      - key: NGINX
        value: web

```

Etapa 1: Adicionar entradas ao modelo de nuvem

Além da entrada do tipo de SO existente, este procedimento atualiza a entrada de posicionamento e adiciona uma entrada de tamanho. Ao personalizar o formulário de solicitação no Service Broker, estes são os três campos no formulário de solicitação que são personalizados.

- 1 Em Cloud Assembly, selecione **Design > Modelo de Nuvem** e crie ou abra o modelo fornecido acima.

O modelo de amostra é usado para explicar as diferentes opções e inclui valores de amostra. Adapte-o ao seu ambiente.

- 2 Adicione a variável de tamanho e defina os tamanhos na seção Entradas.

- a Na seção `Cloud_vSphere_Machine_1`, adicione uma variável à propriedade `flavor`.

```
flavor: '${input.size}'
```

- b Na seção Entradas, adicione um tamanho de nome para entrada pelo usuário, para que o usuário possa selecionar o tamanho da implantação. Isso às vezes é conhecido como o tamanho de camiseta que você definiu para as zonas de nuvem.

```
size:
  type: string
  title: Deployment size
  description: Select the the deployment t-shirt size.
  enum:
    - small
    - medium
    - large
```

- 3 Atualize as entradas de posicionamento com um termo descritivo no lugar das strings de tag.

Essas marcas de restrição serão correspondidas com as tags de recurso que você adicionou em [Tutorial: Usando tags no Cloud Assembly para gerenciar recursos do vSphere](#).

- a Na seção Entradas, adicione uma entrada de usuário chamada **posicionamento** para que o usuário possa selecionar Desenvolvimento ou Produção como o posicionamento da implantação.

Este exemplo usa o atributo `oneOf`, que permite apresentar um rótulo de linguagem natural e, ao mesmo tempo, ainda envia as cadeias de caracteres exigidas pelo processo de implantação. Por exemplo, as tags `env:dev` e `env:prod`.

```
placement:
  type: string
  oneOf:
    - title: Development
      const: 'env:dev'
    - title: Production
      const: 'env:prod'
  default: 'env:dev'
  title: Select Deployment Placement
  description: Target Environment
```

- 4 Revise o YAML completo para garantir que ele seja semelhante ao exemplo a seguir.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating system
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    oneOf:
```

```

- title: Development
  const: 'env:dev'
- title: Production
  const: 'env:prod'
default: 'env:dev'
title: Select Deployment Placement
description: Target Environment
size:
  type: string
  title: Deployment size
  description: Select the the deployment t-shirt size.
  enum:
    - small
    - medium
    - large
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: '${input.installedOS}'
      installedOS: '${input.installedOS}'
      flavor: '${input.size}'
    constraints:
      - tag: '${input.placement}'
    tags:
      - key: db
        value: mysql
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
        tags:
          - key: db
            value: mysql
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
    tags:
      - key: NGINX
        value: web

```

- 5 Clique em **Implantar** e verifique se a segunda página da solicitação é semelhante ao exemplo a seguir. Em seguida, você poderá verificar se a implantação está no desenvolvimento selecionado do pool de recursos de produção após a implantação.

The screenshot shows a window titled 'Deploy Development Te...' with a sidebar on the left containing two items: '1 Deployment Type' and '2 Deployment Inputs'. The '2 Deployment Inputs' item is selected and highlighted. The main area of the window is titled 'Deployment Inputs' and contains three input fields, each with an information icon (i) to its right:

- Operating system ***: A dropdown menu with 'centos' selected.
- Select Deployment Placement**: A dropdown menu with 'Development' selected.
- Deployment size ***: A dropdown menu with a list of options: 'small' (highlighted in blue), 'medium', and 'large'.

At the bottom right of the window, there are three buttons: 'CANCEL' (light blue), 'PREVIOUS' (light blue), and 'DEPLOY' (green).

Etapa 2: Criar uma versão e liberar o modelo de nuvem

Quando você tiver um modelo implantável, poderá disponibilizá-lo no catálogo do Service Broker para outros usuários implantarem. Para tornar o modelo de nuvem detectável de forma que seja possível adicioná-lo ao catálogo, você deve liberá-lo. Neste procedimento, iremos criar uma versão, capturar um snapshot do modelo e, em seguida, liberar o modelo.

- 1 Selecione **Design > Modelo de Nuvem** e abra o modelo na tela de design.
- 2 Clique em **Versão** e insira uma descrição.

The screenshot shows a dialog box titled 'Creating Version' with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Version ***: A text input field containing the number '7'. Below it, it says 'Last Version: 6'.
- Description**: A text area containing the text 'Placement inputs added and tested.'
- Change Log**: An empty text area.
- Release**: A checkbox labeled 'Release this version to the catalog' which is checked. Below the checkbox, there is a note: 'This cloud template is restricted to this project in the catalog. Edit shareability in cloud template level settings.'

At the bottom of the dialog, there are two buttons: 'CANCEL' (light blue) and 'CREATE' (dark blue).

- 3 Marque a caixa de seleção **Liberar** e clique em **Criar**.

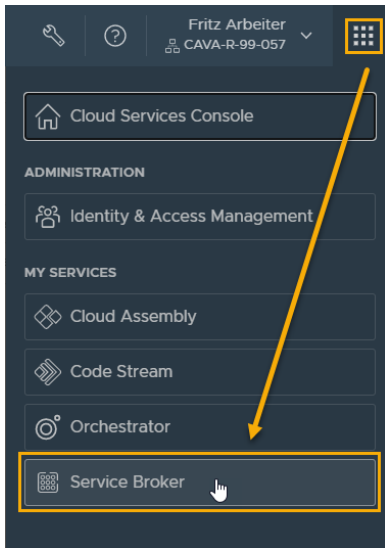
A liberação do modelo de nuvem não o adiciona automaticamente ao Service Broker. Liberá-lo o torna detectável para que você possa adicioná-lo ao catálogo.

Etapa 3: Adicionar o modelo de nuvem ao catálogo do Service Broker

Você pode usar o Service Broker para fornecer modelos de nuvem para outros consumidores na sua organização, onde eles não precisam ter conhecimento de como criar um modelo. O catálogo permite que eles implantem o modelo.

Para poder adicionar o modelo como um item de catálogo, você deve importá-lo para o Service Broker. Apenas é possível importar modelos de nuvem liberados.

- 1 Para abrir o Service Broker a partir do Cloud Assembly, clique no menu de aplicativos no canto superior direito.



- 2 Clique em **Service Broker**.
- 3 Importe o modelo de nuvem
 - a No Service Broker, selecione **Conteúdo e Políticas > Fontes de Conteúdo**.
 - b Clique em **Novo** e depois selecione **VMware Cloud Templates**.
 - c Insira um **Nome**.
Neste tutorial, insira **Cloud Assembly DevProject**.
 - d Para **Projeto**, selecione o **Projeto de Desenvolvimento** que você criou no Cloud Assembly.
 - e Clique em **Validar**.
O sistema deve indicar que foi encontrado pelo menos um item.
 - f Quando validado, clique em **Criar e Importar**.
Cloud Assembly DevProject é adicionado à lista como uma fonte de conteúdo.
- 4 Disponibilize o modelo de nuvem no catálogo.
 - a Selecione **Conteúdo e Políticas > Compartilhamento de Conteúdo**.

- b Na lista suspensa **Projeto**, selecione **Projeto de Desenvolvimento**.
 - c Clique em **Adicionar Itens** e selecione
 - d Na caixa de diálogo **Compartilhar Itens**, selecione **Cloud Assembly DevProject** e clique em **Salvar**.
- 5 Para verificar se o Modelo de Desenvolvimento foi adicionado ao catálogo, clique em **Catálogo**.
 - 6 Clique em **Solicitar** no cartão Modelo de Desenvolvimento.

Perceba que as entradas vistas no modelo de nuvem são fornecidas aqui. O próximo passo é personalizar o formulário de solicitação.

New Request

Development Template Version 8

Project * Development Project

Deployment Name *

Operating system *

Select Deployment Placement Development

Deployment size *

Etapa 4: Criar um formulário personalizado para o modelo

O objetivo desse formulário personalizado é fornecer um formulário no qual o usuário seleciona o sistema operacional e o posicionamento com base nas tags env:dev ou env:prod. Em seguida, a opção env:dev permite que o usuário selecione pequeno ou médio (grande não é uma opção). No entanto, se o usuário selecionar env:prod, não haverá uma opção para selecionar grande. O tamanho ficará oculto para o usuário, mas estará incluído na solicitação.

- 1 Para criar um formulário personalizado no Service Broker, selecione **Conteúdo e Políticas > Conteúdo**.
- 2 Clique nas elipses verticais à esquerda da entrada Modelo de Desenvolvimento e clique em **Personalizar formulário**.

3 Personalize a opção de entrada.

- a Clique nos campos da tela e configure as Propriedades conforme especificado na tabela a seguir.

| Nome do campo da tela | Aparência | Valores | Restrições |
|--|---|---|------------|
| Sistema operacional | Rótulo e tipo <ul style="list-style-type: none"> ■ Rótulo = Sistema operacional | Opções do valor <ul style="list-style-type: none"> ■ Opções de valor = Constante ■ Origem do valor = centos CentOS, ubuntu Ubuntu Este exemplo usa as opções de valor para personalizar todos os nomes de sistema operacional em minúsculas com o nome do SO preferencial. | |
| Selecionar Posicionamento da Implantação | | Opções do valor <ul style="list-style-type: none"> ■ Opções de valor = Constante ■ Origem do valor = env:dev Development, env:prod Production | |
| Tamanho da Implantação | Visibilidade <ul style="list-style-type: none"> ■ Origem do valor = Valor condicional ■ Definir valor = Sim se Selecionar Posicionamento da Implementação for igual a env:dev | Valor padrão <ul style="list-style-type: none"> ■ Origem do valor = Valor condicional ■ Definir valor = Grande se Selecionar Implantação for igual a env:prod Opções do valor <ul style="list-style-type: none"> ■ Opções de valor = Constante ■ Origem do valor = small Small, medium Medium Observe que a origem do valor não inclui Grande. Grande é excluído porque só está disponível para Produção e é o valor necessário. O valor Grande está incluído na solicitação de implantação sem uma ação iniciada pelo usuário. | |

- b Para ativar o formulário no catálogo, clique em **Ativar**.
- c Clique em **Salvar**.

- 4 Para garantir os resultados corretos enviando pelo menos um formulário Desenvolvimento Pequeno e uma solicitação de Produção e teste o formulário no catálogo.

Use os exemplos a seguir para verificar os resultados.

- a Teste o formulário de solicitação Desenvolvimento Pequeno fornecendo um nome, Teste pequeno neste exemplo, e selecionando CentOS, Desenvolvimento e Pequeno para as opções.

- b Para verificar a implantação Desenvolvimento Pequeno, selecione **Recursos > Implantações** e clique na implantação Teste pequeno.
- c Na guia Topologia, clique na guia Cloud_vSphere_Machine e localize a seção Propriedades Personalizadas no painel direito.


Alguns dos valores a revisar incluem cpuCount = 2 e flavor = small.

| Property | Value |
|---------------|----------------------------|
| costCenter | DevProject |
| cpuCount | 2 |
| datastoreName | wld01-sc2vc05-wld01-clu... |
| endpointId | d827e01c-df9e-4c80-9f1d |
| flavor | small |
| image | centos |

- d Teste o formulário de solicitação de Produção inserindo um nome, **Teste grande** neste exemplo, e selecione CentOS e Produção para as opções.

Lembre-se de que você configurou o formulário para não exibir nem exigir que o usuário selecione o tamanho.

New Request

 Development Template Version **3** ▾

Project * Development Project ▾


Deployment Name * Test large

Operating System * CentOS ▾ ⓘ

Select Deployment Placement Production ▾ ⓘ

- e Para verificar a implantação de Produção, selecione **Recursos > Implantações** e clique na implantação Teste grande.
- f Na guia Topologia, clique na guia Cloud_vSphere_Machine e localize a seção Propriedades Personalizadas no painel direito.

Alguns dos valores a serem revisados incluem cpuCount = 8 e flavor = large.


test large
Create Successful
ACTIONS ▾
🔄

No description

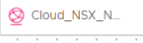

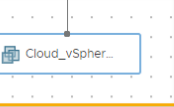
| | | |
|---------------------|----------------------------------|--------------------------|
| Owner | Expires on | Never |
| fritz | Last updated | May 21, 2021, 5:14:56 PM |
| Requestor | Created on | May 21, 2021, 4:53:05 PM |
| fritz | | |
| Project | | |
| Development Project | | |
| Cloud Template | Development Template, version: 6 | |

⬇

[HIDE SUMMARY](#) ⬆

Topology
History

Search resources

| | |
|-----------------|----------------------------|
| costCenter | DevProject |
| cpuCount | 8 |
| datastoreName | wld01-sc2vc05-wld01-clu... |
| endpointId | d827e01c-df9e-4c80-9f1d |
| flavor | large |
| image | centos |
| imageId | centos7 |

Etapa 5: Controlar as versões do modelo de nuvem no catálogo

Na maioria dos casos, você deseja disponibilizar apenas os modelos de nuvem mais recentes no catálogo do Service Broker. O procedimento a seguir oferece suporte ao desenvolvimento iterativo, no qual você libera uma versão do modelo e a adiciona ao catálogo. Porém, agora você aprimorou o modelo e deseja substituir a versão atual pela mais recente.

Na etapa 2, você criou uma versão de modelo e a liberou e, portanto, está familiarizado com o processo. Na etapa 3, você o adicionou ao catálogo. Este procedimento vincula as duas etapas anteriores à medida em que você realiza o desenvolvimento iterativo e atualiza o catálogo com a versão mais recente.

Você tem a opção de disponibilizar várias versões no catálogo.

- 1 No Cloud Assembly, crie uma versão do modelo que você deseja disponibilizar no catálogo.
 - a Selecione **Design > Modelo de Nuvem** e abra o modelo na tela de design.
 - b Clique em **Histórico de Versões**.
 - c Localize a versão que você deseja adicionar ao catálogo e clique em **Versão**.
 - d Insira uma **Descrição**, marque a caixa de seleção **Liberação** e clique em **Criar**.
 Nesse ponto, você tem a opção de manter a versão antiga no catálogo. Se quiser várias versões, ignore a próxima etapa de cancelamento do liberação de uma versão.
 - e Para disponibilizar apenas uma versão do modelo no catálogo, reveja a lista de histórico de versões e clique em **Cancelar liberação** em cada versão que você não deseja no catálogo.
- 2 Para atualizar o catálogo do Service Broker com a versão mais recente e substituir qualquer versão antiga, você deve coletar a nova versão.
 - a No Service Broker, selecione **Conteúdo e Políticas > Fontes de Conteúdo**.
 - b Clique na fonte de conteúdo DevProject do Cloud Assembly usada neste tutorial.
 - c Clique em **Validar**.
 Você deve ver uma mensagem de que um item foi encontrado.
 - d Clique em **Salvar e Importar**.
- 3 Verifique se o catálogo exibe as versões necessárias ou nenhuma versão.
 - a No Service Broker, clique em **Catálogo**.
 - b Localize o item do catálogo e clique em **Solicitação**.
 - c No topo do formulário de solicitação, clique em **Versão** e verifique a(s) versão(ões).

A captura de tela a seguir mostra 8.



Tutorial: integrando e gerenciando recursos do vSphere no vRealize Automation

Como administrador de nuvem que adicionou recentemente uma nova conta de nuvem, você deseja começar a gerenciar algumas das cargas de trabalho do vCenter Server usando o Cloud Assembly e o Service Broker. Este tutorial orienta pelo processo de integração e como configurar algumas das opções de gerenciamento para suas cargas de trabalho do vSphere existentes.

Os exemplos de tarefas de gerenciamento incluem adicionar os recursos a um projeto, criar e aplicar uma política de aprovação no Service Broker e executar algumas ações de dia 2 nos recursos para demonstrar as ferramentas de gerenciamento do ciclo de vida e acionar a política de aprovação.

Este tutorial pressupõe que, mesmo não tendo experiência com o Cloud Assembly, você já tenha configurado uma nova conta de nuvem do vSphere. Quando você adicionar a conta de nuvem, o Cloud Assembly descobrirá os recursos atualmente não gerenciados na sua instância do vSphere.

O que fazer primeiro

- Adicione sua nova conta do vCenter Server. Para obter instruções adicionais, consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- Verifique se a sua conta de usuário tem pelo menos as funções de serviço Administrador do Cloud Assembly e Administrador do Service Broker. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Para testar corretamente a política de aprovação sob a perspectiva de um dos seus usuários, verifique se você tem uma conta de usuário do que tenha apenas as funções de usuário a seguir. Neste tutorial, o usuário se chama Sylvia.
 - Membro da Organização
 - Usuário do Cloud Assembly
 - Usuário do Service Broker

Para obter mais informações sobre funções de usuário, consulte [Quais são as funções de usuário do vRealize Automation](#).

Etapa 1: Verificar se o Cloud Assembly descobriu os recursos

Ao adicionar uma conta do vCenter Server, o Cloud Assembly descobre os recursos na instância do vCenter Server. Você pode verificar se as máquinas que deseja começar a gerenciar estão disponíveis para integração.

- 1 No Cloud Assembly, selecione **Recursos > Recursos > Máquinas Virtuais**.
- 2 Na grade, analise a **Origem** e a **Conta/Região**.

O tipo de origem Descoberta indica que a máquina foi descoberta na sua instância do vSphere em vez de implantada pelo vRealize Automation ou já está integrada.

Neste exemplo, a Conta/Região é `vCenter Account / wld01-DC`.

| Name | Status | Account / Region | Address | Project | Owner | Creation Time | Origin | Tags |
|-----------------------|--------|----------------------------|---------|--------------------|--------|--------------------------|----------|----------|
| DevProject-116 | ▶ On | vCenter Account / wld01-DC | N/A | | | Jul 26, 2021, 2:29:15 PM | Discover | |
| DevProject-centos-010 | ▶ On | vCenter Account / wld01-DC | N/A | Onboarding Project | fritz | Jul 26, 2021, 2:29:18 PM | Deployed | db:mysql |
| DevProject-centos-012 | ▶ On | vCenter Account / wld01-DC | N/A | | | Jul 26, 2021, 2:29:18 PM | Discover | |
| DevProject-centos-013 | ▶ On | vCenter Account / wld01-DC | N/A | | | Jul 26, 2021, 2:29:15 PM | Discover | db:mysql |
| DevProject-centos-016 | ▶ On | vCenter Account / wld01-DC | N/A | Onboarding Project | sylvia | Jul 26, 2021, 2:29:15 PM | Deployed | db:mysql |

Etapa 2: Criar um projeto de destino

Crie um projeto ao qual você possa atribuir as máquinas integradas. Para gerenciar os recursos, eles devem fazer parte de um projeto que inclua a zona de nuvem de origem na qual foram originalmente implantados.

Para testar este tutorial, você deve ter outro usuário que não seja administrador. Nesta etapa, como administrador, você adiciona Sylvia como membro do projeto.

Para obter mais informações sobre projetos, consulte [Capítulo 5 Como adicionar e gerenciar projetos do Cloud Assembly](#).

- 1 No Cloud Assembly, selecione **Infraestrutura > Projetos > .**
- 2 Na página Projetos, clique em **Novo Projeto**.
- 3 Insira o **Nome** do projeto.

Neste tutorial, o nome do projeto é **Projeto de Integração**.

- 4 Clique na guia **Usuários**.
 - a Clique em **Adicionar Usuários** e adicione pelo menos um usuário como membro do projeto.

Neste tutorial, você adiciona Sylvia.

- b Clique em **Adicionar**.
- 5 Clique em **Provisionamento**.
 - a Clique em **Adicionar Zona**.
 - b Clique em **Zona de Nuvem**.
 - c Selecione a conta/região identificada na Etapa 1.

Neste tutorial, o valor de amostra é Conta do vCenter / wld01-DC.

New Project

Summary Users **Provisioning** Kubernetes Provisioning

Zones

Specify the zones that can be used when users provision deployments in this project. ⓘ

+ ADD ZONE × REMOVE

| <input type="checkbox"/> | Name | Status | Description | Priority | Instances | Memory Limit (MB) | CPU Limit | Storage Limit (GB) | Capability Tags |
|--------------------------|----------------------------|--------|-------------|----------|-----------|-------------------|-----------|--------------------|-----------------|
| <input type="checkbox"/> | vCenter Account / wld01-DC | -- | | 0 | Unlimited | Unlimited | Unlimited | Unlimited | |

1 - 1 of 1 zones

Specify the placement policy that will be applied when selecting a cloud zone for provisioning.

Placement policy **DEFAULT** ⓘ

- d Clique em **Adicionar**.
- 6 Clique em **Criar**.

Etapa 3: Criar e executar um plano de integração

Como administrador de nuvem, você integra máquinas descobertas da sua instância do vSphere, para poder aplicar governança e gerenciar os recursos com ações de dia 2.

Para obter mais informações sobre planos de integração, consulte [O que são planos de integração no Cloud Assembly](#).

- 1 No Cloud Assembly, selecione **Infraestrutura > Integração** e clique em **Novo Plano de Integração**.
- 2 Insira as informações de integração.

| Configuração | Valor de amostra |
|----------------|------------------------------|
| Nome do plano | Plano de integração wld01-DC |
| Conta de nuvem | Conta do vCenter |
| Projeto padrão | Projeto de integração |

- 3 Clique em **Criar**.
- 4 Adicione as máquinas que você deseja integrar.

Não execute o plano de integração até concluir todas as etapas a seguir.

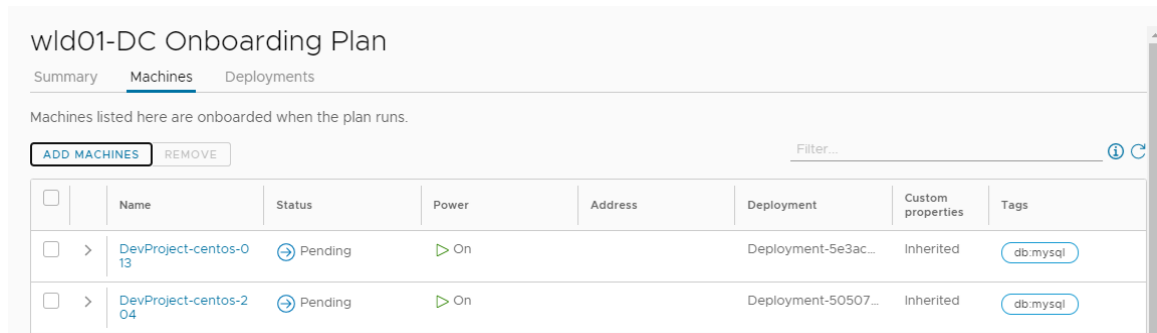
- a Clique em **Máquinas** e depois clique em **Adicionar Máquinas**.
- b Selecione as máquinas que você deseja incluir no plano e clique em **OK**.

Para este tutorial, apenas duas máquinas são selecionadas.

- c Na caixa de diálogo Criar Implantações, selecione **Criar implantações de plano para cada máquina** e clique em **Criar**.

Selecione essa opção quando quiser as máquinas como implantações individuais, para que você possa gerenciá-las como recursos individuais.

- d As máquinas selecionadas são adicionadas à lista.



The screenshot shows the 'wld01-DC Onboarding Plan' interface. It has tabs for 'Summary', 'Machines', and 'Deployments'. Below the tabs, it says 'Machines listed here are onboarded when the plan runs.' There are 'ADD MACHINES' and 'REMOVE' buttons. A table lists the machines with columns for Name, Status, Power, Address, Deployment, Custom properties, and Tags.

| | Name | Status | Power | Address | Deployment | Custom properties | Tags |
|--------------------------|-----------------------|---------|-------|---------|---------------------|-------------------|----------|
| <input type="checkbox"/> | DevProject-centos-013 | Pending | On | | Deployment-5e3ac... | Inherited | db.mysql |
| <input type="checkbox"/> | DevProject-centos-204 | Pending | On | | Deployment-50507... | Inherited | db.mysql |

5 Renomeie as implantações.

- a Clique em **Implantações** na página de integração.
- b Para alterar o nome da implantação gerado, selecione uma implantação e clique em **Renomear**.

- c Insira o novo nome e clique em **Salvar**.

Por exemplo, Máquina integrada 1.

- d Repita conforme necessário.

6 Atribua um proprietário às implantações.

Se nenhum proprietário for atribuído, você se tornará o proprietário. O proprietário deve ser membro do projeto de destino.

Este tutorial atribui todas as implantações ao mesmo proprietário. Opcionalmente, você pode atribuir diferentes implantações a diferentes proprietários.

- a Selecione todas as implantações e clique em **Editar Proprietário**.
- b Selecione o proprietário e clique em **Salvar**.

Revise o nome da implantação e as alterações do proprietário na grade.

wld01-DC Onboarding Plan

Summary Machines Deployments

These deployments will be created or updated when the plan runs. By default each added machine is placed in its own Cloud Assembly deployment.

RENAME EDIT OWNER CLOUD TEMPLATE REMOVE

| <input type="checkbox"/> | Deployment Name | Status | Create Cloud Template | Owner | Components |
|--------------------------|--------------------------|--------|-----------------------|--------|------------|
| <input type="checkbox"/> | > Onboarded deployment 1 | ✓ | | sylvia | 1 |
| <input type="checkbox"/> | > Onboarded deployment 2 | ✓ | | sylvia | 1 |

2 deployments

SAVE RUN CANCEL

7 Clique em **Executar**.

Depois que você executar o plano de integração, não será possível modificar o nome ou atribuir proprietários. Se você adicionar mais máquinas ao plano, poderá modificar o nome ou o proprietário.

8 Revise os recursos que você integrou como implantações.

a Selecione **Recursos > Implantações**.

b Para localizar implantações, é possível pesquisar por nome de implantação, projeto ou proprietário.

Deployments 20 Items of 26

Search deployments | Sort: Created on (descending)

| | Name | Address | Owner | Project | Status | Expires on | Price |
|---|-----------------------|---------|--------|--------------------|------------------|------------|-------|
| > | Onboarded machine 1 | | sylvia | Onboarding Project | | Never | |
| ∨ | Onboarded machine 2 | | sylvia | Onboarding Project | | Never | |
| | DevProject-centos-016 | | | | On | | |
| > | Resize | | fritz | onboard project 2 | | Never | |
| > | Resize Boot Disk | | fritz | Onboarding Project | Onboard — Failed | Never | |
| > | Resize Disk | | fritz | Onboarding Project | | Never | |
| > | Shutdown | | fritz | Onboarding Project | | Never | |
| > | Suspend | | fritz | Onboarding Project | | Never | |
| > | Unregister | | fritz | Onboarding Project | | Never | |
| > | Update Tags | | fritz | Onboarding Project | | Never | |
| > | Delete Snapshot | | fritz | Onboarding Project | | Never | |

Agora que você trouxe máquinas para o vRealize Automation, poderá começar a gerenciá-las.

Etapa 4: Redimensionar uma implantação

Realize essa etapa como administrador de nuvem e familiarize-se com a operação das ações de dia 2. As alterações que você pode fazer nas implantações são chamadas de ações de dia 2. O uso de ações de dia 2 é a primeira etapa no gerenciamento dos seus recursos.

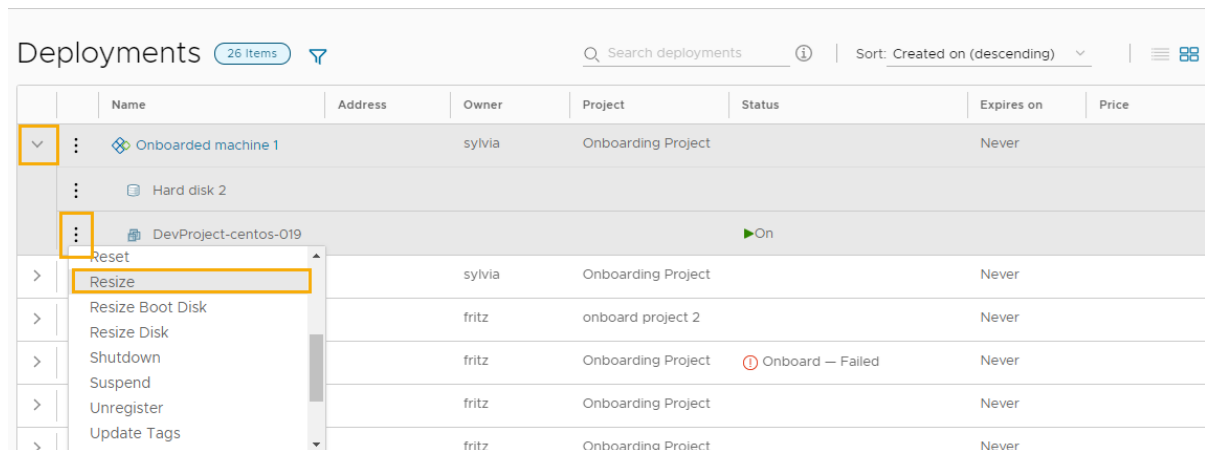
Para este tutorial, você acha que a contagem de CPUs em uma máquina é muito alta e deseja diminuir as CPUs consumidas. Este procedimento pressupõe que você esteja executando a ação de redimensionamento em uma máquina ligada do vSphere. Ele também pressupõe que você não tenha uma política de dia 2 que proíba um usuário de executar essa ação.

As ações disponíveis dependem do tipo de recurso, do estado do recurso e das políticas de dia 2. Para obter mais informações sobre ações de dia 2, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

- 1 No Cloud Assembly, selecione **Recursos > Implantações** e localize suas implantações integradas.

É possível usar as opções de pesquisa ou filtro.

- 2 Expanda a implantação usando a seta à esquerda, clique nas reticências verticais no nome da máquina e clique em **Redimensionar**.

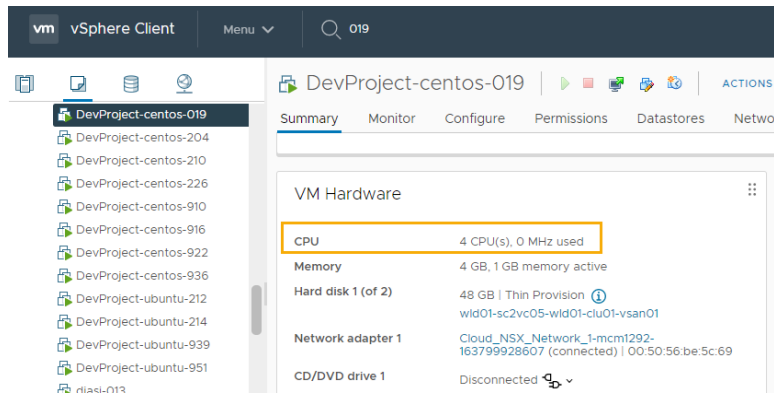


- 3 Na caixa de diálogo **Redimensionar**, diminua a contagem de CPUs para **4** e clique em **Enviar**.

O valor sugerido é um exemplo. Altere a contagem de CPUs para um valor que funcione no seu ambiente.

A ação é executada na máquina.

- 4 Para verificar se a contagem de CPUs foi alterada, abra a implantação e verifique a propriedade personalizada `cpuCount` da máquina.
- 5 Você também pode verificar essa contagem no vCenter Server.



Etapa 5: Aplicar políticas de aprovação

Como administrador de nuvem, você pode aplicar governança ao vRealize Automation para limitar o que os usuários podem fazer ou para exigir que eles recebam aprovação antes de fazer isso. Este tutorial mostra como aplicar políticas de aprovação à ação de redimensionamento, para que os seus usuários não possam reconfigurar uma máquina, talvez de forma catastrófica, sem a sua aprovação ou a aprovação de outro administrador.

As políticas são criadas no Service Broker. No entanto, elas políticas aplicam-se às solicitações relevantes no Cloud Assembly e no Service Broker.

Como aprovador, você deve responder à solicitação de aprovação no Service Broker.

- 1 No Service Broker, selecione **Conteúdo e Políticas > Políticas > Definições** e clique em **Nova Política**.
- 2 Clique em **Política de Aprovação**.
- 3 Configure a política de aprovação.

Resize Approval Policy [DELETE](#)

Approval policies control who must agree to a deployment or day 2 action before the request is provisioned. ⓘ

Type: Approval

Name *: Resize Approval Policy

Description:

Scope *: ☐ Organization / Multiple Projects Apply the policy to all or a selection of projects in this organization. To target multiple projects, select project based criteria. ⓘ
☒ Project Apply the policy to a single project in this organization. ⓘ
Onboarding Project

Criteria: ⓘ

Approval type *: ☒ User based ☐ Role based ⓘ

Approver mode *: ☒ Any ☐ All ⓘ

Approvers *: ⓘ

| <input type="checkbox"/> | Name | Email | Type |
|--------------------------|----------------|-------|------|
| <input type="checkbox"/> | Fritz Arbeiter | fritz | User |
| <input type="checkbox"/> | 1 user | | |

Auto expiry decision *: Reject ⓘ

Auto expiry trigger *: 1 days ⓘ

Actions *: ⓘ

| <input type="checkbox"/> | Actions |
|--------------------------|------------------------------|
| <input type="checkbox"/> | Cloud.vSphere.Machine.Resize |

A tabela a seguir inclui valores de amostra que ilustram como criar a política.

| Configuração | Valor de amostra |
|---------------------------------|--|
| Nome | Redimensionar Política de Aprovação |
| Escopo | Selecione Projeto e depois Projeto de Integração . A política de aprovação é acionada quando um usuário que é membro do projeto executa uma ação de dia 2 de redimensionamento. |
| Tipo de aprovação | Com base no usuário Esse valor permite designar os aprovadores. |
| Modo de aprovador | Qualquer Se você tiver vários aprovadores, a solicitação de aprovação poderá ser resolvida por pelo menos um aprovador. |
| Aprovadores | Adicione a si mesmo como aprovador. |
| Decisão de expiração automática | Rejeitar Ao rejeitar uma solicitação não analisada, você reduz o risco de tornar uma máquina inutilizável ou com excesso de recursos. |

| Configuração | Valor de amostra |
|---------------------------------|---|
| Gatilho de expiração automática | 1 |
| Ações | <p>Selecione a ação de redimensionamento que aciona a política de aprovação.</p> <ol style="list-style-type: none"> 1 Insira machine.resize em Pesquisar. 2 Clique em Selecione vários na lista suspensa de resultados da pesquisa. 3 Selecione Cloud.vSphere.Machine.Resize. <p>Para este tutorial, que é baseado no vSphere, selecione a ação vSphere.Machine. Se quiser que a política de ação seja aplicada a outros tipos de recursos, você poderá adicionar as outras ações Machine.Resize.</p> |

Etapa 6: Fazer uma solicitação de redimensionamento como um usuário

Nesta etapa, você faz login no Service Broker como membro da Organização e usuário do Service Broker e executa uma solicitação de redimensionamento de dia 2. A solicitação cria uma solicitação de aprovação. O usuário também pode realizar as mesmas etapas no Cloud Assembly.

Na etapa seguinte, você fará login como o usuário que atribuiu como aprovador na Etapa 5 e aprovará a solicitação.

- 1 Faça login no Service Broker como usuário.

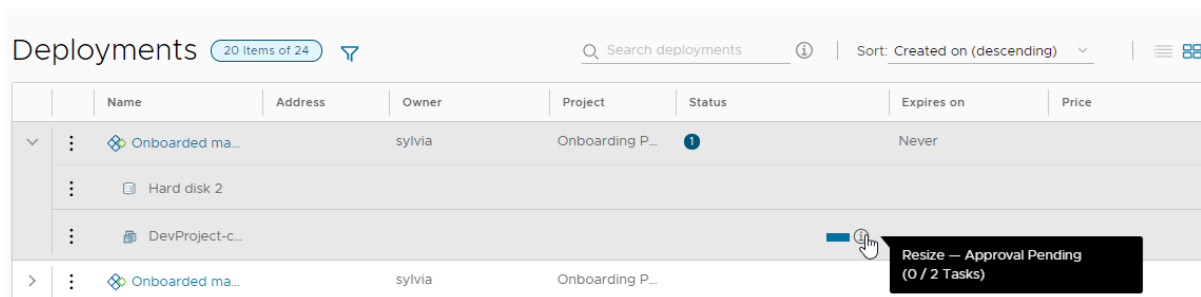
Neste tutorial, o usuário é Sylvia.

- 2 Selecione **Recursos > Implantações** e localize Máquina integrada 1.

Essa implantação é aquela na qual você executou a ação de redimensionamento na Etapa 4, alterando o número de CPUs de 8 para 4. Caso tenha usado um valor diferente, modifique a máquina da maneira que deseja testá-la.

- 3 Execute a ação **Redimensionar** na máquina, aumentando a contagem de CPUs para **6**.
- 4 Observe que a solicitação está aguardando aprovação.

Para ver o status pendente, passe o cursor sobre o ícone de informações na grade ou abra a implantação e reveja a guia **Histórico**.



- 5 Como usuário, a alteração solicitada por Sylvia não continuará até que ela seja aprovada.

- 6 Faça logout do Service Broker como o usuário.

Na Etapa 7, você fará login como o aprovador atribuído e responderá à solicitação.

Etapa 7: Responder a uma solicitação de aprovação

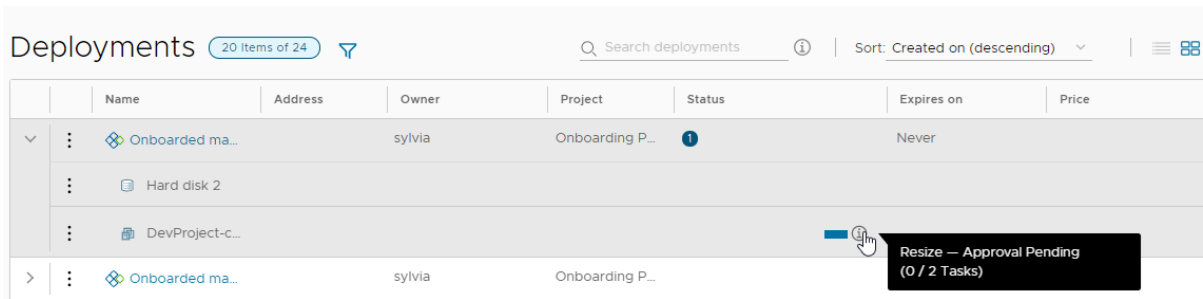
Quando uma solicitação requer uma aprovação e você é o aprovador, você recebe uma mensagem por e-mail. Para este tutorial, não estamos aguardando a mensagem. Em vez disso, o processo orienta diretamente pelo processo de responder a solicitações de aprovação usando a guia Aprovações do Service Broker.

- 1 Faça login no Service Broker como o usuário que você atribuiu como o aprovador na Etapa 5.

Neste tutorial, o aprovador é Fritz.

- 2 Selecione **Recursos > Implantações** e localize Máquina integrada 1.

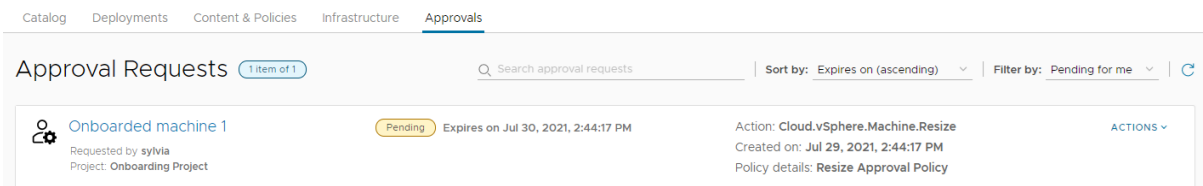
O status é que a grade é idêntica àquela exibida para Sylvia.



| | Name | Address | Owner | Project | Status | Expires on | Price |
|---|---------------------|---------|--------|--------------------|--------------------------------|------------|-------|
| ▼ | Onboarded machine 1 | | sylvia | Onboarding Project | Approval Pending (0 / 2 Tasks) | Never | |
| | Hard disk 2 | | | | | | |
| | DevProject-c... | | | | | | |
| > | Onboarded machine 1 | | sylvia | Onboarding Project | | | |

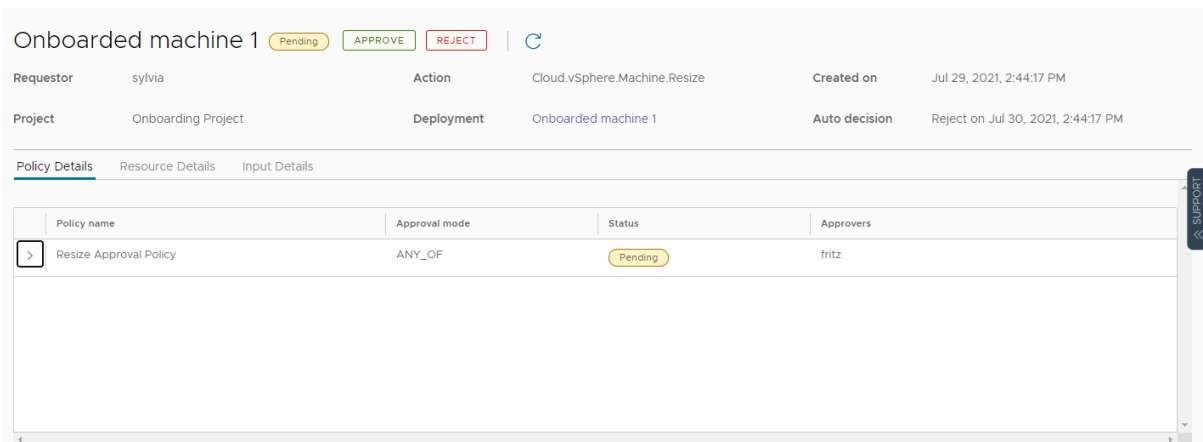
- 3 Clique na guia **Aprovações**.

Observe que você tem uma solicitação de aprovação pendente.



| Approval Requests (1 item of 1) | | | |
|---------------------------------|---------|-------------------------------------|--|
| Onboarded machine 1 | Pending | Expires on Jul 30, 2021, 2:44:17 PM | Action: Cloud.vSphere.Machine.Resize Created on: Jul 29, 2021, 2:44:17 PM Policy details: Resize Approval Policy |

- 4 Para exibir os detalhes da solicitação, clique no nome da implantação.



| Onboarded machine 1 (Pending) | | | |
|-------------------------------|--------------------------|---------------|------------------------------------|
| Requestor | sylvia | Action | Cloud.vSphere.Machine.Resize |
| Project | Onboarding Project | Deployment | Onboarded machine 1 |
| Created on | Jul 29, 2021, 2:44:17 PM | Auto decision | Reject on Jul 30, 2021, 2:44:17 PM |

| Policy Details | | | |
|------------------------|---------------|---------|-----------|
| Policy name | Approval mode | Status | Approvers |
| Resize Approval Policy | ANY_OF | Pending | fritz |

- 5 Clique em **Aprovar**, forneça um comentário, se necessário, e clique em **Aprovar**.
- 6 Retorne à página **Implantações** para ver que a ação de redimensionamento de Sylvia está agora em andamento.

| Name | Address | Owner | Project | Status | Expires on | Price |
|-----------------|---------|--------|-----------------|-----------------|------------|-------|
| Onboarded ma... | | sylvia | Onboarding P... | Onboarding P... | Never | |
| Hard disk 2 | | | | | | |
| DevProject-c... | | | | | | |
| Onboarded ma... | | sylvia | Onboarding P... | | | |

- 7 Quando a ação de redimensionamento for concluída, você poderá verificar o número de CPUs nos detalhes da implantação e no vSphere Client.

Este tutorial orientou você pelo processo de trazer as máquinas no vRealize Automation, para que você possa começar a gerenciar o ciclo de vida do recurso.

Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly

Este tutorial completo do Cloud Assembly mostra como implantar em uma configuração de várias nuvens. Você implanta o mesmo modelo de nuvem em mais de um provedor, neste caso, a AWS e o Microsoft Azure.

Neste exemplo, o aplicativo é um site do WordPress. Observe a configuração sequencial para compreender o processo que leva todo o design até a conclusão.

Lembre-se de que os nomes e valores exibidos são apenas exemplos. Você não poderá usá-los literalmente no seu ambiente.

Para atender às suas próprias necessidades de implantação e infraestrutura de nuvem, considere onde você faria suas próprias substituições dos valores de exemplo.

Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo

Primeiro, configure os recursos nos quais os usuários de engenharia do Cloud Assembly poderão posteriormente desenvolver, testar e colocar o aplicativo em produção.

A infraestrutura inclui destinos de nuvem e definições em torno das máquinas, redes e armazenamento que o site do WordPress precisará.

Pré-requisitos

Fazer login no Cloud Assembly como Administrador do Cloud Assembly.

1. Adicionar contas de nuvem

Nesta etapa, o administrador de nuvem adiciona duas contas de nuvem. O objetivo do projeto de exemplo é desenvolver e testar o trabalho no AWS e partir para a produção no Azure.

- 1 Vá para **Infraestrutura > Conexões > Contas de Nuvem**.
- 2 Clique em **Adicionar Conta de Nuvem**, selecione Amazon Web Services e digite os valores.

| Configuração | Valor de amostra |
|-------------------------|----------------------|
| ID da chave de acesso | R5SDR3PXVV2ZW8B7YNSM |
| Chave secreta de acesso | SZXAINXU4UHNAQ1E156S |
| Nome | OurCo-AWS |
| Descrição | WordPress |

Lembre-se de que todos os valores são apenas exemplos. As especificações da conta variarão.

- 3 Para verificar as credenciais, clique em **Validar**.
- 4 Clique em **Adicionar**.
- 5 Edite a **Configuração** da conta adicionada recentemente e permita o provisionamento para as regiões us-east-1 e us-west-2.
- 6 Clique em **Adicionar Conta de Nuvem**, selecione Microsoft Azure e digite valores.

| Configuração | Valor de amostra |
|-------------------------------------|--|
| ID da assinatura | ef2avpf-dfdv-zxluguii-g4h0-i8ep2jwp4c9arbfe |
| ID do Tenant | dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r |
| ID do aplicativo cliente | bg224oq-3ptp-mbhi6aa05-q511-uflyjr2sttyik6bs |
| Chave secreta do aplicativo cliente | 7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmd |
| Nome | OurCo-Azure |
| Descrição | WordPress |

- 7 Para verificar as credenciais, clique em **Validar**.
- 8 Clique em **Adicionar**.
- 9 Edite a **Configuração** da conta adicionada recentemente e permita o provisionamento para a região East US.

2. Adicionar zonas de nuvem

Nesta etapa de exemplo, o administrador de nuvem adiciona três zonas de nuvem, para desenvolvimento, teste e produção.

- 1 Vá para **Infraestrutura > Configurar > Zonas de Nuvem**.
- 2 Clique em **Nova Zona de Nuvem** e digite os valores para o ambiente de desenvolvimento.

| Configuração da Zona de Nuvem | Valor de amostra |
|-------------------------------|---------------------|
| Conta/região | OurCo-AWS/us-east-1 |
| Nome | OurCo-AWS-US-East |
| Descrição | WordPress |
| Política de colocação | Padrão |
| Tags de capacidade | env:dev |

Lembre-se de que todos os valores são apenas exemplos. As especificidades da zona variarão.

- 3 Clique em **Processamento** e verifique se as zonas esperadas estão lá.
- 4 Clique em **Criar**.
- 5 Repita o processo duas vezes, com valores para os ambientes de teste e produção.

| Configuração da Zona de Nuvem | Valor de amostra |
|-------------------------------|---------------------|
| Conta/região | OurCo-AWS/us-west-2 |
| Nome | OurCo-AWS-US-West |
| Descrição | WordPress |
| Política de colocação | Padrão |
| Tags de capacidade | env:test |

| Configuração da Zona de Nuvem | Valor de amostra |
|-------------------------------|---------------------|
| Conta/região | OurCo-Azure/East US |
| Nome | OurCo-Azure-East-US |
| Descrição | WordPress |
| Política de colocação | Padrão |
| Tags de capacidade | env:prod |

3. Adicionar mapeamentos de tipo

Nesta etapa de exemplo, o administrador de nuvem adiciona mapeamentos de tipo para atender às necessidades de capacidade que podem variar, dependendo da implantação.

O mapeamento de variações considera implantações de máquinas de diferentes tamanhos e é informalmente conhecido como dimensionamento com tamanhos fixos.

- 1 Vá para **Infraestrutura > Configurar > Mapeamentos de Tipo**. Cada zona de nuvem precisa permitir tipos small, medium e large.
- 2 Clique em **Novo Mapeamento de Tipo** e digite os valores para a zona de nuvem de desenvolvimento.

| Configuração | Valor de amostra |
|--------------|---------------------|
| Nome do tipo | small |
| Conta/região | OurCo-AWS/us-east-1 |
| Valor | t2.micro |
| Conta/região | OurCo-AWS/us-west-2 |
| Valor | t2.micro |
| Conta/região | OurCo-Azure/East US |
| Valor | Standard_A0 |

Lembre-se de que todos os valores são apenas exemplos. Os tipos variarão.

- 3 Clique em **Criar**.
- 4 Repita o processo duas vezes, com valores para os tipos médio e grande.

| Configuração | Valor de amostra |
|--------------|---------------------|
| Nome do tipo | medium |
| Conta/região | OurCo-AWS/us-east-1 |
| Valor | t2.medium |
| Conta/região | OurCo-AWS/us-west-2 |
| Valor | t2.medium |
| Conta/região | OurCo-Azure/East US |
| Valor | Standard_A3 |

| Configuração | Valor de amostra |
|--------------|---------------------|
| Nome do tipo | large |
| Conta/região | OurCo-AWS/us-east-1 |
| Valor | t2.large |

| Configuração | Valor de amostra |
|--------------|---------------------|
| Conta/região | OurCo-AWS/us-west-2 |
| Valor | t2.large |
| Conta/região | OurCo-Azure/East US |
| Valor | Standard_A7 |

4. Adicionar mapeamentos de imagem

Nesta etapa de exemplo, o administrador de nuvem adiciona um mapeamento de imagem para o Ubuntu, o host para o servidor WordPress e o servidor do banco de dados MySQL.

Planeje o sistema operacional adicionando mapeamentos de imagem. Cada zona de nuvem precisa de um mapeamento de imagem do Ubuntu.

- 1 Vá para **Infraestrutura > Configurar > Mapeamentos de Imagem**.
- 2 Clique em **Novo Mapeamento de Imagem** e digite os valores para servidores Ubuntu.

| Configuração | Valor de amostra |
|----------------|------------------------------------|
| Nome da imagem | ubuntu |
| Conta/região | OurCo-AWS/us-east-1 |
| Valor | ubuntu-16.04-server-cloudimg-amd64 |
| Conta/região | OurCo-AWS/us-west-2 |
| Valor | ubuntu-16.04-server-cloudimg-amd64 |
| Conta/região | OurCo-Azure/East US |
| Valor | azul-zulu-ubuntu-1604-923eng |

Lembre-se de que todos os valores são apenas exemplos. As imagens variarão.

- 3 Clique em **Criar**.

5. Adicionar perfis de rede

Nesta etapa de exemplo, o administrador de nuvem adiciona um perfil de rede a cada zona de nuvem.

Em cada perfil, o administrador adiciona uma rede para as máquinas do WordPress e uma segunda rede que se situará no outro lado de um balanceador de carga eventual. A segunda rede será aquela à qual os usuários eventualmente se conectam.

- 1 Vá para **Infraestrutura > Configurar > Perfis de Rede**.
- 2 Clique em **Novo Perfil de Rede** e crie um perfil para a zona de nuvem de desenvolvimento.

| Configuração do perfil de rede | Valor de amostra |
|--------------------------------|---------------------|
| Conta/região | OurCo-AWS/us-east-1 |
| Nome | devnets |
| Descrição | WordPress |

3 Clique em **Redes** e clique em **Adicionar Rede**.

4 Selecione wpnet, appnet-public e clique em **Adicionar**.

Lembre-se de que todos os valores são apenas exemplos. Os nomes de rede variarão.

5 Clique em **Criar**.

Este exemplo do WordPress não exige especificar as configurações de política de rede ou de segurança de rede.

6 Repita o processo duas vezes para criar um perfil de rede para o exemplo do WordPress e para as zonas de nuvem de produção. Em cada caso, adicione as redes wpnet e appnet-public.

| Configuração do perfil de rede | Valor de amostra |
|--------------------------------|---------------------|
| Conta/região | OurCo-AWS/us-west-2 |
| Nome | testnets |
| Descrição | WordPress |

| Configuração do perfil de rede | Valor |
|--------------------------------|---------------------|
| Conta/região | OurCo-Azure/East US |
| Nome | prodnets |
| Descrição | WordPress |

6. Adicionar perfis de armazenamento

Nesta etapa de exemplo, o administrador de nuvem adiciona um perfil de armazenamento a cada zona de nuvem.

O administrador coloca o armazenamento rápido na zona de produção e no armazenamento geral em desenvolvimento e teste.

1 Vá para **Infraestrutura > Configurar > Perfis de Armazenamento**.

2 Clique em **Novo Perfil de Armazenamento** e crie um perfil para a zona de nuvem de desenvolvimento.

Campos adicionais aparecem depois de selecionar a conta/região.

| Configuração do perfil de armazenamento | Valor de amostra |
|---|------------------------|
| Conta/região | OurCo-AWS/us-east-1 |
| Nome | OurCo-AWS-US-East-Disk |
| Descrição | WordPress |
| Tipo de dispositivo | EBS |
| Tipo de volume | SSD de Propósito Geral |
| Tags de capacidade | armazenamento:geral |

Lembre-se de que todos os valores são apenas exemplos.

- 3 Clique em **Criar**.
- 4 Repita o processo para criar um perfil para a zona de nuvem de teste.

| Configuração do perfil de armazenamento | Valor de amostra |
|---|------------------------|
| Conta/região | OurCo-AWS/us-west-2 |
| Nome | OurCo-AWS-US-West-Disk |
| Descrição | WordPress |
| Tipo de dispositivo | EBS |
| Tipo de volume | SSD de Propósito Geral |
| Tags de capacidade | armazenamento:geral |

- 5 Repita o processo para criar um perfil para a zona de nuvem de produção, que tem configurações diferentes, pois é uma zona do Azure.

| Configuração do perfil de armazenamento | Valor de amostra |
|---|--------------------------|
| Conta/região | OurCo-Azure/East US |
| Nome | OurCo-Azure-East-US-Disk |
| Descrição | WordPress |
| Tipo de armazenamento | Discos gerenciados |
| Tipo de disco | LRS premium |
| Cache de disco do SO | Somente leitura |
| Cache do disco de dados | Somente leitura |
| Tags de capacidade | armazenamento:rápido |

O que fazer em seguida

Crie um projeto para identificar usuários e para definir configurações de provisionamento. Consulte [Parte 2: Criar o projeto do Cloud Assembly de exemplo](#).

Parte 2: Criar o projeto do Cloud Assembly de exemplo

O projeto do Cloud Assembly de exemplo habilita os usuários que podem provisionar e configurar o nível de provisionamento possível.

Os projetos definem as configurações de usuário e provisionamento.

- Usuários e seu nível de permissão de função
- Prioridade para implantações à medida que elas estão sendo provisionadas para uma zona de nuvem
- Número máximo de instâncias de implantação por zona de nuvem

Procedimentos

- 1 Vá para **Infraestrutura > Administração > Projetos**.
- 2 Clique em **Novo Projeto** e digite o nome WordPress.
- 3 Clique em **Usuários** e clique em **Adicionar Usuários**.
- 4 Adicione endereços de e-mail e funções para os usuários.

Para adicionar um usuário com êxito, o administrador do VMware Cloud Services deverá ativar o acesso do usuário ao Cloud Assembly.

Lembre-se de que os endereços mostrados aqui são apenas exemplos.

- chris.ladd@ourco.com, Membro
 - kerry.mott@ourco.com, Membro
 - pat.tubb@ourco.com, Administrador
- 5 Clique em **Provisionamento** e clique em **Adicionar Zona de Nuvem**.
 - 6 Adicione as zonas de nuvem nas quais os usuários podem implantar.

| Configuração da zona de nuvem do projeto | Valor de amostra |
|--|---------------------|
| Zona de nuvem | OurCo-AWS-US-East |
| Prioridade de provisionamento | 1 |
| Limite de instâncias | 5 |
| Zona de nuvem | OurCo-AWS-US-West |
| Prioridade de provisionamento | 1 |
| Limite de instâncias | 5 |
| Zona de nuvem | OurCo-Azure-East-US |
| Prioridade de provisionamento | 0 |
| Limite de instâncias | 1 |

- 7 Clique em **Criar**.
- 8 Acesse **Infraestrutura > Configurar > Zonas de Nuvem** e abra uma zona criada anteriormente.
- 9 Clique em **Projetos** e verifique se o WordPress é um projeto que tem permissão para provisionar para a zona.
- 10 Verifique as outras zonas que você criou.

Próximo passo

Crie um modelo de nuvem básico.

Parte 3: Projetar e implantar o exemplo de modelo do Cloud Assembly

Em seguida, defina o aplicativo de exemplo (o site do WordPress) na forma de um modelo de nuvem genérico. O modelo pode ser implantado em diferentes fornecedores de nuvem sem a necessidade de alterar seu design.

O exemplo consiste em um servidor de aplicativos WordPress, um servidor de banco de dados MySQL e recursos de suporte. O modelo começa com alguns recursos e, em seguida, se expande conforme esses recursos são modificados e mais recursos são adicionados.

Aqui estão os valores [Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo](#), a infraestrutura que foi definida por um administrador de nuvem:

- Duas contas de nuvem, AWS e Azure.
- Três ambientes de zona de nuvem:
 - Desenvolvimento — OurCo-AWS-US-East
 - Teste — OurCo-AWS-US-West
 - Produção — OurCo-Azure-East-US
- Mapeamentos de tipo com recursos de processamento pequenos, médios e grandes para cada zona.
- Mapeamentos de imagem para o Ubuntu configurado em cada zona.
- Perfis de rede com sub-redes internas e externas para cada zona.
- Armazenamento no qual implantar; armazenamento geral para a zona de desenvolvimento e teste e armazenamento rápido para a zona de produção.
- O projeto de exemplo inclui todos os três ambientes de zona de nuvem, mais os usuários que podem criar designs.

Pré-requisitos

Para acompanhar, você deve estar familiarizado com seus próprios valores de infraestrutura. Esse exemplo usa a AWS para desenvolvimento e teste e o Azure para produção. Ao criar o próprio modelo de nuvem, substitua os valores, normalmente definidos pelo administrador da nuvem.

Procedimentos

1 Criar um modelo de nuvem básico

Neste exemplo de design do Cloud Assembly, comece com um modelo de nuvem que contenha apenas recursos mínimos do WordPress, como ter apenas um servidor de aplicativos.

2 Testar um modelo de nuvem básico

Durante o design, muitas vezes você cria um modelo de nuvem começando com o essencial e, em seguida, implantando e testando conforme esse modelo se expande. Este exemplo demonstra alguns dos testes em andamento integrados ao Cloud Assembly.

3 Expandir um modelo de nuvem

Depois de criar e testar o modelo do Cloud Assembly básico para o aplicativo de exemplo, você o expande em um aplicativo de várias camadas que pode ser implantado para desenvolvimento, teste e, eventualmente, produção.

Criar um modelo de nuvem básico

Neste exemplo de design do Cloud Assembly, comece com um modelo de nuvem que contenha apenas recursos mínimos do WordPress, como ter apenas um servidor de aplicativos.

O Cloud Assembly é uma ferramenta de infraestrutura como código. Arraste os recursos até a tela de design para começar. Em seguida, preencha os detalhes usando o editor de código à direita da tela.

O editor de código permite que você digite, recorte e cole o código diretamente. Se não se sentir à vontade ao editar o código, você poderá selecionar um recurso na tela, clicar na guia **Propriedades** do editor de código e inserir os valores lá. Os valores inseridos aparecerão no código como se você os tivesse digitado diretamente.

Procedimentos

1 Acesse **Projetar > Modelos de Nuvem** e clique em **Novo a partir de > Tela em branco**.

2 Nomeie o modelo de nuvem como **Wordpress-BP**.

3 Selecione o projeto **WordPress** e clique em **Criar**.

4 Nos recursos à esquerda da página de design de modelo de nuvem, arraste duas máquinas independentes de nuvem até a tela.

As máquinas atuam como servidor de aplicativos WordPress (WebTier) e servidor do database MySQL (DBTier).

- 5 À direita, edite o código YAML da máquina para adicionar nomes, imagens, tipos e tags de restrição:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
```

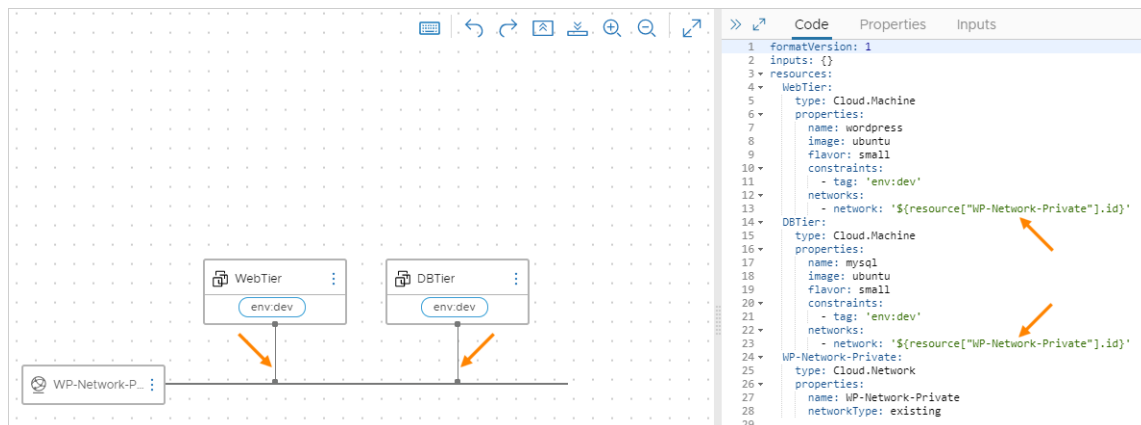
- 6 Arraste uma rede independente de nuvem para a tela e edite seu código:

```
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
```

- 7 Conecte as máquinas à rede:

Na tela, passe o cursor sobre o bloco de rede, clique e segure na bolha onde a linha se une ao bloco, arraste até um bloco de máquina e solte.

Ao criar as linhas de conexão, observe que o código de rede é adicionado automaticamente às máquinas no editor.



8 Adicione o prompt de entrada do usuário.

Em alguns locais, a infraestrutura de exemplo foi configurada para várias opções. Por exemplo:

- Ambientes de zona de nuvem para desenvolvimento, teste e produção
- Mapeamentos de tipo para máquinas pequenas, médias e grandes

É possível definir uma opção específica diretamente no modelo de nuvem, mas uma abordagem melhor é permitir que o usuário selecione a opção no momento da implantação do modelo. A solicitação de entrada de usuário permite criar um modelo que pode ser implantado muitas formas em vez de ter muitos modelos embutidos em código.

- a Crie uma seção `inputs` no código para que os usuários possam selecionar o tamanho da máquina e o ambiente de destino no momento da implantação. Defina os valores selecionáveis.

```
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
```

- b Na seção `resources` do código, adicione o código `${input.input-name}` para solicitar a seleção do usuário:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
```

```
        - network: '${resource["WP-Network-Private"].id}'  
WP-Network-Private:  
  type: Cloud.Network  
  properties:  
    name: WP-Network-Private  
    networkType: existing
```

- 9 Por fim, aprimore o código `WebTier` e `DBTier` usando os exemplos a seguir. O código `WP-Network-Private` não precisa de alterações adicionais.

Observe que os aprimoramentos incluem acesso de login ao servidor do database e scripts de inicialização `cloudConfig` de tempo de implantação.

| Componente | Exemplo |
|-------------------------------|---|
| Entradas adicionais do DBTier | <pre> username: type: string minLength: 4 maxLength: 20 pattern: '[a-z]+' title: Database Username description: Database Username userpassword: type: string pattern: '[a-z0-9A-Z@#]+\$' encrypted: true title: Database Password description: Database Password </pre> |
| Recurso DBTier | <pre> DBTier: type: Cloud.Machine properties: name: mysql image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: #cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/ mysqlld.cnf - service mysql restart - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';" - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';" - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] </pre> |
| Recurso WebTier | <pre> WebTier: type: Cloud.Machine properties: name: wordpress image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true cloudConfig: </pre> |

| Componente | Exemplo |
|------------|--|
| | <pre> #cloud-config repo_update: true repo_upgrade: all packages: - apache2 - php - php-mysql - libapache2-mod-php - mysql-client - gcc - make - autoconf - libc-dev - pkg-config - libmcrypt-dev - php-pear - php-dev runcmd: - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/ latest.tar.gz -C /var/www/html/mywordpresssite --strip-components 1 - i=0; while [\$i -le 10]; do mysql --connect-timeout=3 -h \$ {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break sleep 15; i=\$((i+1)); done - mysql -u root -pmysqlpassword -h \${DBTier.networks[0].address} -e "create database wordpress_blog;" - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/ html/mywordpresssite/wp-config.php - pecl channel-update pecl.php.net - pecl update-channels - pecl install mcrypt - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME', 'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD', 'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '\${DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp- config.php - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini - service apache2 reload </pre> |

Exemplo: Exemplo de código de modelo de nuvem básica concluído

```

formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
  title: Environment
  description: Target Environment
size:
  type: string

```

```

enum:
  - small
  - medium
  - large
description: Size of Nodes
title: Tier Machine Size
username:
  type: string
  minLength: 4
  maxLength: 20
  pattern: '[a-z]+'
  title: Database Username
  description: Database Username
userpassword:
  type: string
  pattern: '[a-z0-9A-Z@#]+$'
  encrypted: true
  title: Database Password
  description: Database Password
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmccrypt-dev
        - php-pear
        - php-dev
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;

```

```

i=$((i+1)); done
    - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
    - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
    - pecl channel-update pecl.php.net
    - pecl update-channels
    - pecl install mcrypt
    - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
${DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
    - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
  networks:
    - network: '${resource["WP-Network-Private"].id}'
      assignPublicIpAddress: true
  remoteAccess:
    authentication: usernamePassword
    username: '${input.username}'
    password: '${input.userpassword}'
  cloudConfig: |
    #cloud-config
    repo_update: true
    repo_upgrade: all
    packages:
      - mysql-server
    runcmd:
      - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
      - service mysql restart
      - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
      - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';"
      - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing

```

Próximo passo

Teste o modelo de nuvem verificando a sintaxe e implementando-o.

Testar um modelo de nuvem básico

Durante o design, muitas vezes você cria um modelo de nuvem começando com o essencial e, em seguida, implantando e testando conforme esse modelo se expande. Este exemplo demonstra alguns dos testes em andamento integrados ao Cloud Assembly.

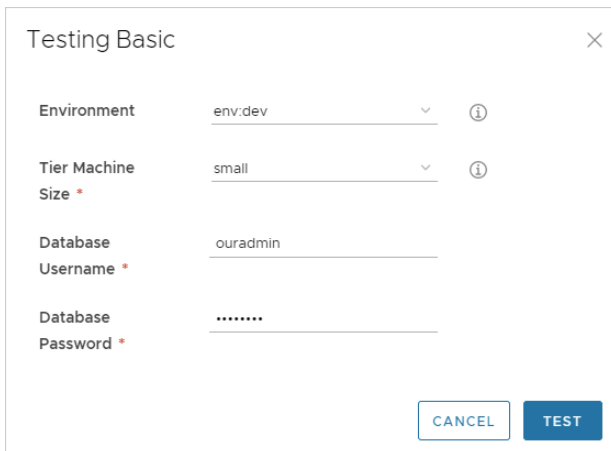
Para garantir que uma implantação funcione da maneira desejada, você pode testar e implantar o modelo de nuvem várias vezes. Gradualmente, você adiciona mais recursos, testa novamente e reimplanta ao longo do caminho.

Pré-requisitos

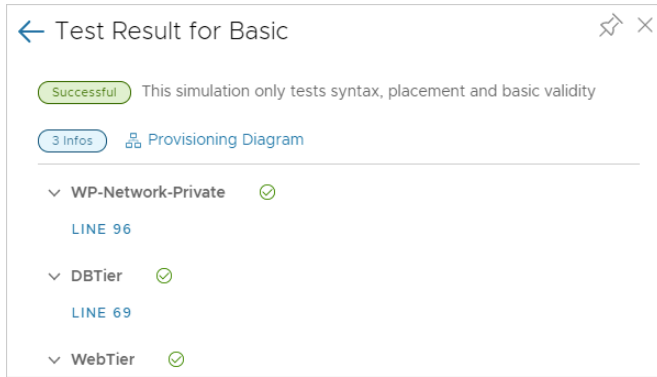
Crie o modelo de nuvem básico. Consulte [Criar um modelo de nuvem básico](#).

Procedimentos

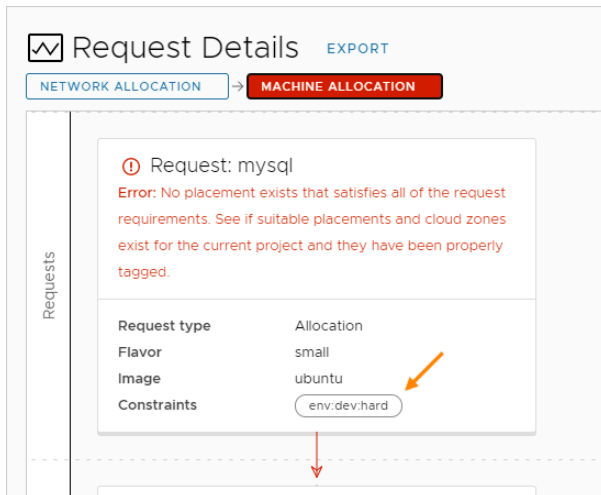
- 1 Clique em **Modelos de Nuvem** e abra o modelo de nuvem WordPress-BP.
O modelo de nuvem básico é exibido na tela de design e no editor de código.
- 2 Para verificar a sintaxe do modelo, o posicionamento e a validade básica, clique em **Testar** no canto inferior esquerdo.
- 3 Insira valores de entrada e clique em **Testar**.



O teste é apenas uma simulação e, na verdade, não implementa máquinas virtuais ou outros recursos.








O teste inclui um link para um **Diagrama de Provisionamento**, no qual você pode inspecionar o fluxo de implantação simulado e ver o que aconteceu. A simulação expõe problemas potenciais, como não ter recursos de recursos definidos que correspondam a restrições fixas no modelo de nuvem. No exemplo de erro a seguir, uma tag de recurso de zona de nuvem `env:dev` não foi encontrada em nenhum lugar na infraestrutura definida.



Uma simulação bem-sucedida não garante que você possa implantar o modelo sem erros.

- 4 Depois que o modelo passar pela simulação, clique em **Implantar** no canto inferior esquerdo.
- 5 Selecione **Criar uma implantação**.
- 6 Especifique **WordPress for OurCo** como nome para a implantação e clique em **Seguinte**.
- 7 Insira valores de entrada e clique em **Implantar**.
- 8 Para verificar se o modelo foi implantado com êxito, procure em **Recursos > Implantações**.

Se uma implantação falhar, clique no nome dela e clique na guia **Histórico** para ver as mensagens que poderão ajudá-lo a solucionar os problemas.

| Timestamp | Status | Resource type | Resource name |
|-------------------|--------------------|---|--------------------|
| Sep 8, 2020, 1... | CREATE_IN_PROGRESS |  Cloud.Machine | WebTier |
| Sep 8, 2020, 1... | CREATE_FINISHED |  Cloud.Machine | DBTier |
| Sep 8, 2020, 1... | CREATE_IN_PROGRESS |  Cloud.Machine | DBTier |
| Sep 8, 2020, 1... | CREATE_FINISHED |  Cloud.Network | WP-Network-Private |
| Sep 8, 2020, 1... | CREATE_IN_PROGRESS |  Cloud.Network | WP-Network-Private |

Algumas entradas de histórico podem ter o link de **Diagrama de Provisionamento** na extrema direita. O diagrama é semelhante ao simulado, em que você inspeciona o fluxograma de pontos de decisão do Cloud Assembly no processo de provisionamento.

Mais fluxogramas estão disponíveis em **Infraestrutura > Atividade > Solicitações**.

- 9 Para verificar se o aplicativo está funcionando, abra o página inicial do WordPress em um navegador.
 - a Aguarde até que os servidores do WordPress sejam totalmente criados e inicializados.
Pode levar 30 minutos ou mais para a inicialização, dependendo do ambiente.
 - b Para localizar o FQDN ou o endereço IP do site, acesse **Recursos > Implantações > Topologia**.
 - c Na tela, clique em WebTier e localize o endereço IP no painel à direita.
 - d Insira o endereço IP como parte da URL completa para a página inicial do WordPress.
Neste exemplo, a URL completa é:
`http://{endereço IP}/mywordpresssite`
ou
`http://{endereço IP}/mywordpresssite/wp-admin/install.php`
- 10 Depois de inspecionar o WordPress em um navegador, se o aplicativo precisar de mais trabalho, faça alterações no modelo e reimplante usando a opção **Atualizar uma implantação existente**.
- 11 Considere a versão do modelo de nuvem. Você poderá reverter para uma versão de trabalho se uma alteração causar falha na implantação.
 - a Na página de design de modelo de nuvem, clique em **Versão**.
 - b Na página Criando Versão, digite **WP-1.0**.
Não insira espaços em nomes de versão.
 - c Clique em **Criar**.

Para revisar ou reverter para uma versão, na página de design, clique na guia **Histórico da Versão**.

- 12 Agora que uma implantação básica é possível, experimente a primeira melhoria no tempo de implantação, aumentando a CPU e a memória nos servidores do aplicativo e do database.

Atualize para um tamanho de nó médio para ambos. Usando o mesmo modelo, selecione **medium** no momento da implantação, reimplante e verifique o aplicativo novamente.

Próximo passo

Expanda o modelo de nuvem em um aplicativo digno de produção, adicionando ainda mais recursos.

Expandir um modelo de nuvem

Depois de criar e testar o modelo do Cloud Assembly básico para o aplicativo de exemplo, você o expande em um aplicativo de várias camadas que pode ser implantado para desenvolvimento, teste e, eventualmente, produção.

Para expandir o modelo de nuvem, adicione os seguintes aprimoramentos.

- Uma opção para servidores de aplicativos de cluster para maior capacidade
- Uma rede voltada para o público e balanceador de carga na frente dos servidores de aplicativo
- Um servidor de backup com armazenamento de arquivos

Pré-requisitos

Crie o modelo de nuvem básico e teste-o. Consulte [Criar um modelo de nuvem básico](#) e [Testar um modelo de nuvem básico](#).

Procedimentos

- 1 Clique em **Modelos de Nuvem** e abra o modelo de nuvem WordPress-BP.

O modelo básico é exibido na tela de design e no editor de código.

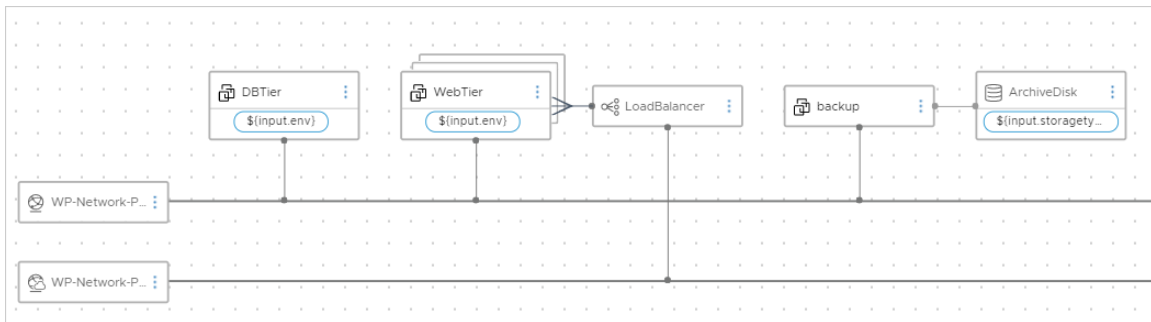
- 2 Faça adições e alterações, usando o exemplo de código e a figura para orientação.

Use a GUI para arrastar novos recursos até a tela, como o balanceador de carga e, em seguida, conclua a configuração no editor de código.

- a Adicione um prompt de entrada do `count` para tornar o servidor de aplicativos do WordPress em um cluster.
- b Adicione um balanceador de carga independente da nuvem.
- c Conecte o balanceador de carga ao cluster do servidor do aplicativo WordPress.
- d Adicione uma máquina de backup independente de nuvem.
- e Conecte a máquina de backup à rede privada/interna.
- f Adicione uma rede pública/externa independente de nuvem.

- g Conecte o balanceador de carga à rede pública.
 - h Adicione um volume de armazenamento independente de nuvem para uso como um disco de arquivamento.
 - i Conecte o disco de arquivamento à máquina de backup.
 - j Adicione um prompt de entrada para a velocidade do disco de arquivamento.
- 3 Implante, teste e faça alterações da mesma maneira que fazia para o modelo de nuvem básico. É possível atualizar implantações existentes ou até mesmo implantar novas instâncias para que possa comparar as implantações.

O objetivo é obter um modelo sólido e repetível que possa ser usado para implantações de produção.



Exemplo: Exemplo de código expandido de modelo de nuvem concluído

```
formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
  username:
    type: string
    minLength: 4
```

```

    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
    encrypted: true
    title: Database Password
    description: Database Password
  count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: WordPress Cluster Size
    description: WordPress Cluster Size (Number of Nodes)
  storagetype:
    type: string
    enum:
      - storage:general
      - storage:fast
    description: Archive Storage Disk Type
    title: Archive Disk Type
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      count: '${input.count}'
      constraints:
        - tag: '${input.env}'
      networks:
        - network: '${resource["WP-Network-Private"].id}'
          assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmccrypt-dev
        - php-pear
        - php-dev

```

```

    runcmd:
      - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
      - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
      - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
      - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
      - pecl channel-update pecl.php.net
      - pecl update-channels
      - pecl install mcrypt
      - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
{DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
      - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
      - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
  remoteAccess:
    authentication: usernamePassword
    username: '${input.username}'
    password: '${input.userpassword}'
  cloudConfig: |
    #cloud-config
    repo_update: true
    repo_upgrade: all
    packages:
      - mysql-server
    runcmd:
      - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
      - service mysql restart
      - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
      - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';"
      - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
LoadBalancer:
  type: Cloud.LoadBalancer
  properties:

```

```

name: myapp-lb
network: '${resource["WP-Network-Public"].id}'
instances:
  - '${WebTier.id}'
routes:
  - protocol: HTTP
    port: '80'
    instanceProtocol: HTTP
    instancePort: '80'
    healthCheckConfiguration:
      protocol: HTTP
      port: '80'
      urlPath: /mywordpresssite/wp-admin/install.php
      intervalSeconds: 6
      timeoutSeconds: 5
      unhealthyThreshold: 2
      healthyThreshold: 2
    internetFacing: true
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
WP-Network-Public:
  type: Cloud.Network
  properties:
    name: WP-Network-Public
    networkType: public
backup:
  type: Cloud.Machine
  properties:
    name: backup
    flavor: '${input.size}'
    image: ubuntu
    networks:
      - network: '${resource["WP-Network-Private"].id}'
    attachedDisks:
      - source: '${resource.ArchiveDisk.id}'
ArchiveDisk:
  type: Cloud.Volume
  properties:
    name: ArchiveDisk
    capacityGb: 5
    constraints:
      - tag: '${input.storagetype}'

```

Próximo passo

Defina a própria infraestrutura e crie seus modelos de nuvem.

Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#) e [Capítulo 6 Como projetar suas implantações do Cloud Assembly](#).

Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation

Este tutorial do vRealize Automation mostra o processo de definição de configurações de modelo de nuvem e infraestrutura de recursos para implantação em um ambiente do VMware Cloud on AWS.

O procedimento requer que o administrador de nuvem já tenha configurado o SDDC do VMware Cloud on AWS da organização, conforme descrito em *Como implantar e gerenciar um Centro de dados definido por software* na [documentação de introdução do VMware Cloud on AWS](#).

Observe a configuração sequencial para entender o processo de configuração do ambiente para VMware Cloud on AWS. Lembre-se de que os valores exibidos são apenas exemplos de caso de uso. Pense no local onde seriam feitas suas próprias substituições ou a extrapolação dos valores de exemplo a fim de atender às suas necessidades de infraestrutura em nuvem e implantação.



Para obter informações relacionadas, veja esse vídeo [Como Configurar o VMware Cloud on AWS para Cloud Assembly](#).

Procedimentos

1 [Configurar um fluxo de trabalho básico do VMware Cloud on AWS no vRealize Automation](#)

Este caso de uso mostra o processo de definição da infraestrutura de recursos e de um modelo de nuvem correspondente para a implantação em um ambiente do VMware Cloud on AWS.

2 [Configurar uma rede isolada no fluxo de trabalho do VMware Cloud on AWS no vRealize Automation](#)

Neste procedimento, você adiciona uma rede isolada para a sua implantação do VMware Cloud on AWS no vRealize Automation.

Configurar um fluxo de trabalho básico do VMware Cloud on AWS no vRealize Automation

Este caso de uso mostra o processo de definição da infraestrutura de recursos e de um modelo de nuvem correspondente para a implantação em um ambiente do VMware Cloud on AWS.

Neste procedimento, você configurará a infraestrutura que oferece suporte à implantação de modelo de nuvem em recursos bi seu ambiente existente do VMware Cloud on AWS.

Pré-requisitos

- Antes de poder criar e configurar uma conta de nuvem do VMware Cloud on AWS no Cloud Assembly, é necessário participar de uma organização em um ambiente do SDDC existente do VMware Cloud on AWS. Para obter informações sobre como configurar o serviço do VMware Cloud on AWS, consulte [documentação do VMware Cloud on AWS](#).

- Para facilitar a conexão necessária entre o SDDC do seu host VMware Cloud on AWS existente no vCenter e uma conta de nuvem do VMware Cloud on AWS no Cloud Assembly, você deve fornecer uma conexão de rede e adicionar regras de firewall usando uma VPN ou uma forma de rede semelhante. Consulte [Preparar seu VMware Cloud on AWS SDDC para se conectar a contas de nuvem do VMware Cloud on AWS no vRealize Automation](#).

Procedimentos

1 [Preparar seu VMware Cloud on AWS SDDC para se conectar a contas de nuvem do VMware Cloud on AWS no vRealize Automation](#)

Ao usar as contas de nuvem do VMware Cloud on AWS no seu ambiente do vRealize Automation, você deve criar uma conexão de rede e configurar regras para permitir a comunicação entre seu SDDC no vCenter e as contas de nuvem do VMware Cloud on AWS no vRealize Automation.

2 [Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra](#)

Nesta etapa, cria-se uma conta de nuvem do VMware Cloud on AWS no vRealize Automation.

3 [Criar uma zona de nuvem para as implantações do VMware Cloud on AWS no vRealize Automation](#)

Nesta etapa, cria-se uma zona de nuvem para especificar um recurso de processamento que o usuário CloudAdmin pode acessar ao trabalhar com o VMware Cloud on AWS no vRealize Automation.

4 [Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation](#)

Nesta etapa, configura-se um perfil de rede e um perfil de armazenamento para especificar os recursos que estão disponíveis para um usuário CloudAdmin do VMware Cloud on AWS no vRealize Automation.

5 [Criar um projeto para dar suporte a implantações do VMware Cloud on AWS no vRealize Automation](#)

Nesta etapa, é definido um projeto do vRealize Automation que pode ser usado para controlar quais recursos estarão disponíveis para as implantações do VMware Cloud on AWS.

6 [Definir um recurso de máquina do vCenter em um design de modelo de nuvem para oferecer suporte à implantação do VMware Cloud on AWS no vRealize Automation](#)

Nesta etapa, você arrasta um recurso de máquina do vCenter até a tela do design e adiciona configurações para uma implantação do VMware Cloud on AWS no vRealize Automation.

Preparar seu VMware Cloud on AWS SDDC para se conectar a contas de nuvem do VMware Cloud on AWS no vRealize Automation

Ao usar as contas de nuvem do VMware Cloud on AWS no seu ambiente do vRealize Automation, você deve criar uma conexão de rede e configurar regras para permitir a comunicação entre seu SDDC no vCenter e as contas de nuvem do VMware Cloud on AWS no vRealize Automation.

Configure as conexões e as regras necessárias para permitir a comunicação do SDDC.

Para facilitar a conexão necessária entre o SDDC do host do VMware Cloud on AWS existente no vCenter e uma conta de nuvem do VMware Cloud on AWS no vRealize Automation, você deve estabelecer uma conexão de rede entre os dois elementos usando uma VPN ou uma rede semelhante.

- 1 Configure uma conexão de VPN por meio da Internet pública ou do AWS Direct Connect.

Consulte informações sobre como configurar a conectividade VPN com o data center local e como configurar o AWS Direct Connect para o VMware Cloud on AWS em *Rede e segurança do VMware Cloud on AWS*, na [Documentação do VMware Cloud on AWS](#).

- 2 Verifique se o FQDN do vCenter Server pode ser resolvido em um endereço IP privado na rede de gerenciamento.

Consulte informações sobre como definir o endereço de resolução do FQDN do vCenter Server em *Rede e segurança do VMware Cloud on AWS*, na [Documentação do VMware Cloud on AWS](#).

- 3 Configure as regras de firewall necessárias.

Você deve configurar as regras de firewall do gateway de gerenciamento no console do VMware Cloud on AWS do SDDC para oferecer suporte à comunicação. As regras devem estar na seção regras de firewall do **Gateway de Gerenciamento**. Crie as regras de firewall usando as opções na guia **Rede e Segurança** do console do SDDC.

- Limite o tráfego de rede até o ESXi para serviços HTTPS (TCP 443) ao endereço IP descoberto do dispositivo/servidor do vRealize Automation ou VIP do balanceador de carga do vRealize Automation.
- Limite o tráfego de rede até o vCenter para os serviços ICMP (todas as portas ICMP), SSO (TCP 7444) e HTTPS (TCP 443) ao endereço IP descoberto do dispositivo/servidor do vRealize Automation ou VIP do balanceador de carga do vRealize Automation.
- Limite o tráfego de rede até o NSX-T Manager para serviços HTTPS (TCP 443) ao endereço IP descoberto do dispositivo/servidor do vRealize Automation ou VIP do balanceador de carga do vRealize Automation.

As regras de firewall necessárias estão resumidas na tabela a seguir.

Tabela 2-2. Resumo das regras de firewall de gateway de gerenciamento necessárias

| Nome | Origem | Destino | Serviço |
|--|--|--|---------------------------|
| vCenter | Bloqueio CIDR do centro de dados local | vCenter | Qualquer (todo o tráfego) |
| Ping do vCenter | Qualquer | vCenter | ICMP (tudo ICMP) |
| NSX Manager | Bloqueio CIDR do centro de dados local | NSX Manager | Qualquer (todo o tráfego) |
| No local para ping do ESXi | Bloqueio CIDR do centro de dados local | Somente gerenciamento do ESXi | ICMP (tudo ICMP) |
| No local para console remoto e provisionamento do ESXi | Bloqueio CIDR do centro de dados local | Somente gerenciamento do ESXi | TCP 902 |
| No local para VM do SDDC | Bloqueio CIDR do centro de dados local | Bloco CIDR de rede lógica SDDC | Qualquer (todo o tráfego) |
| VM do SDDC para no local | Bloco CIDR de rede lógica SDDC | Bloqueio CIDR do centro de dados local | Qualquer (todo o tráfego) |

Para obter informações relacionadas, consulte *Rede e segurança do VMware Cloud on AWS* e *Guia de operações do VMware Cloud on AWS*, na [Documentação do VMware Cloud on AWS](#).

Depois de configurar as regras de acesso e firewall necessárias do gateway, você pode continuar com o processo de criação de uma conta de nuvem do VMware Cloud on AWS. Consulte [Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra](#).

Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra

Nesta etapa, cria-se uma conta de nuvem do VMware Cloud on AWS no vRealize Automation.

Para obter informações relacionadas, consulte a [documentação do VMware Cloud on AWS](#).

Pré-requisitos

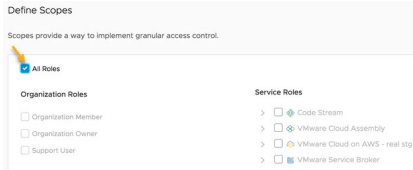
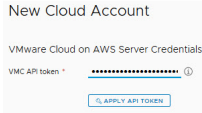
- Esse procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter, e que você tenha ativado o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Para facilitar a conexão necessária entre o SDDC do seu host VMware Cloud on AWS existente no vCenter e uma conta de nuvem do VMware Cloud on AWS no vRealize Automation, você

deve fornecer uma conexão de rede e regras de firewall usando uma VPN ou uma forma de rede semelhante. Consulte [Preparar seu VMware Cloud on AWS SDDC para se conectar a contas de nuvem do VMware Cloud on AWS no vRealize Automation](#). Se estiver usando um proxy de Internet HTTP externo, este deverá ser configurado para IPv4.

- Se você não tiver acesso externo à Internet, configure um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas da Nuvem**.
- 2 Clique em **Adicionar Conta de Nuvem**, selecione VMware Cloud on AWS e digite os valores. Os valores de amostra e as informações de suporte são fornecidos na tabela a seguir.

| Configuração | Valor e instrução de amostra | Descrição |
|---------------------|---|--|
| Token de API do VMC | <ol style="list-style-type: none"> 1 Clique no ícone de ajuda <i>i</i> no final da linha do Token de API do VMC e clique na página Tokens de API na caixa de texto de ajuda para abrir a guia Tokens de API na página Minha Conta da sua empresa. 2 Clique em Gerar Token para exibir as opções Gerar um Novo Token de API. 3 Digite um novo nome de token, por exemplo myinitials_mytoken. 4 Defina o TTL do Token como nunca expirar. Se você criar um token definido para expirar, as operações do VMware Cloud on AWS no vRealize Automation deixarão de funcionar quando o token expirar e apenas continuarão a funcionar quando você atualizar a conta de nuvem com um novo token. 5 Na seção Definir Escopos, selecione Todas as Funções.  6 Clique em Gerar. 7 Na página de token gerada, clique em Copiar e, em seguida, clique em Continuar. 8 Retorne para a página Nova Conta de Nuvem, cole o token copiado na linha Token de API do VMC e clique em Aplicar Token de API.  | <p>É possível criar um novo token ou usar um token existente para a sua organização na página vinculada Tokens de API.</p> <p>Na seção Definir Escopos, as funções mínimas necessárias para o token de API são:</p> <ul style="list-style-type: none"> ■ Funções Organizacionais <ul style="list-style-type: none"> ■ Membro da Organização ■ Proprietário da Organização ■ Funções de Serviço - VMware Cloud on AWS <ul style="list-style-type: none"> ■ Administrador ■ Administrador do NSX Cloud ■ Auditor do NSX Cloud <p>Observação Copie, baixe ou imprima o token gerado. Após sair desta página, não é possível recuperar o token gerado.</p> <p>Aplique o token gerado ou fornecido para se conectar ao ambiente do SDDC disponível na assinatura do VMware Cloud on AWS da sua organização e preencha a lista de nomes do SDDC.</p> <p>Se os serviços do vRealize Automation e do VMware Cloud on AWS estiverem em organizações diferentes, você deverá alternar para a organização do VMware Cloud on AWS e, em seguida, gerar o token.</p> <p>Para obter mais informações sobre tokens de API, consulte Gerar tokens de API.</p> |
| Nome do SDDC | <p>Para esse exemplo, selecione Datacenter:Datacenter-abz.</p> <p>O nome do SDDC válido preenche automaticamente as entradas de FQDN do vCenter e do NSX-T. Se um proxy de nuvem já tiver sido implantado no SDDC, o valor do proxy de nuvem também será preenchido automaticamente.</p> | <p>Selecione na lista de SDDCs disponíveis da sua assinatura do VMware Cloud on AWS. A lista de SDDCs é baseada no token de API do VMware Cloud on AWS.</p> <p>Os SDDCs do NSX-V não são compatíveis com o vRealize Automation e não aparecem na lista de SDDCs disponíveis.</p> |

| Configuração | Valor e instrução de amostra | Descrição |
|--|---|---|
| Endereço IP/FQDN do vCenter | O endereço é preenchido automaticamente com base na seleção do SDDC. | <p>Digite o endereço IP ou FQDN do vCenter Server no SDDC especificado.</p> <p>O endereço IP padrão é o endereço IP privado. Com base no tipo de conectividade de rede usado para acessar seu SDDC, o endereço padrão pode ser diferente do endereço IP do servidor NSX Manager no SDDC especificado.</p> |
| Endereço IP/FQDN do Gerenciador do NSX | O endereço é preenchido automaticamente com base na seleção do SDDC. | <p>Especifica o endereço IP ou FQDN do Gerenciador do NSX no SDDC especificado.</p> <p>O endereço IP padrão é o endereço IP privado. Com base no tipo de conectividade de rede usado para acessar seu SDDC, o endereço padrão pode ser diferente do endereço IP do servidor NSX Manager no SDDC especificado.</p> <p>VMware Cloud on AWS suporta contas de nuvem NSX-T.</p> |
| Nome de usuário e senha do vCenter | O nome de usuário é preenchido automaticamente como cloudadmin@vmc.local. | <p>Digite seu nome de usuário do vCenter para o SDDC especificado, se ele for diferente do padrão.</p> <p>O usuário especificado requer credenciais de CloudAdmin. O usuário não precisa de credenciais do CloudGlobalAdmin.</p> <p>Digite a senha do usuário.</p> |
| Validar | <p>Clique em Validar.</p> <p>Se você receber um <code>Error updating endpoint <Nome>: Endpoint already exists</code>, uma conta de nuvem já foi associada a esse SDDC.</p> | A ação de validação confirma os direitos de acesso ao vCenter especificado e verifica se o vCenter está em execução. |
| Nome e Descrição | <p>Digite OurCo-VMC para o nome da conta de nuvem.</p> <p>Digite Sample deployment for VMC para a descrição da conta de nuvem.</p> | |
| Permitir o provisionamento para esses centros de dados | Essas informações são somente para leitura. | Lista os centros de dados disponíveis no ambiente do SDDC especificado do VMware Cloud on AWS. |
| Criar uma zona de nuvem | Desmarque a caixa de seleção. Neste exemplo, será criada uma zona de nuvem mais tarde no fluxo de trabalho. | Consulte Saiba mais sobre as zonas de nuvem do Cloud Assembly . |
| Tags de capacidade | Deixe esse campo vazio. Esse fluxo de trabalho não usa tags de capacidade. | <p>Use tags de acordo com a estratégia de marcação da sua organização. Consulte Como usar tags para gerenciar recursos e implantações do Cloud Assembly e Criação de uma estratégia de marcação.</p> |

Assim como acontece com as VMs implantadas no vSphere, você pode configurar tags de máquina para que uma VM seja implantada no VMware Cloud on AWS. Você também pode atualizar a tag da máquina após a implantação inicial. Essas tags de máquina permitem que o vRealize Automation atribua dinamicamente uma VM a um grupo de segurança apropriado do NSX-T durante a implantação. Para obter informações relacionadas, consulte [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#).

3 Clique em **Adicionar**.

Resultados

Recursos como máquinas e volumes são coletados por dados do centro de dados SDDC do VMware Cloud on AWS e listados na seção **Recursos** da guia vRealize Automation **Infraestrutura**.

Próximo passo

[Criar uma zona de nuvem para as implantações do VMware Cloud on AWS no vRealize Automation](#).

Criar uma zona de nuvem para as implantações do VMware Cloud on AWS no vRealize Automation

Nesta etapa, cria-se uma zona de nuvem para especificar um recurso de processamento que o usuário CloudAdmin pode acessar ao trabalhar com o VMware Cloud on AWS no vRealize Automation.

No VMware Cloud on AWS, as duas principais credenciais de administrador são CloudGlobalAdmin e CloudAdmin. O Cloud Assembly foi projetado para oferecer suporte ao usuário CloudAdmin. Implantar em recursos que estão disponíveis a um usuário CloudAdmin do VMware Cloud on AWS. Não implantar em recursos que exijam credenciais de CloudGlobalAdmin do VMware Cloud on AWS.

As zonas de nuvem identificam os recursos de processamento nos quais um modelo de nuvem do projeto implanta máquinas, redes e armazenamento. Consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Conclua o procedimento [Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra](#).
- Este procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

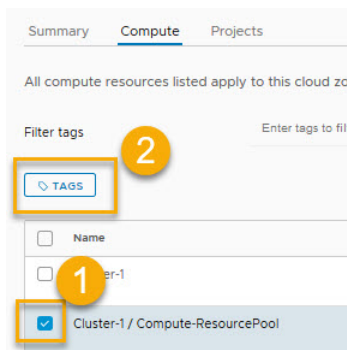
Procedimentos

- 1 Selecione **Infraestrutura > Configurar > Zonas de Nuvem**.
- 2 Clique em **Nova Zona de Nuvem** e digite os valores para o ambiente do VMware Cloud on AWS.

| Configuração | Valor de amostra |
|-----------------------|--|
| Conta/região | OurCo-VMC/Datacenter:Datacenter-abz Esta é a conta e a região de nuvem associadas que você definiu na etapa anterior, Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra . |
| Nome | VMC_cloud_zone-1 |
| Descrição | Somente recursos do VMware Cloud on AWS |
| Política de colocação | Padrão |
| Tags de capacidade | Deixe esse campo vazio. Esse fluxo de trabalho não usa tags de capacidade. |

- 3 Clique na guia **Processamento**.
- 4 Conforme mostrado abaixo na área 1, localize e selecione um recurso de processamento que esteja disponível para o usuário do CloudAdmin. Neste exemplo, use o recurso chamado Cluster 1/ Compute-ResourcePool.

Cluster 1/ Compute-ResourcePool é o recurso de processamento padrão para o VMware Cloud on AWS.



- 5 Conforme mostrado acima na área 2, adicione o nome da tag `vmc_placements_abz`.

Tags

1 object(s) selected

Add tags

vmc_placements_abz X

Enter a new tag

Remove tags

no tags ⓘ

- 6 Filtre os recursos de processamento que são usados nesta zona de nuvem digitando `vmc_placements_abz` na seção **Filtrar tags**.
- 7 Clique em **Salvar**.

| <input type="checkbox"/> | Name | Account / region | Type | Tags |
|-------------------------------------|----------------------------------|----------------------------|--------------|--------------------|
| <input type="checkbox"/> | Cluster-1 | | Cluster | |
| <input checked="" type="checkbox"/> | Cluster-1 / Compute-ResourcePool | OurCo-VMC / SDDC_test1_abz | ResourcePool | vmc_placements_abz |
| <input type="checkbox"/> | Cluster-1 / Mgmt-ResourcePool | | ResourcePool | |

1 ⓘ

Neste exemplo, somente o recurso de processamento chamado `Cluster 1 / Compute-ResourcePool` está disponível para o usuário `CloudAdmin`.

Próximo passo

[Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation.](#)

Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation

Nesta etapa, configura-se um perfil de rede e um perfil de armazenamento para especificar os recursos que estão disponíveis para um usuário `CloudAdmin` do VMware Cloud on AWS no vRealize Automation.

Embora uma imagem e um valor de tipo também sejam necessários, não há nada exclusivo sobre eles em relação às credenciais de usuário do VMware Cloud on AWS. Neste exemplo, você usará um valor de tipo `small` e um valor de imagem `ubuntu-16` para a definição do modelo de nuvem.

Para obter informações gerais sobre mapeamentos e perfis, consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Crie uma zona de nuvem. Consulte [Criar uma zona de nuvem para as implantações do VMware Cloud on AWS no vRealize Automation](#).

- Este procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

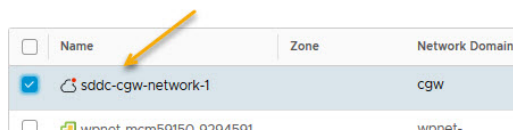
Procedimentos

- 1 Defina um perfil de rede para as implantações do VMware Cloud on AWS.
 - a Selecione **Infraestrutura > Configurar > Perfis de Rede** e clique em **Novo Perfil de Rede**.

| Configuração | Valor de amostra |
|--------------|--|
| Conta/região | OurCo-VMC/Datacenter:Datacenter-abz |
| | Observação Selecione a conta de nuvem do VMware Cloud on AWS e seu centro de dados SDDC correspondente, criado em Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra . |
| Nome | vmc-network1 |
| Descrição | Contém redes que podem ser acessadas por administradores de modelo de nuvem que tenham credenciais de CloudAdmin do VMware Cloud on AWS. |

- b Clique na guia **Rede** e clique em **Adicionar Rede**.
- c Selecione uma rede que um usuário com credenciais do CloudAdmin do VMware Cloud on AWS pode implantar, por exemplo `sddc-cgw-network-1`.

Add Network



| <input type="checkbox"/> | Name | Zone | Network Domain |
|-------------------------------------|---------------------------|------|----------------|
| <input checked="" type="checkbox"/> | sddc-cgw-network-1 | | cgw |
| <input type="checkbox"/> | vmc-net-00000000-00000000 | | vmnet |

- 2 Salve o perfil de rede.

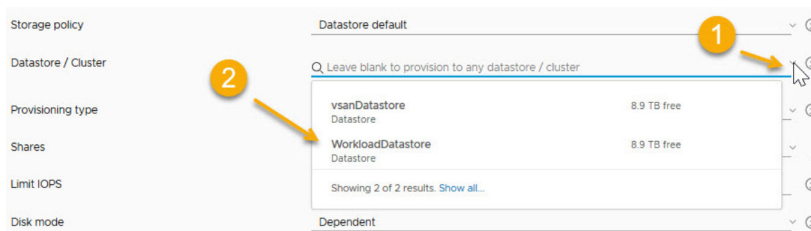
3 Defina um perfil de armazenamento para as implantações do VMware Cloud on AWS.

Configure um perfil de armazenamento que tenha como alvo um repositório de dados/cluster que seja acessível ao usuário CloudAdmin.

- a Selecione **Infraestrutura > Configurar > Perfis de Armazenamento** e clique em **Novo Perfil de Armazenamento**.

| Configuração | Valor de amostra |
|--------------|---|
| Conta/região | OurCo-VMC/Datacenter:Datacenter-abz Selecione a conta de nuvem do VMware Cloud on AWS e seu centro de dados SDDC correspondente, criado em Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra . |
| Nome | vmc-storage1 |
| Descrição | Contém o cluster de repositório de dados que pode ser implantado por administradores de modelo de nuvem que têm credenciais de CloudAdmin do VMware Cloud on AWS. |

- b No menu suspenso **Repositório de Dados/Cluster**, selecione o repositório de dados **WorkloadDatastore**.



Para VMware Cloud on AWS no Cloud Assembly, a política de armazenamento deve usar o repositório de dados **WorkloadDatastore** para oferecer suporte à implantação do VMware Cloud on AWS.

4 Salve o perfil de armazenamento.

Próximo passo

[Criar um projeto para dar suporte a implantações do VMware Cloud on AWS no vRealize Automation.](#)

Criar um projeto para dar suporte a implantações do VMware Cloud on AWS no vRealize Automation

Nesta etapa, é definido um projeto do vRealize Automation que pode ser usado para controlar quais recursos estarão disponíveis para as implantações do VMware Cloud on AWS.

Para obter informações sobre projetos, consulte [Como funcionam os projetos do Cloud Assembly no momento da implantação](#).

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Conclua o procedimento [Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation](#).
- Este procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Administração > Projetos**.
- 2 Clique em **Novo Projeto** e digite o nome do projeto `VMC_proj-1_abz`.
- 3 Clique em **Usuários** e clique em **Adicionar Usuários**.

Os usuários precisam de credenciais CloudAdmin para a assinatura do VMware Cloud on AWS de sua organização.

- `chris.gray@ourco.com`, administrador
- `kerry.white@ourco.com`, membro

- 4 Clique em **Provisionamento** e depois em **Adicionar Zona de Nuvem**.
- 5 Adicione a zona de nuvem configurada na etapa anterior.

| Configuração | Valor de amostra |
|-------------------------------|--|
| Zona de nuvem | VMC_cloud_zone-1 Esta zona de nuvem foi criada etapa anterior, Criar uma zona de nuvem para as implantações do VMware Cloud on AWS no vRealize Automation . |
| Prioridade de provisionamento | 1 |
| Limite de instâncias | 3 |

- 6 Neste exemplo, ignore as outras opções.

Próximo passo

Crie um modelo de nuvem para implantar no seu ambiente do VMware Cloud on AWS. Consulte [Definir um recurso de máquina do vCenter em um design de modelo de nuvem para oferecer suporte à implantação do VMware Cloud on AWS no vRealize Automation](#).

Definir um recurso de máquina do vCenter em um design de modelo de nuvem para oferecer suporte à implantação do VMware Cloud on AWS no vRealize Automation

Nesta etapa, você arrasta um recurso de máquina do vCenter até a tela do design e adiciona configurações para uma implantação do VMware Cloud on AWS no vRealize Automation.

Crie um design de modelo de nuvem que seja possível implantar nos recursos disponíveis do VMware Cloud on AWS.

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Este procedimento pressupõe que você tenha credenciais de designer de modelos de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Este procedimento pressupõe que você tenha credenciais do VMware Cloud on AWS CloudAdmin para o SDDC de destino no vCenter (Datacenter:Datacenter-abz). Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Configure a infraestrutura de recursos e o projeto conforme descrito nas seções anteriores.

Procedimentos

- 1 Clique na guia **Design** e depois em **Novo**.

| Configuração | Valor de amostra |
|--------------|---|
| Nome | vmc-bp_abz |
| Descrição | 1 |
| Projeto | VMC_proj-1_abz Este é o projeto criado anteriormente, que oferece suporte à zona de nuvem também criada anteriormente. O projeto agora está associado à zona de nuvem, que, por sua vez, está associada à conta/região de nuvem do VMware Cloud on AWS criada anteriormente. |

- 2 Deslize um recurso de máquina do vSphere até a tela.
- 3 Edite o seguinte código de recurso do modelo de nuvem (negrito) no recurso de máquina.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
```

```
image: ubuntu-1604
cpuCount: 1
totalMemoryMB: 1024
folderName: Workloads
```

A `image` pode ser qualquer valor apropriado para suas necessidades de implantação.

É necessário adicionar a instrução `folderName: Workloads` ao código do design de modelo de nuvem para oferecer suporte à implantação do VMware Cloud on AWS. A configuração `folderName: Workloads` oferece suporte às credenciais de `CloudAdmin` no ambiente do SDDC do VMware Cloud on AWS e é necessária.

Observação: embora a configuração `folderName: Workloads` mostrada no exemplo de código acima seja necessária, você pode adicioná-la diretamente no código do modelo de nuvem conforme mostrado acima ou pode adicioná-la à zona de nuvem ou projeto associado. Se a configuração for especificada em mais de um desses três lugares, a precedência será a seguinte:

- A configuração do projeto substitui a configuração do modelo de nuvem e a configuração da zona de nuvem.
- A configuração do modelo de nuvem substitui a configuração da zona de nuvem.

Observação: pode-se, opcionalmente, substituir as configurações `cpuCount` e `totalMemoryMB` por uma entrada `flavor` (de dimensionamento), como mostrado abaixo:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu-1604
      flavor: small
      folderName: Workloads
```

Se a zona de nuvem tiver o valor da pasta definido como **Workloads**, não será necessário definir a propriedade `folderName` no modelo de nuvem, a menos que você queira substituir o valor da pasta da zona de nuvem.

Próximo passo

Expanda nesse fluxo de trabalho básico do VMware Cloud on AWS adicionando o isolamento de rede. Consulte [Configurar uma rede isolada no fluxo de trabalho do VMware Cloud on AWS no vRealize Automation](#).

Configurar uma rede isolada no fluxo de trabalho do VMware Cloud on AWS no vRealize Automation

Neste procedimento, você adiciona uma rede isolada para a sua implantação do VMware Cloud on AWS no vRealize Automation.

Quando você define a conta de nuvem do VMware Cloud on AWS, as configurações do NSX-T definidas no serviço do VMware Cloud on AWS são disponibilizadas. Para obter informações sobre como definir as configurações do NSX-T no serviço do VMware Cloud on AWS, consulte a [documentação do produto](#) VMware Cloud on AWS.

O vRealize Automation oferece suporte ao uso do VMware Cloud on AWS com NSX-T. Ele não oferece suporte ao uso do VMware Cloud on AWS com NSX-V.

O vRealize Automation oferece suporte ao isolamento de rede para as implantações do VMware Cloud on AWS. Ele não oferece suporte a outros métodos de rede para VMware Cloud on AWS.

Essa extensão do fluxo de trabalho básico do VMware Cloud on AWS descreve os seguintes métodos de criação de uma rede isolada para uso no modelo de nuvem:

- Configure o isolamento baseado em rede sob demanda.
- Configure o isolamento baseado em grupo de segurança sob demanda.

Pré-requisitos

Esse procedimento expande o fluxo de trabalho básico do VMware Cloud on AWS. Ele usa a mesma conta e região de nuvem, zona de nuvem, projeto e perfil de rede configurados no fluxo de trabalho do [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#).

Procedimentos

1 Definir uma rede isolada para uma implantação do VMware Cloud on AWS no vRealize Automation

É possível configurar o isolamento de rede para uma implantação do VMware Cloud on AWS usando um dos seguintes procedimentos:

2 Definir um componente de rede em um modelo de nuvem para oferecer suporte ao isolamento de rede do VMware Cloud on AWS no vRealize Automation

Nesta etapa, você arrasta um componente de máquina de rede até uma tela do modelo de nuvem do vRealize Automation e adiciona configurações para uma implantação de rede isolada ao ambiente de destino do VMware Cloud on AWS.

Definir uma rede isolada para uma implantação do VMware Cloud on AWS no vRealize Automation

É possível configurar o isolamento de rede para uma implantação do VMware Cloud on AWS usando um dos seguintes procedimentos:

- [Configurar o isolamento baseado em rede sob demanda no vRealize Automation](#)
- [Configurar o isolamento baseado em grupo de segurança sob demanda no vRealize Automation](#)

Configurar o isolamento baseado em rede sob demanda no vRealize Automation

É possível configurar o isolamento de rede para suas necessidades de implantação do VMware Cloud on AWS especificando e usando as configurações de rede sob demanda em um perfil de rede.

É possível especificar uma rede isolada usando um grupo de segurança ou usando as configurações de rede sob demanda. Neste exemplo, configura-se o isolamento de rede especificando as configurações de rede sob demanda no perfil de rede. Mais tarde, a rede é acessada em um modelo de nuvem e usa o modelo de nuvem em uma implantação do VMware Cloud on AWS.

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Conclua o fluxo de trabalho de [Configurar um fluxo de trabalho básico do VMware Cloud on AWS no vRealize Automation](#).
- Revise [Configurar uma rede isolada no fluxo de trabalho do VMware Cloud on AWS no vRealize Automation](#).
- Este procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

Procedimentos

- 1 Abra o perfil de rede usado no fluxo de trabalho básico do VMware Cloud on AWS, por exemplo `vmc-network1`. Consulte [Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation](#).
- 2 Não é necessário selecionar na guia **Redes**.
- 3 Clique na guia **Políticas de Rede**.
- 4 Selecione a opção **Criar uma rede sob demanda** e selecione o domínio de rede padrão `cgw`. Especifique um CIDR e um tamanho de sub-rede apropriados.
- 5 Clique em **Salvar**.

Quando você usa esse perfil de rede, as máquinas são implantadas em uma rede no domínio de rede padrão. A rede é isolada de outras redes usando o acesso à rede privada ou de saída.

Próximo passo

Configure um componente de rede no seu modelo de nuvem. Consulte [Definir um componente de rede em um modelo de nuvem para oferecer suporte ao isolamento de rede do VMware Cloud on AWS no vRealize Automation](#)

Configurar o isolamento baseado em grupo de segurança sob demanda no vRealize Automation

É possível configurar o isolamento de rede para suas necessidades de implantação do VMware Cloud on AWS especificando e usando um grupo de segurança sob demanda em um perfil de rede.

É possível especificar uma rede isolada usando um grupo de segurança ou usando as configurações de rede sob demanda. Neste exemplo, configura-se o isolamento de rede especificando um grupo de segurança sob demanda no perfil de rede. Mais tarde, especifica-se a rede em um modelo de nuvem e usa-se o modelo de nuvem em uma implantação do VMware Cloud on AWS.

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

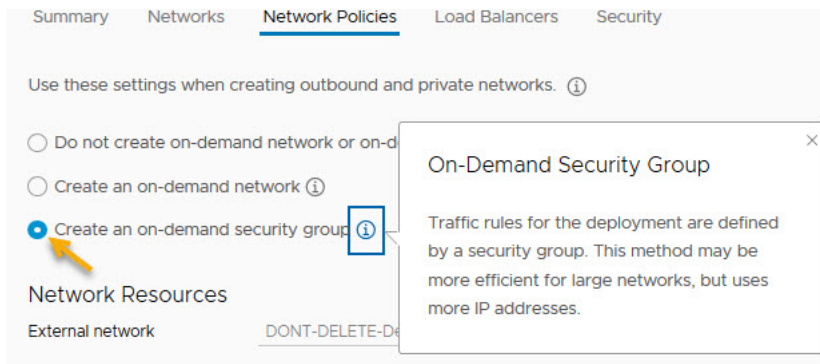
Pré-requisitos

- Conclua o fluxo de trabalho de [Configurar um fluxo de trabalho básico do VMware Cloud on AWS no vRealize Automation](#).
- Revise [Configurar uma rede isolada no fluxo de trabalho do VMware Cloud on AWS no vRealize Automation](#).
- Este procedimento pressupõe que você tenha as credenciais de administrador necessárias, incluindo credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Esse procedimento pressupõe que você tenha a função de usuário administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

Procedimentos

- 1 Abra o perfil de rede usado no fluxo de trabalho básico do VMware Cloud on AWS, por exemplo `vmc-network1`. Consulte [Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation](#).
- 2 Selecione a rede existente usada no fluxo de trabalho básico do VMware Cloud on AWS, por exemplo `sddc-cgw-network-1`. Consulte [Configurar perfis de rede e armazenamento para as implantações do VMware Cloud on AWS no vRealize Automation](#).
- 3 Clique na guia **Políticas de Rede**.

4 Selecione a opção **Criar um grupo de segurança sob demanda**.



5 Clique em **Salvar**.

Quando você usa esse perfil de rede, as máquinas são implantadas na rede selecionada e são isoladas por uma nova política de grupo de segurança. A nova política de segurança permite acesso à rede privada ou de saída.

Próximo passo

Configure um componente de rede no seu modelo de nuvem. Consulte [Definir um componente de rede em um modelo de nuvem para oferecer suporte ao isolamento de rede do VMware Cloud on AWS no vRealize Automation](#)

Definir um componente de rede em um modelo de nuvem para oferecer suporte ao isolamento de rede do VMware Cloud on AWS no vRealize Automation

Nesta etapa, você arrasta um componente de máquina de rede até uma tela do modelo de nuvem do vRealize Automation e adiciona configurações para uma implantação de rede isolada ao ambiente de destino do VMware Cloud on AWS.

Adicione o isolamento de rede ao modelo de nuvem criado anteriormente. O modelo de nuvem já está associado a um projeto e a uma zona de nuvem que oferecem suporte à implantação para o ambiente do VMware Cloud on AWS, bem como ao perfil de rede e à rede configurados para o isolamento.

A menos que seja indicado em contrário, os valores de etapa digitados neste procedimento são apenas para este exemplo de fluxo de trabalho.

Pré-requisitos

- Conclua o procedimento [Configurar o isolamento baseado em grupo de segurança sob demanda no vRealize Automation](#) ou [Configurar o isolamento baseado em rede sob demanda no vRealize Automation](#).
- Este procedimento pressupõe que você tenha credenciais de designer de modelos de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

- Este procedimento pressupõe que você tenha as credenciais de CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).

Procedimentos

- 1 Abra o modelo de nuvem criado no fluxo de trabalho anterior. Consulte [Definir um recurso de máquina do vCenter em um design de modelo de nuvem para oferecer suporte à implantação do VMware Cloud on AWS no vRealize Automation](#).
- 2 Nos componentes à esquerda da página do design de modelo de nuvem, arraste um componente de rede até a tela.
- 3 Edite o código YAML do componente de rede para especificar um tipo de rede de `private` ou `outbound`, conforme mostrado em negrito.

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: private
```

OU

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: outbound
```

Próximo passo

Você está preparado para implantar ou fechar o modelo de nuvem.

Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation

Você pode usar um provedor de IPAM externo para gerenciar atribuições de endereço IP para suas implantações de modelo de nuvem. Este tutorial descreve como configurar a integração de IPAM externa no vRealize Automation usando o Infoblox como o provedor de IPAM externo.

Neste procedimento, você usa um pacote de provedor de IPAM existente, neste caso, um pacote Infoblox e um ambiente em execução existente para compilar um ponto de integração de IPAM específico de provedor. Você configura uma rede existente e cria um perfil de rede para oferecer suporte à alocação de endereços IP do provedor de IPAM externo. Por fim, você cria um modelo de nuvem que corresponde à rede e ao perfil de rede e implanta máquinas em rede usando os valores de IP obtidos do provedor de IPAM externo.

Estão incluídas como referência informações sobre como obter e configurar o pacote de provedor de IPAM e como configurar um ambiente em execução que acessa um proxy de extensibilidade de nuvem para oferecer suporte à integração do provedor IPAM.

Os valores exibidos neste fluxo de trabalho de amostra são valores de exemplo. Você não poderá usá-los literalmente em seu ambiente. Pense no local onde seriam feitas suas próprias substituições para atender às necessidades da sua organização.



Para fazer referência a um cenário do vRealize Automation semelhante, que ilustre um fluxo de trabalho de integração do IPAM do Infoblox na forma de vídeo, consulte [Integração do Plug-in do IPAM do Infoblox com o vRealize Automation/vRealize Automation Cloud](#).

Procedimentos

1 Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation

Para poder baixar e implantar o pacote do provedor Infoblox (`infoblox.zip`) para integração com o vRealize Automation no site do Infoblox ou no VMware Marketplace, você deve adicionar os atributos de extensibilidade necessários no Infoblox.

2 Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation

Antes de poder definir um ponto de integração de IPAM externo no vRealize Automation, você precisará de um pacote de provedor de IPAM configurado.

3 Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation

Antes de poder definir um ponto de integração de IPAM externo no vRealize Automation, você precisa criar ou acessar um ambiente de execução existente para servir como intermediário entre o provedor de IPAM e o vRealize Automation. Normalmente, o ambiente de execução é uma conta de nuvem da Amazon Web Services ou do Microsoft Azure ou um ponto de integração local de extensibilidade com base em ações que está associado a um proxy de extensibilidade de nuvem.

4 Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation

O vRealize Automation oferece suporte para a integração com provedores de IPAM externos. Este exemplo usa a Infoblox como provedor de IPAM externo.

5 Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente no vRealize Automation

Você pode definir uma rede existente para usar os valores de endereço IP obtidos e gerenciados por um provedor de IPAM externo, em vez de internamente do vRealize Automation.

6 Definir e implantar um modelo de nuvem que usa uma atribuição de intervalo de provedor de IPAM externo no vRealize Automation

Você pode definir um modelo de nuvem para obter e gerenciar atribuições de endereços IP do seu provedor de IPAM externo. Este exemplo usa a Infoblox como provedor de IPAM externo.

7 Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation

Você pode usar propriedades específicas do Infoblox para projetos do vRealize Automation que contenham integrações de IPAM externas para o Infoblox.

8 Controlar a coleta de dados de rede usando filtros Infoblox no vRealize Automation

Para o Infoblox, você pode limitar o número de redes com dados coletados a apenas as redes necessárias para as operações do vRealize Automation. Isso reduz a quantidade de dados transferidos e melhora o desempenho do sistema.

Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation

Para poder baixar e implantar o pacote do provedor Infoblox (`infoblox.zip`) para integração com o vRealize Automation no site do Infoblox ou no VMware Marketplace, você deve adicionar os atributos de extensibilidade necessários no Infoblox.

Este procedimento será aplicável se você estiver criando um ponto de integração de IPAM externo para a integração do Infoblox com o Cloud Assembly.

Antes de poder usar o download de `infoblox.zip`, você deve fazer login na sua conta Infoblox, usando as credenciais de administrador da conta da organização, e pré-criar os seguintes atributos extensíveis do Infoblox:

- VMware NIC index
- VMware resource ID

Pré-requisitos

- Verifique se você tem uma conta com o [Infoblox](#) e se tem as credenciais de acesso corretas para a conta Infoblox da sua organização.
- Confirme se a versão da Infoblox WAPI é compatível. A integração de IPAM com o Infoblox depende da Infoblox WAPI versão v2.7. Todos os dispositivos Infoblox que oferecem suporte à WAPI v2.7 são compatíveis.
- Reveja [Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation](#).

Procedimentos

- 1 Faça login na sua conta Infoblox usando credenciais de administrador.

Estas são as mesmas credenciais de nome de usuário e senha de administrador que você especifica ao criar um ponto de integração de IPAM externo no Cloud Assembly usando a sequência de menu **Infraestrutura > Conexões > Integrações > .**

- 2 Use o procedimento descrito na documentação do Infoblox para criar os seguintes atributos extensíveis necessários no seu aplicativo Infoblox.

- VMware NIC index - digite Inteiro
- VMware resource ID - digite Cadeia de Caracteres

O procedimento está descrito na seção sobre como *adicionar atributos extensíveis* do tópico da documentação do Infoblox [sobre atributos extensíveis](#). Consulte também a seção sobre como [gerenciar atributos extensíveis](#).

Próximo passo

Depois de adicionar os atributos necessários, você poderá retomar o processo de download e implantação do pacote Infoblox, conforme descrito em [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation

Antes de poder definir um ponto de integração de IPAM externo no vRealize Automation, você precisará de um pacote de provedor de IPAM configurado.

Você pode baixar um pacote de integração específico do provedor no site do seu provedor de IPAM ou no [VMware Marketplace](#).

Observação Este exemplo usa o pacote Infoblox fornecido pela VMware `Infoblox.zip`, que está disponível para download no [VMware Marketplace](#), da seguinte maneira:

- **Plug-in Infoblox versão 1.4** - Compatível com a versão vRealize Automation 8.3 - 8.7 e fornecendo todas as funcionalidades das versões anteriores. Com essa versão, você pode usar o mesmo nome de host com um sufixo DNS diferente para as duas NICs. Consulte as notas de versão do plug-in para obter detalhes adicionais.
- **Plug-in Infoblox versão 1.3** - compatível com o vRealize Automation 8.3.x e fornece filtros adicionais de coleta de dados de rede. Consulte [Controlar a coleta de dados de rede usando filtros Infoblox no vRealize Automation](#). Se você estiver usando o vRealize Automation 8.3.x, poderá, em vez disso, usar o plug-in Infoblox 1.4 para aproveitar os recursos adicionais.

O **plug-in Infoblox v1.3** pode ser usado com o vRealize Automation 8.1 ou 8.2, mas somente em situações e com cautela, conforme descrito no artigo da base de dados de conhecimento [Compatibilidade do Infoblox 1.3 com o vRealize Automation 8.x \(82142\)](#).

- **Plug-in vRA Cloud Infoblox versão 1.2** - compatível com o vRealize Automation 8.1.x e 8.2.x
- **Plug-in vRA Cloud Infoblox versão 1.1** - compatível com o vRealize Automation 8.1.x
- **Plug-in vRA Cloud Infoblox versão 1.0** - compatível com o vRealize Automation 8.0.1.x com ou sem conexão com a Internet com a rede global.
- **Plug-in vRA Cloud Infoblox versão 0.4** - compatível com o vRealize Automation 8.0.0.x e o 8.0.1.x quando há uma conexão com a Internet com a rede global.

A integração de IPAM com o Infoblox depende da Infoblox WAPI versão v2.7. Todos os dispositivos Infoblox que oferecem suporte à WAPI v2.7 são compatíveis.

Para obter informações sobre como criar um pacote de integração de IPAM para outros provedores de IPAM, se um ainda não existir no [VMware Marketplace](#), consulte [Como usar o SDK de IPAM para criar um pacote de integração de IPAM externo específico do provedor para o vRealize Automation](#).

O pacote de provedor de IPAM contém scripts que são empacotados com metadados e outras configurações. Os scripts contêm o código-fonte usado para as operações que o vRealize Automation realiza em coordenação com o provedor de IPAM externo. As operações de exemplo incluem `Allocate an IP address for a virtual machine`, `Fetch a list of IP ranges from the provider` e `Update the MAC address of a host record in the provider`.

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o [Infoblox](#) ou o [Bluecat](#), e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM.
- Se você estiver usando o Infoblox como seu provedor de IPAM externo, certifique-se de ter adicionado os atributos extensíveis necessários à sua conta do Infoblox antes de continuar. Consulte [Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation](#).

Observação Existe um problema de cadeia de certificados em relação a como o elemento Python no plug-in Infoblox lida com handshakes SSL. Para obter informações sobre o problema e suas ações necessárias para resolver o problema, consulte o Artigo da Base de Conhecimento [Plug-in Infoblox do vRA Cloud lança um erro de cadeia de certificados durante o processo de autenticação \(88057\)](#).

Procedimentos

- 1 Navegue até a página de download correta do plug-in Infoblox. Consulte acima para obter links para uma versão específica do plug-in Infoblox.

Veja acima as opções do plug-in Infoblox que estão disponíveis no [VMware Marketplace](#).

- 2 Faça login e baixe o pacote de plug-ins.
- 3 Se ainda não tiver feito isso, adicione os atributos extensíveis necessários no Infoblox. Consulte [Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation](#).

Resultados

O pacote agora está disponível para você implantar usando a sequência de menu **Integrações > Adicionar Integração > IPAM > Gerenciar Provedores > Importar pacote**, conforme descrito em [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).

Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation

Antes de poder definir um ponto de integração de IPAM externo no vRealize Automation, você precisa criar ou acessar um ambiente de execução existente para servir como intermediário entre o provedor de IPAM e o vRealize Automation. Normalmente, o ambiente de execução é uma conta de nuvem da Amazon Web Services ou do Microsoft Azure ou um ponto de integração local de extensibilidade com base em ações que está associado a um proxy de extensibilidade de nuvem.

A integração com o IPAM externo requer um ambiente de execução. Ao definir o ponto de integração de IPAM, é possível criar uma conexão entre o Cloud Assembly e seu provedor de IPAM especificando um ambiente de execução disponível.

A integração de IPAM usa um conjunto baixado de scripts ou plug-ins específicos de provedor em um ambiente de execução que é facilitado por um provedor de Recurso como Serviço (FaaS), como o Amazon Web Services Lambda, Microsoft Azure Functions ou um ponto de integração incorporado de extensibilidade com base em ações (ABX) no local. O ambiente de execução é usado para conexão com o provedor de IPAM externo, por exemplo, o Infoblox.

Observação Um ponto de integração de IPAM Infoblox requer um ponto de integração incorporado de extensibilidade com base em ações (ABX) no local.

Cada tipo de ambiente de tempo de execução tem vantagens e desvantagens:

- Um ponto de integração de extensibilidade baseada em ações (ABX):
 - gratuito, não há custos adicionais de uso do fornecedor.
 - pode conectar-se a dispositivos de fornecedores de IPAM que residem em um centro de dados local protegido por um NAT/Firewall não acessível publicamente, por exemplo, o Infoblox.
 - é mais lento, com desempenho ligeiramente menos disponível do que a nuvem comercial.
- Amazon Web Services
 - tem custos associados de conexão/uso do FaaS do fornecedor
 - não pode conectar-se a dispositivos de fornecedores de IPAM que residem em um centro de dados local atrás de um NAT/Firewall que não está acessível publicamente.
 - tem desempenho rápido e altamente confiável.
- Microsoft Azure
 - tem custos associados de conexão/uso do FaaS do fornecedor
 - não pode conectar-se a dispositivos de fornecedores de IPAM que residem em um centro de dados local atrás de um NAT/Firewall que não está acessível publicamente.
 - tem desempenho rápido e altamente confiável.

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o [Infoblox](#) ou o [Bluecat](#), e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM.

- Verifique se você tem acesso a um pacote de integração implantado para seu provedor de IPAM, como o Infoblox ou o BlueCat. O pacote implantado é obtido inicialmente como um download de arquivo .zip do site do provedor de IPAM ou no [VMware Marketplace](#) e, em seguida, implantado no Cloud Assembly.

Para obter informações sobre como implantar o arquivo .zip de pacote do provedor e torná-lo disponível como um valor de **Provedor** na página Integração com o IPAM, consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

Procedimentos

- 1 Para criar uma ação de extensibilidade com base em FaaS local para uso como um ambiente de execução de integração de IPAM, selecione **Extensibilidade > Biblioteca > Ações**.
- 2 Clique em **Nova Ação**, insira um nome e uma descrição da ação e especifique um projeto.
- 3 No menu suspenso **Provedor FaaS**, selecione **Local**.
- 4 Preencha o formulário para definir a ação de extensibilidade.

Para obter mais informações sobre como criar ações de extensibilidade, consulte [Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade](#).



Para obter informações relacionadas ao ambiente de execução, consulte este vídeo do blog [Infoblox IPAM Plug-in Integration](#) aproximadamente aos 24 minutos do vídeo.

Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation

O vRealize Automation oferece suporte para a integração com provedores de IPAM externos. Este exemplo usa a Infoblox como provedor de IPAM externo.

Você pode usar um ponto de integração do IPAM específico do provedor para obter e gerenciar endereços IP e características de rede relacionadas para implantações de modelo de nuvem.

Neste exemplo, você cria um ponto de integração de IPAM externo para oferecer suporte ao acesso à conta da sua organização com um provedor de IPAM externo. Neste exemplo de fluxo de trabalho, o provedor de IPAM é o Infoblox, e o pacote de integração específico do provedor já existe. Embora essas instruções sejam específicas para uma integração com o Infoblox, elas podem ser usadas como referência caso você esteja criando uma integração de IPAM para um provedor de IPAM externo diferente.

Você pode obter um pacote de integração específico do provedor no site do seu provedor de IPAM ou no [VMware Marketplace](#).

Este exemplo usa o pacote Infoblox fornecido pela VMware `Infoblox.zip`, que está disponível para download no [VMware Marketplace](#). Para obter informações sobre as versões mais recentes do plug-in Infoblox que estão disponíveis no [VMware Marketplace](#), consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo e se tem as credenciais de acesso corretas para a conta da sua organização com o provedor de IPAM.
- Verifique se você tem acesso a um pacote de integração implantado para o seu provedor de IPAM. O pacote implantado é obtido inicialmente como o download de um arquivo .zip no site do provedor de IPAM ou no VMware Solutions Exchange Marketplace e, em seguida, é implantado no vRealize Automation.

Para obter informações sobre como baixar e implantar o arquivo .zip do pacote do provedor e torná-lo disponível como um valor de **Provedor** na página Integração com o IPAM, consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

- Verifique se você tem acesso a um ambiente de execução configurado para o provedor de IPAM. O ambiente de execução é em geral um ponto de integração incorporado no local de extensibilidade com base em ações (ABX).

Para obter informações sobre as características do ambiente de execução, consulte [Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation](#).

- Habilite os atributos extensíveis necessários no seu aplicativo Infoblox. Consulte [Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation](#).
- Se você não tiver acesso externo à internet, poderá configurar um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).
- Verifique se você tem as credenciais de usuário necessárias para acessar e usar o produto de IPAM da Infoblox. Por exemplo, abra a guia Administração no dispositivo Infoblox e personalize as entradas de administrador, grupos e funções. Você deve ser membro de um grupo que tenha permissões de administrador ou superusuário ou um grupo personalizado que tenha permissões de DHCP, DNS, IPAM e Grade. Essas configurações permitem o acesso a todas as funcionalidades disponíveis no plug-in Infoblox, permitindo que você crie uma integração de IPAM da Infoblox e que is designers usem essa integração de IPAM em modelos de nuvem e implantações. Para obter mais informações sobre permissões de usuário, consulte a documentação do produto Infoblox.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Clique em **IPAM**.

- 3 No menu suspenso **Provedor**, selecione um pacote de provedor de IPAM configurado na lista, por exemplo, *Infoblox_hrg*.

Se a lista estiver vazia, clique em **Importar Pacote do Provedor**, navegue até um arquivo .zip de pacote de provedor existente e selecione-o. Se você não tiver o arquivo .zip do provedor, poderá obtê-lo no site do seu provedor de IPAM ou no [VMware Marketplace](#).

Para obter informações sobre como implantar o arquivo .zip do pacote de provedor no vCenter e torná-lo disponível como um valor de **Provedor** na página Integração, consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

Para obter informações sobre como atualizar uma integração de IPAM existente para usar uma versão mais recente do pacote de integração de IPAM de um fornecedor, consulte [Como fazer upgrade para um pacote de integração de IPAM externo mais recente no vRealize Automation](#).

- 4 Insira suas credenciais de nome de usuário e senha de administrador da sua conta com o provedor de IPAM externo, juntamente com todos os outros campos obrigatórios (se houver), como o nome de host do seu provedor.

Neste exemplo, você obtém o nome do host do seu provedor de IPAM Infoblox usando as seguintes etapas:

- a Em uma guia separada do navegador, faça login na sua conta de provedor de IPAM usando suas credenciais de administrador do Infoblox.
- b Copie a URL do nome do host.
- c Cole a URL do nome do host no campo **Nome do Host** na página Integração com o IPAM.

- 5 Na lista suspensa **Ambiente em Execução**, selecione um ponto de integração local de extensibilidade com base em ações, por exemplo, *Infoblox_abx_intg*.

O ambiente de execução oferece suporte à comunicação entre o vRealize Automation e o provedor de IPAM externo.

Observação Se você usar uma conta de nuvem do Amazon Web Services ou Microsoft Azure como o ambiente de execução da integração, certifique-se de que o dispositivo do provedor de IPAM esteja acessível na Internet, não esteja atrás de um NAT ou firewall e tenha um nome DNS que possa ser resolvido publicamente. Se o provedor de IPAM não estiver acessível, o Amazon Web Services Lambda ou o Microsoft Azure Functions não conseguirão se conectar a ele, e a integração falhará. Para obter informações relacionadas, consulte [Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation](#).

A estrutura de IPAM só é compatível com um ambiente de execução incorporado de extensibilidade com base em ações (ABX) no local.

Observação Um ponto de integração de IPAM Infoblox requer um ponto de integração incorporado de extensibilidade com base em ações (ABX) no local.

A conta de nuvem ou o ponto de integração configurado permite a comunicação entre o vRealize Automation e o provedor de IPAM, neste exemplo a Infoblox, por meio de um proxy de extensibilidade de nuvem associado. Você pode selecionar um provedor que já tenha sido criado ou pode criar um.

Para obter informações sobre como criar um ambiente de execução, consulte [Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation](#).

6 Clique em **Validar**.

Como este exemplo usa a integração de extensibilidade com base em ações no local para o ambiente de execução, você pode visualizar a ação de validação.

- a Clique na guia **Extensibilidade**.
- b Clique em **Atividade > Execuções de Ação** e selecione **Todas as Execuções** ou **Execuções de integração** no filtro para observar se uma ação de validação de endpoint é iniciada e está em execução.

7 Quando solicitado a confiar no certificado autoassinado do provedor de IPAM, clique em **Aceitar**.

Depois que você aceitar o certificado autoassinado, a ação de validação poderá continuar até ser concluída.

8 Insira um **Nome** para esse ponto de integração de IPAM, como *Infoblox_Integration*, e uma **Descrição**, como *Infoblox IPAM com integração de ABX para a equipe HRG*.

9 Clique em **Adicionar** para salvar o novo ponto de integração de IPAM externo.

Uma ação de coleta de dados é iniciada. As redes e os intervalos de IP são coletados por dados pelo provedor de IPAM. Você pode visualizar a ação de coleta de dados da seguinte maneira:

- a Clique na guia **Extensibilidade**.
- b Clique em **Atividade > Execuções de Ação** e observe se uma ação de coleta de dados é iniciada e está em execução. Você pode abrir e visualizar o conteúdo de execução da ação.

Resultados

A integração de IPAM externo específica do provedor agora está disponível para uso com redes e perfis de rede.

Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente no vRealize Automation

Você pode definir uma rede existente para usar os valores de endereço IP obtidos e gerenciados por um provedor de IPAM externo, em vez de internamente do vRealize Automation.

É possível definir uma rede para acessar configurações de IP existentes que você definiu na conta do provedor de IPAM externo da sua organização. Essa etapa expande a integração com o provedor Infoblox que você criou na etapa anterior.

Neste exemplo, você configura um perfil de rede com redes existentes cujos dados foram coletados do vCenter. Em seguida, essas redes são configuradas para obter informações de IP de um provedor de IPAM externo, neste caso, o Infoblox. As máquinas virtuais provisionadas do vRealize Automation que podem ser correspondidas a esse perfil de rede obtêm o IP e outras configurações relacionadas ao TCP/IP do provedor de IPAM externo.

Para obter mais informações sobre redes, consulte [Recursos de rede no vRealize Automation](#).

Para obter mais informações sobre perfis de rede, consulte [Como adicionar perfis de rede no vRealize Automation](#) e [Saiba mais sobre perfis de rede no vRealize Automation](#).

Para obter informações relacionadas, consulte [Como configurar um perfil de rede para oferecer suporte a uma rede sob demanda para uma integração de IPAM externa no vRealize Automation](#).

Pré-requisitos

Essa sequência de etapas é mostrada no contexto de um fluxo de trabalho de integração do provedor de IPAM. Consulte [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#).

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o [Infoblox](#) ou o [Bluecat](#), e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM. Neste exemplo de fluxo de trabalho, o provedor de IPAM é o Infoblox.
- Verifique se você tem um ponto de integração de IPAM para o provedor de IPAM. Consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).

Procedimentos

- 1 Para configurar uma rede, clique em **Infraestrutura > Recursos > Redes**.
- 2 Na guia **Redes**, selecione uma rede existente a ser usada com o ponto de integração com o provedor de IPAM. Neste exemplo, o nome da rede é *net.23.117-only-IPAM*.

As redes listadas tiveram os dados coletados pelo vRealize Automation de um vCenter na sua organização.

- 3 Para obter valores do provedor de IPAM externo, certifique-se de que, exceto pela **Conta/região**, o **Nome** e o **Domínio de rede**, todas as outras configurações de rede estejam vazias, incluindo o seguinte:

- Domínio (consulte a Observação na etapa 8)

- CIDR
 - Gateway padrão
 - Servidores DNS
 - Domínios de pesquisa de DNS
- 4 Clique na guia **Intervalos de IP** e clique em **Adicionar Intervalo de IP do IPAM**.
 - 5 No menu **Rede**, selecione a rede que você acabou de configurar, por exemplo *net.23.117-only-IPAM*.
 - 6 No menu **Provedor**, selecione o ponto de integração com o IPAM *Infoblox_Integration* que você criou anteriormente no fluxo de trabalho
 - 7 No menu suspenso **Espaço de Endereço** agora visível, selecione uma das exibições de rede listadas.

Um espaço de endereço no Infoblox é chamado de exibição de rede.

As exibições de rede são obtidas da conta do provedor de IPAM. Este exemplo usa a sub-rede que você acabou de configurar, por exemplo *net.23.117-only-IPAM*, o ponto de integração *Infoblox_Integration* criado anteriormente no fluxo de trabalho e um espaço de endereço denominado *default*.

Os valores de espaço de endereço listados são obtidos do provedor de IPAM externo.

- 8 Na lista de redes exibidas que estão disponíveis para o espaço de endereço selecionado, selecione uma ou mais redes, por exemplo, selecione 10.23.117.0/24.

Para esse exemplo, os valores das colunas **Domínios** e **Servidores DNS** da rede selecionada contêm valores do Infoblox.

Observação Se você selecionar uma rede na Etapa 3 que tinha um Domínio especificado para o vRealize Automation e, em seguida, selecionar uma rede do espaço de endereço do provedor de IPAM externo que contém um valor de Domínio, o valor de Domínio na rede do provedor de IPAM externo terá precedência sobre o Domínio especificado no vRealize Automation. Se a configuração de intervalo de IPs do IPAM não tiver um valor de Domínio especificado no Cloud Assembly ou no provedor de IPAM externo, conforme descrito acima, o provisionamento falhará.

Para o Infoblox, você pode usar a propriedade de blueprint

`Infoblox.IPAM.Network.dnsSuffix` no nível da máquina para substituir o valor de Domínio. Para obter informações relacionadas, consulte [Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation](#).

- 9 Clique em **Adicionar** para salvar o intervalo de IPs do IPAM da rede.
- O intervalo fica visível na tabela **Intervalos de IP**.

10 Clique na guia **Endereços IP**.

Depois de provisionar uma máquina usando o novo intervalo de endereços do provedor de IPAM externo, um novo registro estará visível na tabela **Endereços IP**.

11 Para configurar um perfil de rede para usar a rede, clique em **Infraestrutura > Configurar > Perfis de Rede**.**12** Dê um nome para o perfil de rede, como *Infoblox-NP* e adicione as seguintes configurações de amostra.

■ Guia Resumo

- Especifique uma conta/região de nuvem do vSphere.
- Adicione uma tag de capacidade para o perfil de rede, por exemplo, com o nome *infoblox_abx*.

Anote a tag de capacidade, já que você também deve usá-la como uma tag de restrição de modelo de nuvem para fazer a associação de provisionamento no modelo de nuvem.

■ Guia Redes

- Adicione a rede criada anteriormente, por exemplo, *net.23.117-only-IPAM*.

13 Clique em **Salvar** para salvar o perfil de rede com essas configurações.**Resultados**

A configuração da rede e do perfil de rede está agora definida para um tipo de rede existente a ser usado para a integração de IPAM da Infoblox em um modelo de nuvem.

Definir e implantar um modelo de nuvem que usa uma atribuição de intervalo de provedor de IPAM externo no vRealize Automation

Você pode definir um modelo de nuvem para obter e gerenciar atribuições de endereços IP do seu provedor de IPAM externo. Este exemplo usa a Infoblox como provedor de IPAM externo.

Nesta etapa final no fluxo de trabalho de integração de IPAM externo, você define e implanta um modelo de nuvem que conecta a rede e o perfil de rede previamente definidos à conta do Infoblox da sua organização para obter e gerenciar atribuições de endereços IP para VMs implantadas do provedor de IPAM externo, e não do vRealize Automation.

Este fluxo de trabalho usa o Infoblox como o provedor de IPAM externo e, em algumas etapas, os valores de exemplo são exclusivos para o Infoblox, embora a intenção seja que o procedimento possa ser aplicado a outras integrações de IPAM externo.



O blog do Infoblox, [Automatizar o IPAM e o DNS para VMs usando o VMware vRealize Automation e o Infoblox DDI](#), fornece informações relacionadas.

Depois que você implantar o modelo de nuvem e a VM for iniciada, o endereço IP usado para cada VM na implantação aparecerá como uma entrada de rede na página **Recursos > Redes**, como um novo registro de host na rede do provedor de IPAM na sua conta de provedor de IPAM e no registro do vSphere Web Client para cada VM implantada no host vCenter.

Pré-requisitos

Esta sequência de etapas é mostrada no contexto de um fluxo de trabalho de integração do provedor de IPAM externo. Consulte [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#).

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o Infoblox ou o BlueCat, e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM.
- Verifique se você tem acesso de administrador à conta de host e a quaisquer requisitos de função necessários para exibir registros de status no registro do vSphere Web Client para suas VMs implantadas no host vCenter.
- Verifique se você tem um ponto de integração de IPAM para o provedor de IPAM externo. Consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).
- Verifique se você configurou uma rede do vRealize Automation e um perfil de rede que oferecem suporte à integração de IPAM externo para o seu ponto de integração de IPAM pretendido. Consulte [Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente no vRealize Automation](#).
- Verifique se o seu projeto e a zona de nuvem estão marcados para corresponder as tags no ponto de integração de IPAM e na rede e no perfil de rede. Opcionalmente, configure o projeto para oferecer suporte à nomenclatura de nome de recurso personalizado.

Para obter mais informações do que o fornecido sobre a função de um projeto e uma zona de nuvem, bem como sobre a função de outros elementos de infraestrutura no seu modelo de nuvem, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#). Para obter mais informações sobre marcação, consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).

Para obter informações sobre as VMs de nomenclatura personalizadas usando as configurações no seu projeto, consulte [Nomenclatura personalizada para recursos implantados no Cloud Assembly](#).

Procedimentos

- 1 Clique em **Modelos de nuvem > Novo**, insira as seguintes informações na página **Novo modelo de nuvem** e clique em **Criar**.
 - **Nome** = ipam-bpa
 - **Descrição** = Modelo de nuvem que usa a integração de IPAM da Infoblox
 - **Projeto** = 123VC
- 2 Para esse exemplo, adicione um componente de máquina independente de nuvem e um componente de rede independente de nuvem à tela do modelo de nuvem e conecte esses dois componentes.
- 3 Edite o código do modelo de nuvem para adicionar uma tag de restrição ao componente de rede que corresponde à tag de capacidade que você adicionou ao perfil de rede. Para esse exemplo, esse valor de tag é *infoblox_abx*.
- 4 Edite o código do modelo de nuvem para especificar que o tipo de atribuição de rede é *static*.
Ao usar um provedor de IPAM externo, a configuração do `assignment: static` é necessária.
Para esse exemplo, o 10.23.117.4 de endereço IP especificado pode estar disponível no momento no espaço de endereço do IPAM externo selecionado para a rede no perfil de rede associado. Embora a configuração `assignment: static` seja necessária, a configuração `address: value` não é. Você pode optar por iniciar a seleção do endereço IP externo em um valor de endereço específico, mas isso não é obrigatório. Se você não especificar uma configuração `address: value`, o provedor de IPAM externo selecionará o próximo endereço disponível na rede do IPAM externo.
- 5 Verifique o código do modelo de nuvem no exemplo a seguir.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      name: ipam
      constraints:
        - tag: infoblox_abx
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
          address: 10.23.117.4
          name: '${resource.Cloud_Network_1.name}'
```

Para exemplos de propriedades Infoblox que estão disponíveis para especificar configurações de DNS e DHCP em modelos de nuvem, consulte [Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation](#).

- 6 Clique em **Implantar** na página do modelo de nuvem, especifique o nome *Infoblox-1* para a implantação e clique em **Implantar** na página **Tipo de Implantação**.
- 7 Conforme o modelo de nuvem estiver sendo implantado, clique na guia **Extensibilidade** e selecione **Atividades > Execuções de Ação** para ver a ação de extensibilidade *Infoblox_AllocateIP_n* em execução.

Depois que a ação de extensibilidade for concluída e a máquina for provisionada, a ação *Infoblox_Update_n* propagará o endereço MAC para o Infoblox.
- 8 Você pode fazer login e abrir sua conta do Infoblox para ver o novo registro de host para o endereço de IPAM na rede 10.23.117.0/24 associada. Você também pode abrir a guia DNS no Infoblox para ver o novo registro de host DNS.
- 9 Para verificar se a VM está sendo provisionada, faça login no seu host vCenter e vSphere Web Client para localizar a máquina provisionada e exibir o nome e o endereço IP do DNS.

Depois que a VM provisionada for iniciada, o endereço MAC será propagado ao Infoblox por uma ação de extensibilidade *Infoblox_AllocateIP*.
- 10 Para exibir o novo registro de rede no vRealize Automation, selecione **Infraestrutura > Recursos > Redes** e clique para abrir a guia **Endereços IP**.
- 11 Se você excluir a implantação, o endereço de IPAM das VMs na implantação será liberado, e os endereços IP voltarão a ficar disponíveis para o provedor de IPAM externo para outras alocações. A ação de extensibilidade para esse evento no vRealize Automation é *Infoblox_Deallocate*.

Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation

Você pode usar propriedades específicas do Infoblox para projetos do vRealize Automation que contenham integrações de IPAM externas para o Infoblox.

As seguintes propriedades do Infoblox estão disponíveis para uso com as suas integrações de IPAM do Infoblox em designs e implantações de modelos de nuvem. Você pode usá-las no vRealize Automation para controlar ainda mais a alocação de endereços IP durante a implantação do modelo de nuvem. O uso dessas propriedades é opcional.

Observação Se você estiver usando o plug-in Infoblox 1.4 ou versão anterior, uma propriedade do Infoblox global substituirá uma propriedade do Infoblox local para as propriedades *dnsSuffix*, *dnsView*, *enableDns* e *enableDhcp*. Uma propriedade global se aplica a todas as NICs.

As propriedades a seguir estão disponíveis e incluídas na versão mais recente do plug-in Infoblox para o vRealize Automation. Para obter informações sobre as versões do plug-in Infoblox e onde obter a versão mais recente do plug-in Infoblox para sua integração de IPAM no vRealize Automation, consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

- `Infoblox.IPAM.createFixedAddress`

Essa propriedade permite criar um registro de endereço fixo dentro do Infoblox. Os valores possíveis são True e False. Por padrão, um registro de host é criado. O valor padrão é False.

- `Infoblox.IPAM.Network.dnsView`

Essa propriedade permite que usar uma exibição de DNS ao criar um registro de host dentro do Infoblox.

- `Infoblox.IPAM.Network.enableDns`

Ao alocar um IP no Infoblox, essa propriedade permite que você também crie um registro de DNS. Os valores possíveis são True e False. O valor padrão é True.

- `Infoblox.IPAM.Network.enableDhcp`

Essa propriedade permite que você defina a configuração de DHCP para o endereço do host. Os valores possíveis são True e False. O valor padrão é True.

- `Infoblox.IPAM.Network.dnsSuffix`

Essa propriedade permite que você substitua a opção de DHCP *domain* de uma rede Infoblox por uma nova. Esse recurso é útil quando a rede Infoblox não tem a opção de DHCP *domínio* definida ou quando a opção de DHCP *domínio* deve ser substituída. O valor padrão é nulo (string vazia).

Ao usar um provedor de IPAM externo, como o Infoblox, você deve especificar um sufixo DNS ao provisionar uma máquina. Embora o sufixo DNS seja necessário, você pode especificá-lo de qualquer uma das seguintes maneiras:

- Especifique o sufixo DNS na sub-rede da rede vSphere no vRealize Automation.
- Especifique a propriedade `Infoblox.IPAM.Network.dnsSuffix` no código de recurso da máquina no modelo de nuvem do vRealize Automation.

Um exemplo é mostrado abaixo na seção `Infoblox.IPAM.Network.hostnameNicSuffix`.

`Infoblox.IPAM.Network.dnsSuffix` apenas será aplicável se `Infoblox.IPAM.Network.enableDns` estiver definido como True.

- `Infoblox.IPAM.Network.hostnameNicSuffix`

Você pode usar essa propriedade para especificar um sufixo de índice de NIC ao gerar um nome de host.

Isso permite provisionar uma máquina com mais de uma NIC, de forma que os nomes de host de cada NIC sejam diferenciados por um sufixo definido personalizado. Como visto no exemplo a seguir, você pode provisionar uma máquina, por exemplo *my-machine*, que possui 2 NICs, para que o sufixo de nome de host da primeira NIC seja *-nic1* e o outro seja *-nic2*.

Você também pode especificar um sufixo DNS conforme mostrado no exemplo. A propriedade `Infoblox.IPAM.Network.dnsSuffix` é usada com um valor de `test.local` para fazer com que a primeira NIC receba o nome *my-machine-nic1.test.local* e a outra, *my-machine-nic2.test.local*.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network.dnsSuffix: test.local
      Infoblox.IPAM.Network0.hostnameNicSuffix: -nic1
      Infoblox.IPAM.Network1.hostnameNicSuffix: -nic2
    image: ubuntu
    flavor: small
    networks:
      - network: '${resource.Cloud_Network_1.id}'
        deviceIndex: 0
      - network: '${resource.Cloud_Network_2.id}'
        deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
  Cloud_Network_2:
    type: Cloud.Network
    properties:
      networkType: existing
```

Essa propriedade foi introduzida com o plug-in Infoblox versão 1.3. Consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

- Também é possível especificar propriedades usando uma assinatura de extensibilidade.

Para obter informações relacionadas sobre atributos extensível do Infoblox relativos a esse caso de uso, consulte [Adicionar atributos extensíveis necessários no aplicativo Infoblox para integração com o vRealize Automation](#).

Usando as propriedades Infoblox em NICs de máquinas diferentes em um modelo de nuvem

As seguintes propriedades Infoblox podem oferecer suporte a um valor diferente para cada NIC de máquina no modelo de nuvem:

- `Infoblox.IPAM.Network.enableDhcp`
- `Infoblox.IPAM.Network.dnsView`

- `Infoblox.IPAM.Network.enableDns`
- `Infoblox.IPAM.Network.hostnameNicSuffix`

Por exemplo, para usar um valor `Infoblox.IPAM.Network.dnsView` diferente para cada NIC, use uma entrada `Infoblox.IPAM.Network<nicIndex>.dnsView` para cada NIC. O exemplo a seguir mostra valores `Infoblox.IPAM.Network.dnsView` diferentes para duas NICs.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network0.dnsView: default
      Infoblox.IPAM.Network1.dnsView: my-net
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
  Cloud_Network_2:
    type: Cloud.Network
    properties:
      networkType: existing
```

Por padrão, a integração do Infoblox cria um registro de host DNS na exibição de DNS *default* no Infoblox. Se o administrador do Infoblox tiver criado exibições de DNS *custom*, poderá substituir o comportamento de integração padrão e especificar uma exibição nomeada usando a propriedade `Infoblox.IPAM.Network.dnsView` no componente de máquina. Por exemplo, você pode adicionar a propriedade a seguir ao componente `Cloud_Machine_1` para especificar uma exibição de DNS nomeada no Infoblox.

```
Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: ubuntu
    flavor: small
    Infoblox.IPAM.Network.dnsView:<dns-view-name>
```

Para obter informações sobre como configurar e usar modos de exibição de DNS, consulte [Exibições de DNS](#) na documentação do produto Infoblox. Para obter exemplos no fluxo de trabalho de integração Infoblox, consulte [Definir e implantar um modelo de nuvem que usa uma atribuição de intervalo de provedor de IPAM externo no vRealize Automation](#).

Como especificar propriedades do Infoblox

É possível especificar uma propriedade do Infoblox usando um dos seguintes métodos no Cloud Assembly:

- Você pode especificar as propriedades em um projeto usando a seção **Propriedades personalizadas** na página **Infraestrutura > Administração > Projetos**. Usando esse método, as propriedades especificadas são aplicadas a todas as máquinas que são provisionadas no escopo desse projeto.
- Você pode especificar propriedades em cada componente de máquina de um modelo de nuvem. Um exemplo de código de modelo de nuvem ilustrando o uso da propriedade `Infoblox.IPAM.Network.dnsView` é mostrado abaixo:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      Infoblox.IPAM.Network.dnsView: default
      image: ubuntu
      cpuCount: 1
      totalMemoryMB: 1024
      networks:
        - network: '${resource.Cloud_Network_1.id}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      constraints:
        - tag: mk-ipam-demo
```

Controlar a coleta de dados de rede usando filtros Infoblox no vRealize Automation

Para o Infoblox, você pode limitar o número de redes com dados coletados a apenas as redes necessárias para as operações do vRealize Automation. Isso reduz a quantidade de dados transferidos e melhora o desempenho do sistema.

O vRealize Automation coleta dados a cada 10 minutos do sistema IPAM externo. Para o Infoblox, você pode filtrar de várias maneiras para descobrir e coletar dados de apenas um subconjunto de redes que são usadas pelas operações do vRealize Automation.

Para filtrar a coleta de dados para redes que usam endereços IP gerados pelo Infoblox, use as seguintes propriedades na guia Integração com o IPAM. As propriedades de filtro estão disponíveis à medida que você cria ou edita o ponto de integração do IPAM externo para o Infoblox.

Esses filtros só estão disponíveis com o vRealize Automation 8.3 e versões posteriores e com o [plug-in Infoblox versão 1.3](#) e posteriores (por exemplo, [plug-in Infoblox versão 1.4](#)).

Observação O [plug-in Infoblox 1.3](#) pode ser usado com o vRealize Automation 8.1 ou 8.2, mas somente em situações e com cautela, conforme descrito no artigo da base de dados de conhecimento [Compatibilidade do Infoblox 1.3 com o vRealize Automation 8.x \(82142\)](#).

- `Infoblox.IPAM.NetworkContainerFilter`

Filtros em contêineres de rede.

- `Infoblox.IPAM.NetworkFilter`

Filtro em redes.

- `Infoblox.IPAM.RangeFilter`

Filtro em intervalos de endereços IP.

Tenha cuidado ao aplicar esses filtros de coleta de dados a redes que já tenham passado por uma coleta de dados. Se você aplicar filtros para impedir que algumas redes tenham dados coletados, as redes sem coleta serão consideradas desnecessárias e serão excluídas do vRealize Automation. A exceção são redes que estão associadas a sub-redes do vRealize Automation. As redes anteriormente com dados coletados que não forem descobertas posteriormente e cujos dados não forem coletados, por exemplo, porque foram removidas da tarefa de coleta de dados, serão excluídas do banco de dados do vRealize Automation. No entanto, se as redes coletadas anteriormente estiverem em uso no vRealize Automation, elas não serão excluídas.

Esses filtros são aplicados como parâmetros de consulta nas solicitações de pesquisa para os diferentes objetos de rede. Você pode usar qualquer parâmetro de pesquisa com suporte pelo Infoblox. A filtragem é feita por CIDR ou por atributos extensíveis que se baseiam em expressões regulares ou correspondências exatas. O formato usa o formato de filtragem Infoblox WAPI, conforme descrito na [documentação do Infoblox WAPI](#). Os métodos de filtragem por CIDR ou atributos extensíveis são mostrados nos exemplos a seguir:

- Filtrar com base no CIDR para redes e contêineres de rede. Exemplos:

- Correspondência exata - `Infoblox.IPAM.NetworkFilter: network=192.168.0.0`

- Corresponder por atributo extensível - `Infoblox.IPAM.NetworkFilter: network~=192.168`

- Filtrar com base no CIDR para o intervalo de endereços IP. Exemplo:

Corresponder por expressão regular e nome da exibição de rede -

`Infoblox.IPAM.RangeFilter: network~=192.168.&network_view=my_view`

- Filtrar com base em atributos extensíveis para redes, intervalos de IP e contêineres de rede.

A sintaxe usa o formato `filter_name=*ext_attr=ext_attr_value`. Exemplos:

- Correspondência exata - `*Building=Data Center`

- Corresponder por expressão regular com '~' - `*Building~=*Center`

- Correspondência com diferenciação entre maiúsculas e minúsculas com ':' -
`*Building:=data center`
- Excluir correspondência com '!' - `*Building!=Data Center`
- Corresponder por expressão regular (é possível combinar diferenciação entre maiúsculas e minúsculas com exclusão): `*Building! ~:=Data Cent / *Building~:=center`
- Filtrar com base em CIDR e atributos extensíveis usando a sintaxe dos métodos de filtragem acima. Exemplo:
`network=192.168.&*Building=Data Center`

Para obter mais informações sobre como usar atributos extensíveis e expressões regulares nessas propriedades, consulte [Expressões com suporte pelo Infoblox para parâmetros de pesquisa](#) e o [Guia de referência de REST APIs do Infoblox](#).

Como configurar o Cloud Assembly para sua organização

3

Como administrador do Cloud Assembly, é necessário compreender as funções do usuário e configurar as conexões com o fornecedor da sua conta de nuvem e com os aplicativos de integração.

Ao configurar as contas de nuvem e as integrações, você está configurando a comunicação entre o Cloud Assembly e esses sistemas de destino.

Este capítulo inclui os seguintes tópicos:

- Quais são as funções de usuário do vRealize Automation
- Como adicionar contas de nuvem ao Cloud Assembly
- Como integrar o vRealize Automation a outros aplicativos
- O que são planos de integração no Cloud Assembly
- Configuração avançada para o ambiente do Cloud Assembly

Quais são as funções de usuário do vRealize Automation

O vRealize Automation tem vários níveis de funções de usuário. Esses níveis diferentes controlam o acesso à organização, aos serviços, aos projetos que produzem ou consomem os modelos de nuvem, itens do catálogo e pipelines, e a capacidade dos usuários de usar ou ver partes individuais da interface do usuário. Esses níveis diferentes dão aos administradores de nuvem diferentes ferramentas para aplicar qualquer nível de granularidade exigido pelas suas necessidades operacionais.

Descrição geral das funções

As funções de usuário são definidas em diferentes níveis. As funções de nível de serviço são definidas para cada serviço.

Mais detalhes sobre as funções de serviço são fornecidos abaixo desta tabela.

| Função | Permissões gerais | Onde a função está definida |
|-----------------------------|---|-----------------------------|
| Proprietário da Organização | <p>Pode acessar o console e adicionar usuários à organização.</p> <p>O proprietário da organização não pode acessar um serviço, a menos que ele tenha uma função de serviço.</p> <p>Mais sobre o Funções de usuário de organização</p> | Console da organização |
| Membro da Organização | <p>Pode acessar o console.</p> <p>O membro da organização não pode acessar um serviço, a menos que ele tenha uma função de serviço.</p> <p>Mais sobre o Funções de usuário de organização</p> | Console da organização |
| Administrador do serviço | <p>Pode acessar o console e tem os privilégios de visualizar, atualizar e excluir privilégios no serviço.</p> <ul style="list-style-type: none"> ■ Funções de serviço do Cloud Assembly ■ Funções de serviço do Service Broker ■ Funções de serviço do Code Stream ■ Funções de serviço do vRA Migration Assistant ■ Funções de serviço do Orchestrator ■ Função de serviço do SaltStack Config | Console da organização |
| Usuário do serviço | <p>Pode acessar o console e o serviço com permissões limitadas.</p> <p>O membro de serviço tem uma interface de usuário limitada. O que ele pode ver ou fazer depende da associação no projeto.</p> <ul style="list-style-type: none"> ■ Funções de serviço do Cloud Assembly ■ Funções de serviço do Service Broker ■ Funções de serviço do Code Stream | Console da organização |

| Função | Permissões gerais | Onde a função está definida |
|--|--|--|
| Visualizador do serviço | <p>Pode acessar o console e o serviço em um modo somente para exibição.</p> <ul style="list-style-type: none"> ■ Funções de serviço do Cloud Assembly ■ Funções de serviço do Service Broker ■ Funções de serviço do Code Stream ■ Funções de serviço do vRA Migration Assistant ■ Funções de serviço do Orchestrator | Console da organização |
| Executor (somente Code Stream) | <p>Pode acessar o console e gerenciar execuções de pipeline.</p> <p>Funções de serviço do Code Stream</p> | Console da organização |
| Designer de fluxo de trabalho do Orchestrator (somente Orchestrator) | <p>Pode criar, executar, editar e excluir o próprio conteúdo de cliente do vRealize Orchestrator. Pode adicionar seu próprio conteúdo ao grupo atribuído. Não tem acesso aos recursos de administração e solução de problemas do cliente do vRealize Orchestrator.</p> <p>Funções de serviço do Orchestrator</p> | Console da organização |
| Funções de projeto | <p>Pode visualizar e gerenciar os recursos do projeto, dependendo da função do projeto.</p> <p>As funções do projeto incluem administrador, membro e visualizador.</p> <p>Funções de usuário de serviço e organização no vRealize Automation</p> | Cloud Assembly, Service Broker e Code Stream |
| Funções personalizadas | <p>As permissões são definidas pelo Administrador do Cloud Assembly para todos os serviços.</p> <p>O usuário deve ter pelo menos uma função de visualizador nos serviços pertinentes para que possa acessar o serviço. As funções personalizadas têm precedência sobre as funções de serviço.</p> <p>Personalizar funções de usuário no vRealize Automation</p> | Cloud Assembly e Service Broker |
| Função integrada de administrador de infraestrutura | <p>Concede permissões predefinidas para tarefas no vRealize Automation.</p> <p>Como atribuir a função integrada de Administrador de Infraestrutura do Cloud Assembly a um usuário</p> | Usando a API |

Funções de usuário de serviço e organização no vRealize Automation

As funções de usuário de serviço e organização que você define para os serviços Cloud Assembly, Service Broker e Code Stream determinam o que o usuário vê e faz em cada serviço.

Funções de usuário de organização

Funções de usuário são definidas para a organização no console do vRealize Automation por um proprietário da organização. Há dois tipos de funções, funções de organização e funções de serviço.

As funções da organização são globais e aplicam-se a todos os serviços na organização. As funções no nível da organização são Proprietário da organização ou Membro da organização.

Para obter mais informações sobre funções de organização, consulte [Administrando o vRealize Automation](#)

As funções de serviço do Cloud Assembly, que são permissões específicas de serviço, também são atribuídas no nível da organização no console.

Funções de serviço

Essas funções de serviço são atribuídas pelo proprietário da organização.

Este artigo inclui informações sobre os serviços a seguir.

- [Funções de serviço do Cloud Assembly](#)
- [Funções de serviço do Service Broker](#)
- [Funções de serviço do Code Stream](#)
- [Funções de serviço do vRA Migration Assistant](#)
- [Funções de serviço do Orchestrator](#)
- [Função de serviço do SaltStack Config](#)

Funções de serviço do Cloud Assembly

As funções de serviço do Cloud Assembly determinam o que você pode ver e fazer no Cloud Assembly. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 3-1. Descrições das funções de serviço do Cloud Assembly

| Função | Descrição |
|---------------------------------|--|
| Administrador do Cloud Assembly | Um usuário que tenha acesso de leitura e gravação para toda a interface do usuário e recursos de API. Essa é a única função de usuário que pode ver e fazer tudo, incluindo adicionar contas de nuvem, criar novos projetos e atribuir um administrador de projeto. |
| Usuário do Cloud Assembly | Um usuário que não tem a função Administrador do Cloud Assembly. Em um projeto Cloud Assembly, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto. |
| Expectador do Cloud Assembly | Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. Esta é uma função somente leitura em todos os projetos. Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

Além das funções de serviço, o Cloud Assembly tem funções de projeto. Todos os projetos estão disponíveis em todos os serviços.

As funções de projeto são definidas no Cloud Assembly e podem variar entre projetos.

Nas tabelas a seguir, que indicam o que as diferentes funções de serviço e projeto podem ver e fazer, lembre-se de que os administradores de serviços têm permissão total em todas as áreas da interface do usuário.

As descrições das funções de projetos ajudarão você a decidir quais permissões conceder aos usuários.

- Os administradores de projetos aproveitam a infraestrutura criada pelo administrador de serviços para garantir que os membros do projeto tenham os recursos necessários para o trabalho de desenvolvimento.
- Os membros do projeto trabalham em seus projetos para projetar e implantar modelos de nuvem. Seus projetos podem incluir apenas os recursos que você possui ou os recursos compartilhados com outros membros do projeto.
- Os espectadores de projeto estão restritos ao acesso somente leitura, com exceção de alguns casos em que eles podem realizar ações não destrutivas, como baixar modelos de nuvem.

- Os supervisores de projeto são aprovadores no Service Broker nos projetos em que uma política de aprovação é definida com um aprovador de supervisor de projeto. Para fornecer contexto ao supervisor para as aprovações, considere também conceder a ele a função de membro ou visualizador do projeto.

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|--|---------------------------------|------------------------------|--|--------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Acessar o Cloud Assembly | | | | | | | |
| Console | No console do vRA, você pode ver e abrir o Cloud Assembly | Sim | Sim | Sim | Sim | Sim | Sim |
| Infraestrutura | | | | | | | |
| | Visualizar e abrir a guia Infraestrutura | Sim | Sim | Sim | Sim | Sim | Sim |
| Configurar - Projetos | Criar projetos | Sim | | | | | |
| | Atualizar ou excluir valores do resumo do projeto, provisionamento, Kubernetes, integrações e testar configurações de projeto. | Sim | | | | | |
| | Adicionar usuários e grupos e atribuir funções em projetos. | Sim | | Sim. Seus projetos. | | | |
| | Visualizar projetos | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos |
| Configurar - Zonas de Nuvem | Criar, atualizar ou excluir zonas de nuvem | Sim | | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|--------------------------------------|---|---------------------------------|------------------------------|--|-------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Visualizar zonas de nuvem | Sim | Sim | | | | |
| | Visualizar o dashboard Insights da zona da nuvem | Sim | Sim | | | | |
| | Visualizar alertas de zonas de nuvem | Sim | Sim | | | | |
| Configurar - Zonas do Kubernetes | Criar, atualizar ou excluir zonas do Kubernetes | Sim | | | | | |
| | Exibir zonas do Kubernetes | Sim | Sim | | | | |
| Configurar - Tipos | Criar, atualizar ou excluir tipos | Sim | | | | | |
| | Exibir tipos | Sim | Sim | | | | |
| Configurar - Mapeamentos de Imagem | Criar, atualizar ou excluir mapeamentos de imagens | Sim | | | | | |
| | Visualizar mapeamentos de imagem | Sim | Sim | | | | |
| Configurar - Perfis de Rede | Criar, atualizar ou excluir perfis de rede | Sim | | | | | |
| | Exibir perfis de rede de imagem | Sim | Sim | | | | |
| Configurar - Perfis de Armazenamento | Criar, atualizar ou excluir perfis de armazenamento | Sim | | | | | |
| | Exibir perfis de armazenamento de imagem | Sim | Sim | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|--|---------------------------------|------------------------------|--|-------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Configurar - Cartões de Preços | Criar, atualizar ou excluir cartões de preços | Sim | | | | | |
| | Exibir cartões de preços | Sim | Sim | | | | |
| Configurar - Tags | Criar, atualizar ou excluir tags | Sim | | | | | |
| | Exibir tags | Sim | Sim | | | | |
| Recursos - Processamento | Adicionar tags aos recursos de processamento descobertos | Sim | | | | | |
| | Exibir recursos de processamento descobertos | Sim | Sim | | | | |
| Recursos - Redes | Modificar tags de rede, intervalos de IP, endereços IP | Sim | | | | | |
| | Exibir recursos de rede descobertos | Sim | Sim | | | | |
| Recursos - Segurança | Adicionar tags a grupos de segurança descobertos | Sim | | | | | |
| | Exibir grupos de segurança descobertos | Sim | Sim | | | | |
| Recursos - Armazenamento | Adicionar tags ao armazenamento descoberto | Sim | | | | | |
| | Exibir armazenamento | Sim | Sim | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|---|---------------------------------|------------------------------|--|--------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Recursos - Kubernetes | Implantar ou adicionar clusters do Kubernetes e criar ou adicionar namespaces | Sim | | | | | |
| | Exibir clusters e namespaces do Kubernetes | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Atividade - Solicitações | Excluir registros de solicitação de implantação | Sim | | | | | |
| | Exibir registros de solicitação de implantação | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Atividade - Logs de Eventos | Exibir logs de eventos | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Conexões - Contas de Nuvem | Criar, atualizar ou excluir contas de nuvem | Sim | | | | | |
| | Exibir contas de nuvem | Sim | Sim | | | | |
| Conexões - Integrações | Criar, atualizar ou excluir integrações | Sim | | | | | |
| | Visualizar integrações | Sim | Sim | | | | |
| Integração | Criar, atualizar ou excluir planos de integração | Sim | | | | | |
| | Visualizar planos de integração | Sim | Sim | | | Sim. Seus projetos | |
| Extensibilidade | | | | | | | |
| | Ver e abrir a guia Extensibilidade | Sim | Sim | | | Sim | |
| Eventos | Exibir eventos de extensibilidade | Sim | Sim | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|--|--|---------------------------------|------------------------------|--|--------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Assinaturas | Criar, atualizar ou excluir assinaturas de extensibilidade | Sim | | | | | |
| | Desativar assinaturas | Sim | | | | | |
| | Exibir assinaturas | Sim | Sim | | | | |
| Biblioteca - Tópicos de eventos | Exibir tópicos do evento | Sim | Sim | | | | |
| Biblioteca - Ações | Criar, atualizar ou excluir ações de extensibilidade | Sim | | | | | |
| | Exibir ações de extensibilidade | Sim | Sim | | | | |
| Biblioteca - Fluxos de trabalho | Exibir fluxos de trabalho de extensibilidade | Sim | Sim | | | | |
| Atividade - Execuções de ação | Cancelar ou excluir execuções de ação de extensibilidade | Sim | | | | | |
| | Exibir execuções de ação de extensibilidade | Sim | Sim | | | Sim. Seus projetos | |
| Atividade - Execuções de fluxo de trabalho | Exibir execuções de fluxo de trabalho de extensibilidade | Sim | Sim | | | | |
| Projetar | | | | | | | |
| Projetar | Abrir a guia Design | Sim | Sim | Sim. | Sim. | Sim. | Sim |
| Modelos de nuvem | Criar, atualizar e excluir modelos de nuvem | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|---|---------------------------------|------------------------------|---|--------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Visualizar modelos de nuvem | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| | Baixar modelos de nuvem | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| | Carregar modelos de nuvem | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| | Implantar modelos de nuvem | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| | Versão e restauração de modelos de nuvem | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| | Lançar modelos de nuvem no catálogo | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| Recursos Personalizados | Criar, atualizar ou excluir recursos personalizados | Sim | | | | | |
| | Visualizar recursos personalizados | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Ações Personalizadas | Criar, atualizar ou excluir ações personalizadas | Sim | | | | | |
| | Exibir ações personalizadas | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Recursos | | | | | | | |
| | Ver e abrir a guia Recursos | Sim | Sim | Sim | Sim | Sim | Sim |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|---|---------------------------------|------------------------------|--|---------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Implantações | Visualizar implantações, incluindo detalhes, histórico, preço, monitor, alertas, otimização e informações sobre solução de problemas | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| | Gerenciar alertas | Sim | | Sim. Seus projetos | Sim. seus projetos | | |
| | Executar ações de Dia 2 em implantações com base em políticas | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| Recursos - Todos os recursos | Exibir todos os recursos descobertos | Sim | Sim | | | | |
| | Execute ações de dia 2 nos recursos descobertos. Ações disponíveis apenas em máquinas e limitadas a ligar e desligar todas as máquinas e o console remoto das máquinas vSphere. | Sim | | | | | |
| Recursos - Todos os recursos | Exibir recursos implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|--|---------------------------------|------------------------------|--|---------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Executar ações de Dia 2 nos recursos implantados, integrados e migrados com base em políticas | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Máquinas virtuais | Exibir máquinas descobertas | Sim | Sim | | | | |
| | Execute ações de dia 2 nas máquinas descobertas. As ações estão limitadas a ligar e desligar e ao console remoto das máquinas vSphere. | Sim | | | | | |
| | Criar nova VM | Sim | | | | | |
| | Exibir recursos implantados, integrados e migrados. | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |
| | Executar ações de dia 2 nos recursos implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Volumes | Exibir volumes descobertos | Sim | Sim | | | | |
| | Nenhuma ação de dia 2 disponível | | | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|---|---------------------------------|------------------------------|--|---------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Exibir volumes implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |
| | Executar ações de dia 2 nos volumes implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Rede e segurança | Exibir redes descobertas, balanceadores de carga e grupos de segurança | Sim | Sim | | | | |
| | Nenhuma ação de dia 2 disponível | | | | | | |
| | Exibir redes, balanceadores de carga e grupos de segurança implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |
| | Executar ações de dia 2 em redes, balanceadores de carga e grupos de segurança implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Alertas | | | | | | | |

Tabela 3-2. Funções de serviço e funções de projeto do Cloud Assembly (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Cloud Assembly | Expectador do Cloud Assembly | Usuário do Cloud Assembly | | | |
|----------------------------------|----------------------------|---------------------------------|------------------------------|--|--------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador ou membro do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Ver e abrir a guia Alertas | Sim | Sim | Sim | Sim | Sim | |
| | Gerenciar alertas | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| | Visualizar alertas | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |

Funções de serviço do Service Broker

As funções de serviço do Service Broker determinam o que você pode ver e fazer no Service Broker. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 3-3. Descrições de funções de serviço do Service Broker

| Função | Descrição |
|---------------------------------|--|
| Administrador do Service Broker | É necessário ter acesso de leitura e gravação para toda a interface do usuário e recursos de API. Esta é a única função de usuário que pode executar todas as tarefas, incluindo a criação de um novo projeto e a atribuição de um administrador de projeto. |
| Usuário do Service Broker | Qualquer usuário que não tenha a função Administrador do Service Broker. Em um projeto Service Broker, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto. |
| Espectador do Service Broker | Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

Além das funções de serviço, o Service Broker tem funções de projeto. Todos os projetos estão disponíveis em todos os serviços.

As funções de projeto são definidas no Service Broker e podem variar entre projetos.

Nas tabelas a seguir, que indicam o que as diferentes funções de serviço e projeto podem ver e fazer, lembre-se de que os administradores de serviços têm permissão total em todas as áreas da interface do usuário.

Use as seguintes descrições de funções de projeto como ajuda para decidir quais permissões dar aos seus usuários.

- Os administradores de projetos aproveitam a infraestrutura criada pelo administrador de serviços para garantir que os membros do projeto tenham os recursos necessários para o trabalho de desenvolvimento.
- Os membros do projeto trabalham em seus projetos para projetar e implantar modelos de nuvem. Na tabela a seguir, Seus projetos podem incluir apenas os recursos que você possui ou os recursos compartilhados com outros membros do projeto.
- Os espectadores de projeto estão restritos ao acesso somente leitura.
- Os supervisores de projeto são aprovadores no Service Broker nos projetos em que uma política de aprovação é definida com um aprovador de supervisor de projeto. Para fornecer contexto ao supervisor para as aprovações, considere também conceder a ele a função de membro ou visualizador do projeto.

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker | | | |
|----------------------------------|--|---------------------------------|------------------------------|--|-------------------|-----------------------|-----------------------|
| | | | | O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| Acessar o Service Broker | | | | | | | |
| Console | No console, você pode ver e abrir o Service Broker | Sim | Sim | Sim | Sim | Sim | Sim |
| Infraestrutura | | | | | | | |
| | Visualizar e abrir a guia Infraestrutura | Sim | Sim | | | | |
| Configurar - Projetos | Criar projetos | Sim | | | | | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|--|---------------------------------|------------------------------|---|--------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Atualizar ou excluir valores do resumo do projeto, provisionamento, Kubernetes, integrações e testar configurações de projeto. | Sim | | | | | |
| | Adicionar usuários e grupos e atribuir funções em projetos. | Sim | | Sim. Seus projetos. | | | |
| | Visualizar projetos | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| Configurar - Zonas de Nuvem | Criar, atualizar ou excluir zonas de nuvem | Sim | | | | | |
| | Visualizar zonas de nuvem | Sim | Sim | | | | |
| Configurar - Zonas do Kubernetes | Criar, atualizar ou excluir zonas do Kubernetes | Sim | | | | | |
| | Exibir zonas do Kubernetes | Sim | Sim | | | | |
| Conexões - Contas de Nuvem | Criar, atualizar ou excluir contas de nuvem | Sim | | | | | |
| | Exibir contas de nuvem | Sim | Sim | | | | |
| Conexões - Integrações | Criar, atualizar ou excluir integrações | Sim | | | | | |
| | Visualizar integrações | Sim | Sim | | | | |
| Atividade - Solicitações | Excluir registros de solicitação de implantação | Sim | | | | | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|-----------------------------------|--|---------------------------------|------------------------------|---|-------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Exibir registros de solicitação de implantação | Sim | | | | | |
| Atividade - Logs de Eventos | Exibir logs de eventos | Sim | | | | | |
| Conteúdo e Políticas | | | | | | | |
| | Ver e abrir a guia Conteúdo e Políticas | Sim | Sim | | | | |
| Fontes de conteúdo | Criar, atualizar ou excluir fontes de conteúdo | Sim | | | | | |
| | Exibir fontes de conteúdo | Sim | Sim | | | | |
| Compartilhamento de Conteúdo | Adicionar ou remover conteúdo compartilhado | Sim | | | | | |
| | Exibir conteúdo compartilhado | Sim | Sim | | | | |
| Conteúdo | Personalizar o formulário e configurar o item | Sim | | | | | |
| | Visualizar conteúdo | Sim | Sim | | | | |
| Políticas – Definições | Criar, atualizar ou excluir definições de política | Sim | | | | | |
| | Exibir definições de política | Sim | Sim | | | | |
| Políticas – Aplicação | Exibir log de aplicação | Sim | Sim | | | | |
| Notificações - Servidor de E-mail | Configure um servidor de e-mail | Sim | | | | | |
| Catálogo | | | | | | | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|--|---------------------------------|------------------------------|---|--------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Ver e abrir a guia Catálogo | Sim | Sim | Sim | Sim | Sim | Sim |
| | Exibir itens de catálogo disponíveis | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| | Solicitar um item de catálogo | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| Recursos | | | | | | | |
| | Ver e abrir a guia Recursos | Sim | Sim | Sim. | Sim | Sim | Sim |
| Implantações | Visualizar implantações, incluindo detalhes de implantação, histórico de implantações, preço, monitor, alertas, otimização e informações de solução de problemas | Sim | Sim | Sim. Seus projetos | Sim. Seus projetos | Sim. Seus projetos | |
| | Gerenciar alertas | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| | Executar ações de Dia 2 em implantações com base em políticas | Sim | | Sim. Seus projetos | Sim. Seus projetos | | |
| Recursos - Todos os recursos | Exibir todos os recursos descobertos | Sim | Sim | | | | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|---|---------------------------------|------------------------------|---|---------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Execute ações de dia 2 nos recursos descobertos. Ações disponíveis apenas em máquinas e limitadas a ligar e desligar todas as máquinas e o console remoto das máquinas vSphere. | Sim | | | | | |
| Recursos - Todos os recursos | Exibir recursos implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |
| | Executar ações de Dia 2 nos recursos implantados, integrados e migrados com base em políticas | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Máquinas virtuais | Exibir máquinas descobertas | Sim | Sim | | | | |
| | Execute ações de dia 2 nas máquinas descobertas. As ações estão limitadas a ligar e desligar e ao console remoto das máquinas vSphere. | Sim | | | | | |
| | Criar nova VM | Sim | | | | | |
| | Exibir recursos implantados, integrados e migrados. | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|---|---------------------------------|------------------------------|---|---------------------|-----------------------|-----------------------|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Executar ações de dia 2 nos recursos implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Volumes | Exibir volumes descobertos | Sim | Sim | | | | |
| | Nenhuma ação de dia 2 disponível | | | | | | |
| | Exibir volumes implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |
| | Executar ações de dia 2 nos volumes implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Recursos - Rede e segurança | Exibir redes descobertas, balanceadores de carga e grupos de segurança | Sim | Sim | | | | |
| | Nenhuma ação de dia 2 disponível | | | | | | |
| | Exibir redes, balanceadores de carga e grupos de segurança implantados, integrados e migrados | Sim | Sim | Sim. Seus projetos. | Sim. Seus projetos. | Sim. Seus projetos. | |

Tabela 3-4. Funções de serviço e funções de projeto do Service Broker (continuação)

| Contexto da interface do usuário | Tarefa | Administrador do Service Broker | Espectador do Service Broker | Usuário do Service Broker O usuário deve ser administrador do projeto para ver e realizar tarefas relacionadas ao projeto. | | | |
|----------------------------------|---|---------------------------------|------------------------------|---|--|--|--|
| | | | | Administrador do projeto | Membro do projeto | Expectador de projeto | Supervisor de projeto |
| | Executar ações de dia 2 em redes, balanceadores de carga e grupos de segurança implantados, integrados e migrados com base em políticas | Sim | | Sim. Seus projetos. | Sim. Seus projetos. | | |
| Aprovações | | | | | | | |
| | Ver e abrir a guia Aprovações | Sim | Sim | Sim | Sim | Sim | Sim |
| | Responder a solicitações de aprovação | Sim | | Sim. Seus projetos e o aprovador da política é o Administrador do Projeto | Somente se você for um aprovador nomeado | Somente se você for um aprovador nomeado | Sim. Seus projetos e o aprovador da política é o Supervisor do Projeto |

Funções de serviço do Code Stream

As funções de serviço do Code Stream determinam o que você pode ver e fazer no Code Stream. Essas funções são definidas no console pelo proprietário da organização. Todos os projetos estão disponíveis em todos os serviços.

Tabela 3-5. Descrição das funções de serviço do Code Stream

| Função | Descrição |
|------------------------------|--|
| Administrador do Code Stream | Um usuário que tenha acesso de leitura e gravação para toda a interface do usuário e recursos de API. Essa é a única função de usuário que pode ver e fazer tudo, inclusive criar projetos, integrar endpoints, adicionar acionadores, criar pipelines e painéis personalizados, marcar endpoints e variáveis como recursos restritos, executar pipelines que usam recursos restritos e solicitar que os pipelines sejam publicados no Service Broker. |
| Desenvolvedor do Code Stream | Um usuário que pode trabalhar com pipelines, mas não pode trabalhar com variáveis ou endpoints restritos. Se um pipeline incluir uma variável ou endpoint restrito, esse usuário deverá obter aprovação para a tarefa de pipeline que usa a variável ou o endpoint restrito. |

Tabela 3-5. Descrição das funções de serviço do Code Stream (continuação)

| Função | Descrição |
|---------------------------|---|
| Executor do Code Stream | Um usuário que pode executar pipelines e aprovar ou recusar tarefas de operação do usuário. Esse usuário pode retomar, pausar e cancelar execuções de pipeline, mas não pode modificar pipelines. |
| Usuário do Code Stream | Um usuário que pode acessar o Code Stream, mas não tem nenhum outro privilégio no Code Stream. |
| Espectador do Code Stream | Um usuário que tem acesso de leitura para ver pipelines, endpoints, execuções de pipelines e painéis, mas não pode criá-los, atualizá-los nem excluí-los. Um usuário que também tem a função de Visualizador de serviços pode ver todas as informações disponíveis ao administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

Além das funções de serviço, o Code Stream tem funções de projeto. Todos os projetos estão disponíveis em todos os serviços.

As funções de projeto são definidas no Code Stream e podem variar entre projetos.

Nas tabelas a seguir, que informam o que as diferentes funções de serviço e projeto podem ver e fazer, lembre-se de que os administradores de serviços têm permissão total em todas as áreas da interface do usuário.

Use as seguintes descrições de funções do projeto para ajudar você a decidir quais permissões devem ser conferidas aos seus usuários.

- Os administradores de projetos aproveitam a infraestrutura criada pelo administrador de serviços para garantir que os membros do projeto tenham os recursos necessários para o trabalho de desenvolvimento. O administrador do projeto pode adicionar membros.
- Os membros do projeto que têm uma função de serviço podem usar os serviços.
- Os visualizadores de projeto podem ver projetos, mas não podem criá-los, atualizá-los nem excluí-los.

Todas as ações, exceto as restritas significa que essa função tem permissão para executar ações de criação, leitura, atualização e exclusão em entidades, exceto para variáveis restritas e endpoints.

Tabela 3-6. Recursos de funções de serviço do Code Stream

| Contexto da interface do usuário | Recursos | Função Administrador do Code Stream | Função Desenvolvedor do Code Stream | Função Executor do Code Stream | Função Espectador do Code Stream | Função Usuário do Code Stream |
|----------------------------------|------------------|-------------------------------------|-------------------------------------|--------------------------------|----------------------------------|-------------------------------|
| Pipelines | | | | | | |
| | Exibir pipelines | Sim | Sim | Sim | Sim | |

Tabela 3-6. Recursos de funções de serviço do Code Stream (continuação)

| Contexto da interface do usuário | Recursos | Função Administrador do Code Stream | Função Desenvolvedor do Code Stream | Função Executor do Code Stream | Função Expectador do Code Stream | Função Usuário do Code Stream |
|-----------------------------------|--|-------------------------------------|-------------------------------------|--------------------------------|----------------------------------|-------------------------------|
| | Criar pipelines | Sim | Sim | | | |
| | Executar pipelines | Sim | Sim | Sim | | |
| | Executar pipelines que incluem variáveis ou endpoints restritos | Sim | | | | |
| | Atualizar pipelines | Sim | Sim | | | |
| | Excluir pipelines | Sim | Sim | | | |
| Execução de Pipeline | | | | | | |
| | Exibir execuções de pipeline | Sim | Sim | Sim | Sim | |
| | Retomar, pausar e cancelar execuções de pipeline | Sim | Sim | Sim | | |
| | Retomar pipelines que pararam para aprovação em recursos restritos | Sim | | | | |
| Integrações Personalizadas | | | | | | |
| | Criar integrações personalizadas | Sim | Sim | | | |
| | Ler integrações personalizadas | Sim | Sim | Sim | Sim | |
| | Atualizar integrações personalizadas | Sim | Sim | | | |
| Endpoints | | | | | | |

Tabela 3-6. Recursos de funções de serviço do Code Stream (continuação)

| Contexto da interface do usuário | Recursos | Função Administrador do Code Stream | Função Desenvolvedor do Code Stream | Função Executor do Code Stream | Função Expectador do Code Stream | Função Usuário do Code Stream |
|--|--|-------------------------------------|-------------------------------------|--------------------------------|----------------------------------|-------------------------------|
| | Exibir execuções | Sim | Sim | Sim | Sim | |
| | Criar execuções | Sim | Sim | | | |
| | Atualizar execuções | Sim | Sim | | | |
| | Excluir execuções | Sim | Sim | | | |
| Marcar os recursos como restritos | | | | | | |
| | Marcar uma variável ou um endpoint como restrito | Sim | | | | |
| Painéis | | | | | | |
| | Exibir painéis | Sim | Sim | Sim | Sim | |
| | Criar painéis | Sim | Sim | | | |
| | Atualizar painéis | Sim | Sim | | | |
| | Excluir painéis | Sim | Sim | | | |

Funções de serviço do vRA Migration Assistant

As funções de serviço do vRA Migration Assistant determinam o que você pode ver e fazer no vRA Migration Assistant e no Cloud Assembly. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 3-7. Descrições das funções do serviço do vRealize Automation Migration Assistant

| Função | Descrição |
|---|--|
| Administrador do assistente de migração | Um usuário que tem privilégios de visualização completa, atualização e exclusão no vRA Migration Assistant e no Cloud Assembly. Essa função também deve ter pelo menos a função de visualizador do Cloud Assembly. |
| Visualizador do assistente de migração | Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores no vRA Migration Assistant ou no Cloud Assembly. Essa função também deve ter pelo menos a função de visualizador do Cloud Assembly. |

Funções de serviço do Orchestrator

As funções de serviço do Orchestrator determinam o que você pode ver e fazer no vRealize Orchestrator Client. Essas funções de serviço são definidas no console por um proprietário da organização.

Tabela 3-8. Descrições das funções do serviço do vRealize Orchestrator

| Função | Descrição |
|---|--|
| Administrador do Orchestrator | Um usuário que tem privilégios completos de visualização, atualização e exclusão no vRealize Orchestrator. Um administrador também pode acessar o conteúdo criado por grupos específicos. |
| Orchestrator Viewer | Um usuário que tem acesso de leitura para ver recursos e conteúdo, incluindo todos os grupos e conteúdo do grupo, mas não pode criar, atualizar, executar, excluir valores ou exportar conteúdo. |
| Designer de fluxo de trabalho do Orchestrator | Um usuário que pode criar, executar, editar e excluir seu próprio conteúdo do vRealize Orchestrator Client. Ele pode adicionar seu próprio conteúdo ao grupo atribuído. O designer de fluxo de trabalho não tem acesso aos recursos de administração e solução de problemas do vRealize Orchestrator Client. |

Função de serviço do SaltStack Config

A função de serviço do SaltStack Config determina o que você pode ver e fazer no vRealize Automation. Essa função de serviço é definida no console por um proprietário da organização.

Tabela 3-9. Descrição da função do serviço de configuração do vRealize Automation SaltStack Config

| Função | Descrição |
|-----------------------------------|---|
| Administrador do SaltStack Config | Um usuário que pode acessar o bloco SaltStack Config no console quando a integração com o Cloud Assembly está configurada. Para fazer login na instância do SaltStack Config, o usuário deve ter permissões de administrador do SaltStack, que são definidas no SaltStack Config. O usuário também deve ter a função de Administrador do Cloud Assembly. |

Personalizar funções de usuário no vRealize Automation

Como administrador do Cloud Assembly, você pode criar funções personalizadas que definem o que os usuários podem ver e fazer no vRealize Automation. Em seguida, você pode atribuir usuários a essas funções.

Permissões de função de usuário personalizada

Usando o Cloud Assembly, você pode definir funções de usuário mais detalhadas e, em seguida, atribuir usuários a essas funções. As funções personalizadas têm duas categorias: visualizar e gerenciar.

- **Visualizar.** Um usuário atribuído a uma função com essa permissão pode ver todos os itens de todos os projetos nas seções selecionadas da interface do usuário. Essa função é útil para os usuários que precisam ver contas, configurações ou valores atribuídos.
- **Gerenciar.** Um usuário atribuído a uma função com essa permissão pode ver todos os itens e tem permissões totais para adicionar, editar e excluir permissões em todos os projetos nas seções selecionadas da interface do usuário.

Essas permissões estendem os privilégios concedidos pelas outras funções e não são restritas pela associação do projeto. Por exemplo, você pode expandir as permissões de um administrador de projeto para gerenciar partes da infraestrutura ou dar a um visualizador de serviço a capacidade de analisar e responder às solicitações de aprovação.

Para definir as funções do usuário e atribuir usuários, abra Cloud Assembly ou Service Broker como administrador de serviço e selecione **Infraestrutura > Administração > Funções personalizadas**. Não é possível configurar as funções personalizadas no Code Stream; no entanto, as funções se aplicam a todos os serviços.

Tabela 3-10. Funções personalizadas

| Interface do usuário | Permissão | Descrição |
|-----------------------|-----------------------------|-----------------------------|
| Infraestrutura | | |
| | Visualizar contas de nuvem. | Visualizar contas de nuvem. |

Tabela 3-10. Funções personalizadas (continuação)

| Interface do usuário | Permissão | Descrição |
|----------------------|----------------------------------|---|
| | Gerenciar contas de nuvem | Criar, atualizar ou excluir contas de nuvem. |
| | Visualizar mapeamentos de imagem | Visualizar mapeamentos de imagem. |
| | Gerenciar mapeamentos de imagem | Criar, atualizar ou excluir mapeamentos de imagem. |
| | Visualizar mapeamentos de tipo | Visualizar mapeamentos de tipo. |
| | Gerenciar mapeamentos de tipo | Criar, atualizar ou excluir mapeamentos de tipo. |
| | Visualizar zonas de nuvem | Visualizar zonas de nuvem, insights e alertas. |
| | Gerenciar zonas de nuvem | Criar, atualizar ou excluir zonas de nuvem. Gerenciar alertas. |
| | Visualizar solicitações | Visualizar solicitações de atividade. |
| | Gerenciar solicitações | Excluir solicitações da lista. |
| | Visualizar integrações | Visualizar integrações. |
| | Gerenciar integrações | Criar, atualizar ou excluir integrações. |
| | Visualizar projetos | Visualizar projetos. |
| | Gerenciar projetos | Criar projetos. Adicionar usuários e atribuir funções em projetos. Atualizar ou excluir valores do resumo do projeto, usuários, provisionamento, Kubernetes, integrações e testar configurações de projeto. |
| | Visualizar planos de integração | Visualizar planos de integração |
| | Gerenciar planos de integração | Criar, atualizar, executar ou excluir planos de integração |
| Catálogo | | |
| | Visualizar conteúdo | |
| | Gerenciar conteúdo | Adicionar, atualizar, excluir fontes de conteúdo. Compartilhar conteúdo. Personalizar o conteúdo, incluindo ícones de catálogo e formulários de solicitação. |
| Políticas | | |
| | Visualizar políticas | Visualizar definições de política. |

Tabela 3-10. Funções personalizadas (continuação)

| Interface do usuário | Permissão | Descrição |
|-------------------------|--|--|
| | Gerenciar políticas | Criar, atualizar ou excluir definições de política. |
| Implantações | | |
| | Visualizar implantações | Visualizar todas as implantações, incluindo detalhes de implantação, histórico de implantações, alertas e informações sobre solução de problemas. |
| | Gerenciar implantações | Visualizar todas as implantações, responder a alertas e executar todas as ações de dia 2 que as políticas do dia 2 permitem que um administrador execute em implantações e componentes de implantação. |
| Modelos de Nuvem | | |
| | Visualizar modelos de nuvem | Visualizar modelos de nuvem. |
| | Gerenciar modelos de nuvem | Criar, atualizar, testar, excluir, controlar versão, compartilhar modelos de nuvem e liberar/cancelar a liberação de uma versão de modelo de nuvem. |
| | Editar modelos de nuvem | Criar, atualizar, testar, controlar versão, compartilhar modelos de nuvem e lançar/cancelar lançamento de uma versão de modelo de nuvem. A função não tem permissão para excluir modelos de nuvem. |
| | Implantar modelos de nuvem | Testar e implementar qualquer modelo de nuvem em qualquer projeto. |
| | Implantar conteúdo de modelo de nuvem em linha | Implantar qualquer modelo de nuvem nos projetos aos quais os responsáveis estão associados. As funções do projeto podem ser de administrador, membro ou visualizador. |
| XaaS | | |
| | Visualizar recursos personalizados | Visualizar recursos personalizados. |
| | Gerenciar recursos personalizados | Criar, atualizar ou excluir recursos personalizados. |
| | Visualizar ações de recursos | Visualizar ações personalizadas. |

Tabela 3-10. Funções personalizadas (continuação)

| Interface do usuário | Permissão | Descrição |
|------------------------|--------------------------------------|--|
| | Gerenciar ações de recursos | Criar, atualizar ou excluir ações personalizadas |
| Extensibilidade | | |
| | Visualizar recursos extensibilidade | Visualizar eventos, inscrições, tópicos de eventos, ações, fluxos de trabalho, execuções de ação e fluxos de trabalho. |
| | Gerenciar recursos extensibilidade | Criar, atualizar, excluir e desativar assinaturas de extensibilidade. Criar, atualizar ou excluir ações de extensibilidade. Cancelar ou excluir execuções de ação de extensibilidade. |
| Pipeline | | |
| | Gerenciar Pipelines | Criar, editar e excluir as configurações de pipeline, endpoint, variável e acionador. Os modelos restritos estão excluídos. |
| | Gerenciar Pipelines Restritos | Criar, editar e excluir as configurações de pipeline, endpoint, variável e acionador. Os modelos restritos estão incluídos. |
| | Gerenciar integrações personalizadas | Adicionar, editar e excluir integrações personalizadas. |
| | Executar Pipelines | Executar execuções e acionadores de modelos de pipeline, e pausar, cancelar, retomar ou executar novamente as execuções e os acionadores. |
| | Executar Pipelines Restritos | Executar execuções e acionadores de modelos de pipeline, e pausar, cancelar, retomar ou executar novamente as execuções e os acionadores. Resolver variáveis e endpoints restritos. |
| | Gerenciar execuções | Executar execuções e acionadores de modelos de pipeline, e pausar, cancelar, retomar ou executar novamente as execuções e os acionadores. Resolver variáveis e endpoints restritos. Excluir execuções. |

Tabela 3-10. Funções personalizadas (continuação)

| Interface do usuário | Permissão | Descrição |
|----------------------|----------------------|---|
| Aprovação | | |
| | Gerenciar aprovações | <p>Visualizar a guia Aprovações, onde é possível aprovar ou recusar solicitações de aprovação.</p> <p>O aprovador com essa função não receberá notificações por e-mail sobre uma solicitação de aprovação, a menos que seja um aprovador na política.</p> |

Casos de uso: Como funções de usuário podem me ajudar a controlar o acesso no vRealize Automation

Como administrador de nuvem, você deseja controlar as tarefas que os seus usuários podem realizar no vRealize Automation. Dependendo dos seus objetivos de gerenciamento e das responsabilidades da equipe de desenvolvimento de aplicativos, há diferentes maneiras de configurar funções de usuário para oferecer suporte a esses objetivos.

Os seguintes exemplos do Cloud Assembly e do Service Broker são baseados em três casos de uso. Esses exemplos fornecem apenas instruções suficientes para ilustrar a aplicação das funções de usuário.

O público-alvo desses casos de uso é o administrador da nuvem, que também é considerado o administrador da nuvem, e os administradores de serviços.

Os casos de uso se complementam. Se você estiver pronto para ir diretamente ao caso de uso 3, pode ser necessário revisar os casos de uso 1 e 2 para entender melhor por que as funções devem ser configuradas das maneiras especificadas.

O objetivo dos casos de uso é demonstrar funções de usuário, e não fornecer informações detalhadas sobre como configurar sua infraestrutura, gerenciar projetos, criar modelos de nuvem e trabalhar com implantações.

Antes de começar, você deve entender os níveis de funções de usuário que são configurados por um administrador de nuvem no console do vRealize Automation.

■ Funções de organização

As funções de organização controlam quem pode acessar o console.

Como proprietário de uma organização, você deve garantir que todos os usuários de qualquer um dos serviços tenham pelo menos uma função de membro da organização atribuída.

| Função | Descrição |
|-----------------------------|---|
| Proprietário da Organização | Um administrador pode adicionar usuários, alterar a função dos usuários e remover usuários da organização. O proprietário gerencia a quais serviços os usuários têm acesso. |
| Membro da Organização | Um usuário geral pode fazer login no console da organização. Para acessar os serviços, um proprietário da organização deve designar as funções de serviço dos usuários. |

■ Funções de serviço

As funções de serviço controlam quem pode acessar seus serviços atribuídos.

Como proprietário da organização, você deve garantir que os usuários que precisam de acesso aos serviços tenham a função apropriada. Você usa as funções para controlar o quanto o usuário pode fazer em cada serviço.

Tabela 3-11. Descrições das funções de serviço do Cloud Assembly

| Função | Descrição |
|---------------------------------|--|
| Administrador do Cloud Assembly | Um usuário que tenha acesso de leitura e gravação para toda a interface do usuário e recursos de API. Essa é a única função de usuário que pode ver e fazer tudo, incluindo adicionar contas de nuvem, criar novos projetos e atribuir um administrador de projeto. |
| Usuário do Cloud Assembly | Um usuário que não tem a função Administrador do Cloud Assembly. Em um projeto Cloud Assembly, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto. |
| Expectador do Cloud Assembly | Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. Esta é uma função somente leitura em todos os projetos. Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

Tabela 3-12. Descrições de funções de serviço do Service Broker

| Função | Descrição |
|---------------------------------|---|
| Administrador do Service Broker | É necessário ter acesso de leitura e gravação para toda a interface do usuário e recursos de API. Esta é a única função de usuário que pode executar todas as tarefas, incluindo a criação de um novo projeto e a atribuição de um administrador de projeto. |
| Usuário do Service Broker | Qualquer usuário que não tenha a função Administrador do Service Broker. Em um projeto Service Broker, o administrador adiciona usuários a projetos como membros, administradores ou visualizadores do projeto. O administrador também pode adicionar um administrador de projeto. |
| Espectador do Service Broker | Um usuário que tem acesso de leitura para ver informações, mas não pode criar, atualizar ou excluir valores. |

Tabela 3-12. Descrições de funções de serviço do Service Broker (continuação)

| Função | Descrição |
|--------|--|
| | Os usuários com a função de visualizador podem ver todas as informações que estão disponíveis para o administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

Tabela 3-13. Descrição das funções de serviço do Code Stream

| Função | Descrição |
|------------------------------|---|
| Administrador do Code Stream | Um usuário que tenha acesso de leitura e gravação para toda a interface do usuário e recursos de API. Essa é a única função de usuário que pode ver e fazer tudo, inclusive criar projetos, integrar endpoints, adicionar acionadores, criar pipelines e painéis personalizados, marcar endpoints e variáveis como recursos restritos, executar pipelines que usam recursos restritos e solicitar que os pipelines sejam publicados no Service Broker. |
| Desenvolvedor do Code Stream | Um usuário que pode trabalhar com pipelines, mas não pode trabalhar com variáveis ou endpoints restritos. Se um pipeline incluir uma variável ou endpoint restrito, esse usuário deverá obter aprovação para a tarefa de pipeline que usa a variável ou o endpoint restrito. |
| Executor do Code Stream | Um usuário que pode executar pipelines e aprovar ou recusar tarefas de operação do usuário. Esse usuário pode retomar, pausar e cancelar execuções de pipeline, mas não pode modificar pipelines. |
| Usuário do Code Stream | Um usuário que pode acessar o Code Stream, mas não tem nenhum outro privilégio no Code Stream. |
| Espectador do Code Stream | Um usuário que tem acesso de leitura para ver pipelines, endpoints, execuções de pipelines e painéis, mas não pode criá-los, atualizá-los nem excluí-los. Um usuário que também tem a função de Visualizador de serviços pode ver todas as informações disponíveis ao administrador. Ele não pode realizar nenhuma ação, a menos que você o torne um administrador de projeto ou membro do projeto. Se o usuário for afiliado a um projeto, ele terá as permissões relacionadas à função. A função de visualizador de projeto não abrange as permissões da mesma forma que a função de administrador ou membro. |

- Funções de associação ao projeto

A associação ao projeto determina quais recursos de infraestrutura e modelos de nuvem estão disponíveis.

A associação ao projeto é definida no serviço por um usuário com função de administrador de serviço. O administrador de serviço deve garantir que os usuários que precisam de acesso a um ou mais projetos recebam a função de projeto apropriada em cada projeto.

Tabela 3-14. Funções de projeto

| Função | Descrição |
|--------------------------|---|
| Administrador do projeto | Um administrador de projeto pode gerenciar seus próprios projetos, criar e implantar modelo de nuvem associados a seus projetos e gerenciar implantações de projeto para todos os membros do projeto. |
| Membro do projeto | Um membro do projeto pode criar e implantar modelos de nuvem associados a seus projetos, gerenciar suas próprias implantações e gerenciar quaisquer implantações compartilhadas. |
| Expectador de projeto | Um espectador de projeto é um membro do projeto com acesso somente leitura a seus recursos de projeto, modelos de nuvem e implantações. |

■ Funções personalizadas

As funções personalizadas são criadas pelo Cloud Assembly para refinar as funções de membro e de visualizador.

Os procedimentos fornecidos nesses casos de uso têm como objetivo destacar as funções de usuário. Eles não são procedimentos detalhados ou definitivos para a configuração do vRealize Automation.

Ao configurar as funções, lembre-se de que os usuários que estão executando as operações de API estão sujeitos às funções que aqui atribuídas.

Pré-requisitos

- Verifique se você tem a função Proprietário da Organização. Você deve ver a guia **Gerenciamento de Identidade e Acesso** ao fazer login no console. Se ela não estiver visível, entre em contato com o proprietário da organização.
- Verifique se você tem a função de administrador de serviço para os vários serviços. Se não tiver certeza sobre sua função, entre em contato com o proprietário da organização.
- Verifique se os seus usuários foram adicionados ao vRealize Automation.

Quando você instala o vRealize Automation, seus usuários do Active Directory são adicionados como parte do processo.

- Para uma lista de tarefas e funções mais detalhadas para várias funções, consulte [Organização e funções de usuário de serviço no vRealize Automation](#).

Procedimentos

1 Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos

Como administrador de nuvem do vRealize Automation, você é responsável por gerenciar o acesso e o orçamento dos seus recursos de infraestrutura. Você adiciona a si mesmo e outros dois usuários como administradores. Essa pequena equipe pode criar a infraestrutura e desenvolver os modelos de nuvem que correspondem aos objetivos de negócios das equipes que consomem esses modelos de nuvem. Você e sua pequena equipe de administradores implantam então os modelos de nuvem para os consumidores que não são administradores. Você não permite que os não administradores acessem o vRealize Automation.

2 Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo

Como um proprietário de organização do vRealize Automation, você é responsável por gerenciar o acesso e o orçamento dos seus recursos de infraestrutura. Você tem uma equipe de desenvolvedores de modelo de nuvem que criam e implementam modelos iterativamente para diferentes projetos, até que eles estejam prontos para serem entregues aos consumidores. Em seguida, você distribui os recursos implantáveis para os consumidores em um catálogo.

3 Caso de uso de função de usuário 3: Configurar funções de usuário personalizadas no vRealize Automation para refinar as funções do sistema

Como proprietário da organização ou administrador de serviços do vRealize Automation, você gerencia o acesso dos usuários usando as funções da organização e do sistema de serviço. No entanto, você também deseja criar funções personalizadas para os usuários selecionados e realizar tarefas ou ver conteúdo que está fora das funções deles no sistema.

Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos

Como administrador de nuvem do vRealize Automation, você é responsável por gerenciar o acesso e o orçamento dos seus recursos de infraestrutura. Você adiciona a si mesmo e outros dois usuários como administradores. Essa pequena equipe pode criar a infraestrutura e desenvolver os modelos de nuvem que correspondem aos objetivos de negócios das equipes que consomem esses modelos de nuvem. Você e sua pequena equipe de administradores implantam então os modelos de nuvem para os consumidores que não são administradores. Você não permite que os não administradores acessem o vRealize Automation.

Neste caso de uso, você é o proprietário da organização e tem uma pequena equipe em que todos têm a função de administrador de serviço.

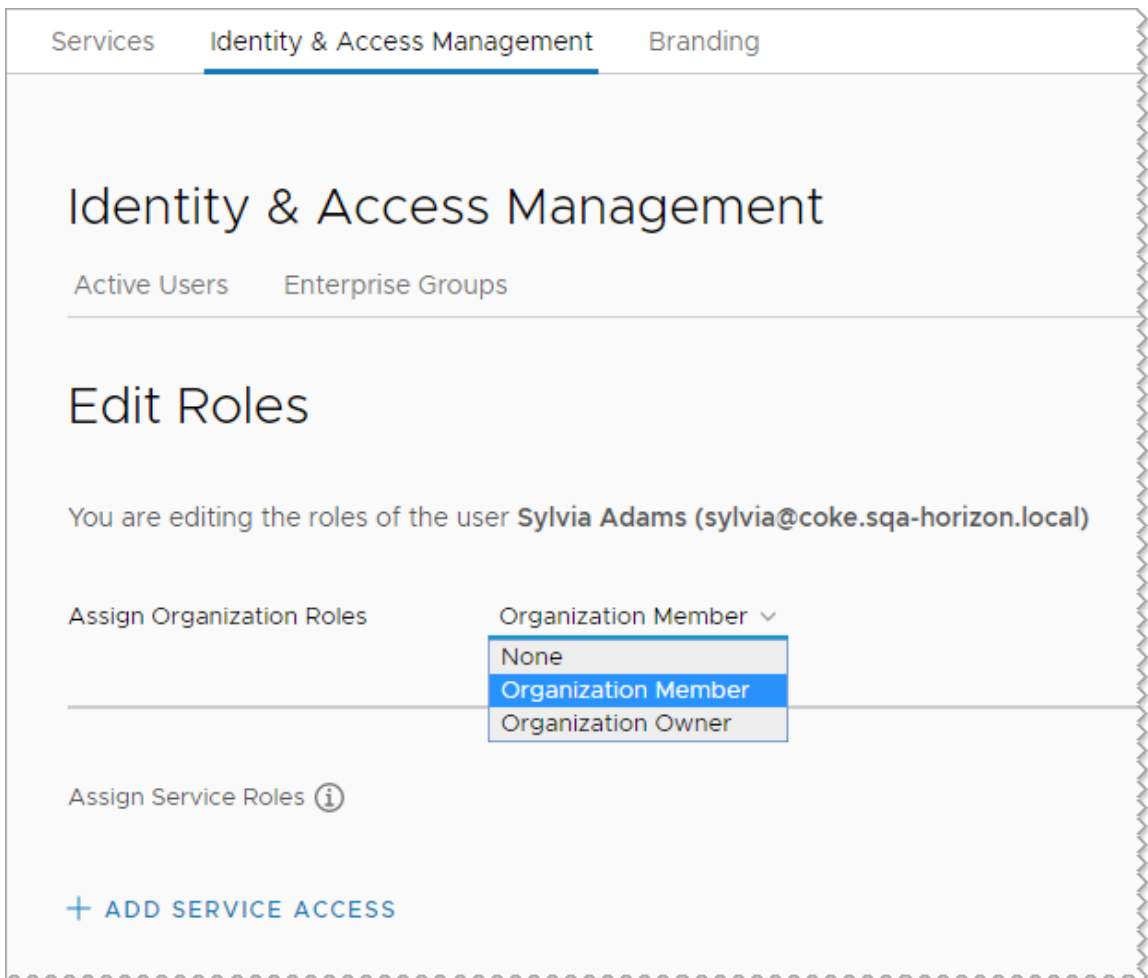
O procedimento a seguir acompanha um usuário durante todo o processo. Você pode executar cada etapa para vários usuários.

Pré-requisitos

- Verifique se você atende a todos os pré-requisitos estipulados na introdução do caso de uso. Consulte [Casos de uso: Como funções de usuário podem me ajudar a controlar o acesso no vRealize Automation](#).

Procedimentos

- 1 Atribua funções de organização. Clique em **Gerenciamento de Identidade e Acesso**.
 - a Faça login no console do vRealize Automation.
 - b Clique em **Gerenciamento de Identidade e Acesso**.
 - c Selecione o nome do usuário e clique em **Editar Funções**.
 - d No menu suspenso **Atribuir Funções da Organização**, selecione **Membro da Organização**.



A função de membro da organização garante que o usuário possa acessar o console e quaisquer serviços aos quais você o adicione. Eles não podem gerenciar usuários da organização.

Deixe a página Editar Função aberta para esse usuário e prossiga para a próxima etapa.

- 2 Atribua a função Administrador do Cloud Assembly a você mesmo e a um ou dois outros administradores neste cenário.

A função de administrador de serviço tem privilégios totais para adicionar, editar e excluir infraestruturas, projetos, modelo de nuvem e implantações. A definição de uma função de administrador para uma pessoa e a função de usuário para uma pessoa diferente é abordada no Cenário 2. Este exemplo usa Sylvia.

- a Clique em **Adicionar Acesso ao Serviço**.
- b Configure o usuário com o seguinte valor.

| Serviço | Função |
|----------------|---------------------------------|
| Cloud Assembly | Administrador do Cloud Assembly |

[Services](#)
[Identity & Access Management](#)
[Branding](#)

Identity & Access Management

[Active Users](#) [Enterprise Groups](#)

Edit Roles

You are editing the roles of the user **Sylvia Adams** (sylvia@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Cloud Assembly ▾
with roles
Cloud Assembly Administrator ▾
×

[+ ADD SERVICE ACCESS](#)

SAVE
CANCEL

- 3 Crie um projeto no Cloud Assembly que você usa para agrupar recursos e gerenciar o faturamento de recursos para diferentes grupos comerciais.

- a No console, clique na guia **Serviços** e depois em **Cloud Assembly**.
- b Selecione **Infraestrutura > Projetos > Novo Projeto**.

Este caso de uso de função de usuário se concentra em fornecer exemplos de como você pode implementar funções de usuário, e não na criação de um sistema totalmente definido.

Para obter informações sobre como configurar a infraestrutura, consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#). Para obter mais informações sobre projetos, consulte [Capítulo 5 Como adicionar e gerenciar projetos do Cloud Assembly](#).

- c Insira **WebAppTeam** como o nome do projeto.
- d Clique em **Usuários** e depois em **Adicionar Usuários**.
- e Insira os endereços de e-mail das pessoas que podem ajudá-lo a construir e gerenciar a infraestrutura e os modelos de nuvem.

Por exemplo, tony@mycompany.com, syliva@mycompany.com.

- f No menu suspenso **Atribuir função**, selecione **Administrador**.

Como administradores do Cloud Assembly, esses dois usuários já têm acesso de administrador às contas de nuvem, à infraestrutura e a todos os projetos. Essa etapa ajuda a compreender as funções usadas nos cenários posteriores. Nos últimos cenários, você definiu as funções de administrador e membro do projeto, que têm permissões diferentes.

- g Clique na guia **Provisionamento** e adicione uma ou mais zonas de nuvem.

Outro lembrete. Este caso de uso é sobre funções de usuário.

4 Desenvolva um modelo de nuvem simples para que possa testar o projeto WebAppTeam.

Esta seção de modelo de nuvem é abreviada. O foco são os usuários e as funções de usuário conforme definido por projetos, e não como criar um modelo de nuvem.

- a Selecione **Modelos de Nuvem > Novo**.
- b Para o novo nome do modelo de nuvem, insira **WebApp**.
- c Para **Projeto**, selecione WebAppTeam.

New Cloud Template

Name * WebApp

Description

Project * WebAppTeam

Cloud template sharing in Service Broker

☒ Share only with this project

☐ Allow an administrator to share with any project in this organization

CANCEL CREATE

- d Selecione **Compartilhar apenas com o projeto**.

Essa configuração garante que o modelo de nuvem esteja disponível apenas para membros do projeto. Quando estiver pronto para fornecer os modelos de nuvem para outras equipes, você poderá selecionar Permitir que um administrador compartilhe com qualquer projeto nesta organização. Compartilhar o modelo de nuvem com outros projetos significa que você não precisa manter instâncias duplicadas dos mesmos modelos de base. Você pode mover modelos de nuvem de projetos de desenvolvimento para projetos de produção, para que os consumidores do catálogo possam implantar em recursos de infraestrutura de produção.

- e Clique em **Criar**.
- f No designer do modelos de nuvem, arraste o componente **Máquina > Independente de Nuvem** até a tela.

Para obter mais informações sobre como configurar modelos de nuvem, consulte [Capítulo 6 Como projetar suas implantações do Cloud Assembly](#).

- g Clique em **Implantar**.
- h Continue iterando no modelo de nuvem até que você esteja pronto para fornecê-lo aos seus consumidores.
- i Clique em **Versão** e lance a versão do modelo de nuvem.

5 Envie aos usuários as informações de login usando o método mais comum.

Resultados

Neste caso de uso, você designou dois colegas como membros da organização. Em seguida, você nomeou Sylvia como administradora do Cloud Assembly. Você nomeou Tony como administrador de projetos do WebApp. Essa configuração de função de usuário funciona apenas para pequenas equipes nas quais você entrega aplicativos implantados a seus consumidores, em vez de fornecer a eles acesso via autoatendimento ou um catálogo.

Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo

Como um proprietário de organização do vRealize Automation, você é responsável por gerenciar o acesso e o orçamento dos seus recursos de infraestrutura. Você tem uma equipe de desenvolvedores de modelo de nuvem que criam e implementam modelos iterativamente para diferentes projetos, até que eles estejam prontos para serem entregues aos consumidores. Em seguida, você distribui os recursos implantáveis para os consumidores em um catálogo.

Este caso de uso pressupõe que você entenda que o caso de uso 1 é um caso de uso apenas para administradores. Agora, você deseja expandir o sistema para oferecer suporte a mais equipes e metas maiores.

- Deixe os desenvolvedores criarem e implantarem seus próprios modelos de nuvem de aplicativos durante o desenvolvimento. Você se adiciona como administrador e, em seguida, adiciona outros usuários com a função de usuário do serviço e espectador do serviço. Em seguida, você adiciona os usuários como membros do projeto. Os membros do projeto podem desenvolver e implantar seus próprios modelos de nuvem.
- Publique modelos de nuvem em um catálogo no qual você os disponibiliza para implantação por usuários não desenvolvedores. Agora, você está atribuindo funções de usuário para o Service Broker. O Service Broker fornece um catálogo para os consumidores do modelo de nuvem. Você também pode usá-lo para criar políticas, incluindo concessões e direitos, mas essa funcionalidade não faz parte deste caso de uso de função de usuário.

Pré-requisitos

- Reveja o primeiro caso de uso. Consulte [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).
- Identifique os seguintes usuários com base nas permissões que você deseja que eles tenham:
 - desenvolvedores de modelos de nuvem que serão usuários e expectadores do Cloud Assembly
 - Um administrador do Service Broker
 - Usuários não desenvolvedores, que serão consumidores de catálogo como usuários do Service Broker

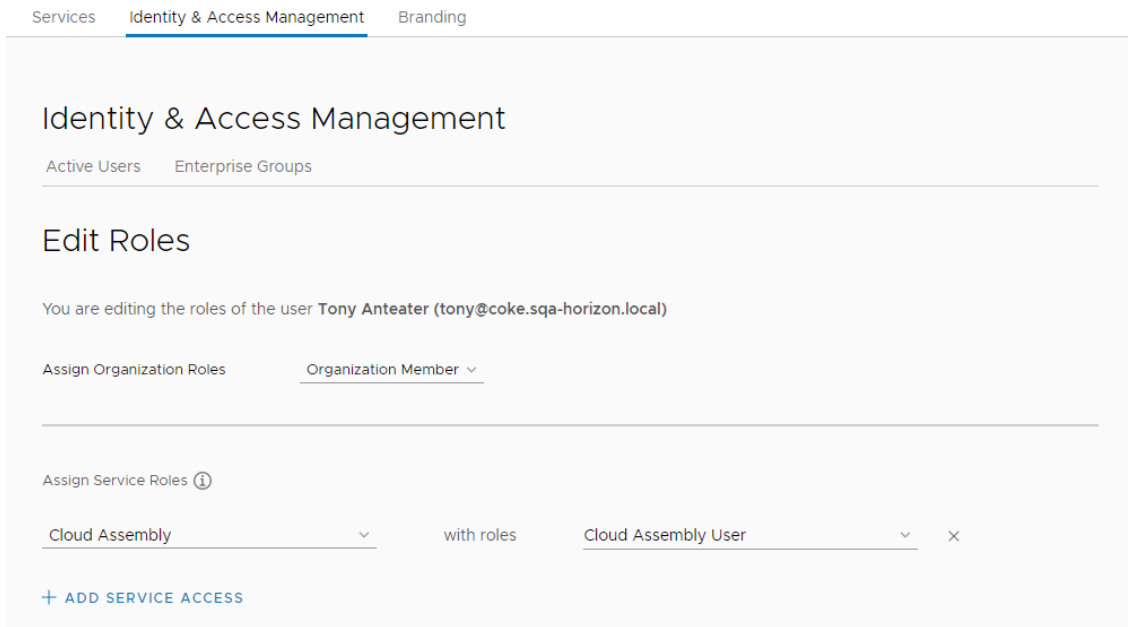
Procedimentos

- 1 Atribua funções de membro da organização aos seus usuários desenvolvedores de modelo de nuvem.

Se precisar de instruções, consulte o [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).

- 2 Atribua a função de membro do serviço do Cloud Assembly aos seus desenvolvedores de modelo de nuvem.

- a Clique em **Adicionar Acesso ao Serviço**.



- b Configure o usuário com o seguinte valor.

| Serviço | Função |
|----------------|--------------------------------|
| Cloud Assembly | Usuário do Cloud Assembly |
| Cloud Assembly | Visualizador do Cloud Assembly |

Neste caso de uso, seus desenvolvedores precisam ver a infraestrutura para garantir que estejam construindo modelos de nuvem implantáveis. Como usuários que você designará como administradores e membros do projeto na próxima etapa, eles não podem ver a infraestrutura. Como espectadores do serviço, eles podem ver como a infraestrutura está configurada, mas não podem fazer nenhuma alteração. Como administrador da nuvem, você permanece no controle, mas dá a eles acesso às informações de que precisam para desenvolver modelos de nuvem.

- 3 Crie projetos no Cloud Assembly que você usa para agrupar usuários de recursos.

Nesse caso de uso, você cria dois projetos. O primeiro projeto é **PersonnelAppDev** e o segundo é **PayrollAppDev**.

- a No console, clique na guia **Serviços** e depois em **Cloud Assembly**.
- b Selecione **Infraestrutura > Projetos > Novo Projeto**.
- c Insira **PersonnelAppDev** como o nome.
- d Clique em **Usuários** e depois em **Adicionar Usuários**.

- e Adicione membros do projeto e atribua um administrador de projeto.

| Função do Projeto | Descrição |
|--------------------------|---|
| Usuário do Projeto | Um membro do projeto é a principal função de usuário desenvolvedor em um projeto. Projetos determinam quais recursos de nuvem estão disponíveis quando você está pronto para testar seu trabalho de desenvolvimento implantando um modelo de nuvem. |
| Administrador do projeto | Um administrador de projeto oferece suporte aos desenvolvedores adicionando e removendo usuários para seus projetos. Você também pode excluir seus projetos. Para criar um projeto, você deve ter privilégios de administrador de serviço. |

- f Para os usuários que você está adicionando como membros de projeto, insira o endereço de e-mail de cada usuário, separado por vírgula, e selecione **Usuário** no menu suspenso **Atribuir função**.

Por exemplo, tony@mycompany.com, sylvia@mycompany.com.

PersonnelAppDev DELETE

Summary Users Provisioning Kubernetes Provisioning Integrations

Deployment sharing ☒ Deployments are shared between all users in the project

User roles Specify the users and groups related to this project.

+ ADD USERS + ADD GROUPS X REMOVE

Q Search users or groups

| <input type="checkbox"/> | Name | Account | Role |
|--------------------------|-----------------|---------|---------------|
| <input type="checkbox"/> | Sylvia Adams | sylvia | Administrator |
| <input type="checkbox"/> | Gloria Martinez | gloria | Member |
| <input type="checkbox"/> | Tony Anteater | tony | Member |

1 - 3 of 3 users

SAVE CANCEL

- g Para os administradores designados, selecione **Administrador** no menu suspenso **Atribuir função** e forneça o endereço de e-mail necessário.
- h Clique na guia **Provisionamento** e adicione uma ou mais zonas de nuvem.
- Quando os desenvolvedores de modelo de nuvem que fazem parte desse projeto implantam um modelo, ele é implantado nos recursos disponíveis nas zonas de nuvem. Você deve garantir que os recursos da zona de nuvem correspondam às necessidades dos modelos da equipe de desenvolvimento do projeto.
- i Repita o processo para adicionar o projeto PayrollAppDev com os usuários necessários e um administrador.

- 4 Forneça ao usuário do serviço as informações de login necessárias e verifique se os membros de cada projeto podem realizar as seguintes tarefas.
 - a Abrir o Cloud Assembly.
 - b Ver a infraestrutura em todos os projetos.
 - c Criar um modelo de nuvem para o projeto do qual eles são membros.
 - d Implantar o modelo de nuvem nos recursos da zona de nuvem definidos no projeto.
 - e Gerenciar suas implantações.
- 5 Atribua funções de membro da organização aos seus usuários desenvolvedores de modelo de nuvem.

Se precisar de instruções, consulte o [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).

- 6 Atribua funções a um administrador de catálogo, aos consumidores de catálogos e aos desenvolvedores de modelo de nuvem com base em seus respectivos trabalhos.

- a Clique em **Adicionar Acesso ao Serviço**.
- b Configure o administrador do catálogo com o seguinte valor.

Essa função pode ser você, o administrador da nuvem ou outra pessoa na sua equipe de desenvolvimento de aplicativos.

| Serviço | Função |
|----------------|---------------------------------|
| Service Broker | Administrador do Service Broker |

- c Configure os consumidores de modelo de nuvem com o seguinte valor.

| Serviço | Função |
|----------------|---------------------------|
| Service Broker | Usuário do Service Broker |

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Gloria Martinez** (gloria@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Service Broker ▾

with roles

Service Broker User ▾

×

[+ ADD SERVICE ACCESS](#)

- d Configure os desenvolvedores de modelo de nuvem com o seguinte valor.

| Serviço | Função |
|------------------------------|---------------------------|
| Cloud AssemblyCloud Assembly | Usuário do Cloud Assembly |

- 7 Crie projetos no Cloud Assembly que você usa para agrupar recursos e usuários.
 Nesse caso de uso, você cria dois projetos. O primeiro projeto é PersonnelAppDev e o segundo é PayrollAppDev.
 Se precisar de instruções, consulte o [Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo](#).
- 8 Crie e lance modelos de nuvem para cada equipe de projeto.
 Se precisar de instruções, consulte o [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).
- 9 Importe um modelo de nuvem do Cloud Assembly para o Service Broker.
 Você deve fazer login como um usuário com a função de Administrador do Service Broker.
 - a Faça login como um usuário com a função de Administrador do Service Broker.
 - b No console, clique em Service Broker.

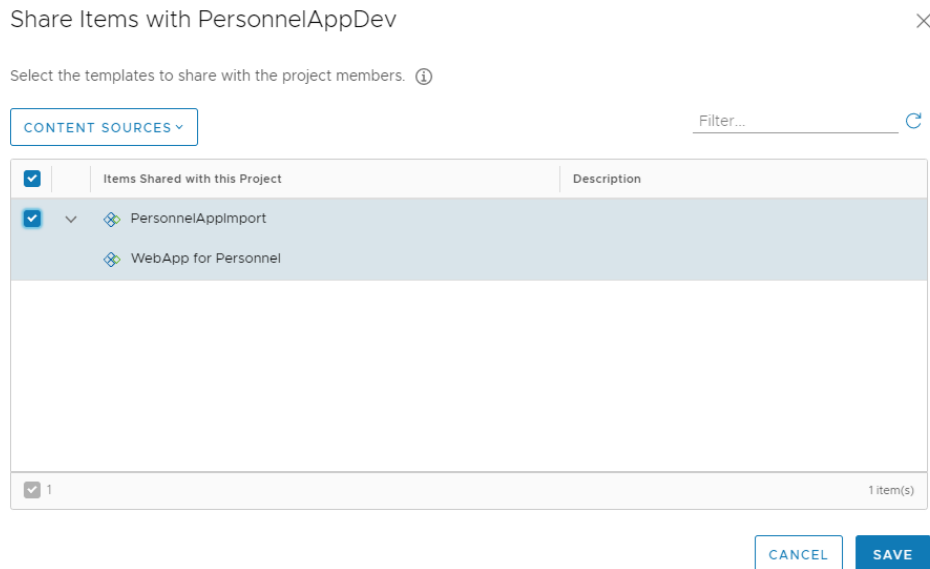
- c Selecione **Conteúdo e Políticas > Origens de Conteúdo** e clique em **Novo**.

The screenshot shows the 'New Content Source' configuration page. On the left, a sidebar contains a navigation menu with 'Content Sources' highlighted. The main area is titled 'New Content Source' and contains the following fields and sections:

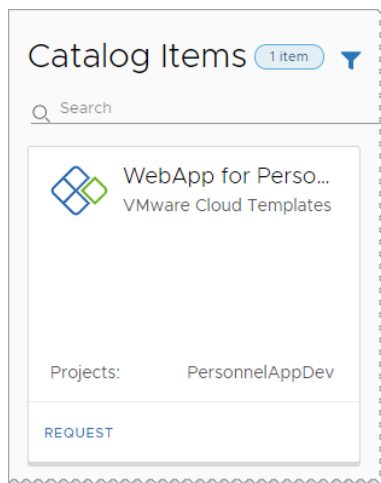
- Type:** A dropdown menu set to 'VMware Cloud Templates'.
- Name:** A text input field containing 'PersonnelAppImport'.
- Description:** A large text area for additional details.
- Get cloud templates from:** A section with a search bar and a dropdown menu.
- Source project:** A dropdown menu set to 'PersonnelAppDev'.
- VALIDATE:** A button to verify the configuration.
- Deploy cloud templates to:** A section with a note: 'Cloud templates will be deployed to cloud zones in projects they are shared with.'
- CREATE & IMPORT:** A blue button to create and import the content source.
- CANCEL:** A button to cancel the operation.

- d Selecione **Modelo de nuvem do Cloud Assembly**.
- e Insira **PersonnelAppImport** como o nome.
- f No menu suspenso **Projeto de Origem**, selecione PersonnelAppDev e clique em **Validar**.
- g Quando a origem estiver validada, clique em **Criar e Importar**.
- h Repita o processo para PayrollAppDev usando PayrollAppImport como o nome da origem de conteúdo.
- 10 Compartilhe um modelo de nuvem importado com um projeto.
- Embora o modelo de nuvem já esteja associado a um projeto, você o compartilha no Service Broker para disponibilizá-lo no catálogo.
- a Continue como um usuário com a função de administrador do Service Broker.
- b No Service Broker, selecione **Conteúdo e Políticas > Compartilhamento de Conteúdo**.
- c Selecione o projeto **PersonnelAppDev**, que inclui os usuários que devem ser capazes de implantar o modelo de nuvem do catálogo.

- d Clique em **Adicionar Itens** e selecione o modelo de nuvem PersonnelApp para compartilhar com os membros do projeto.



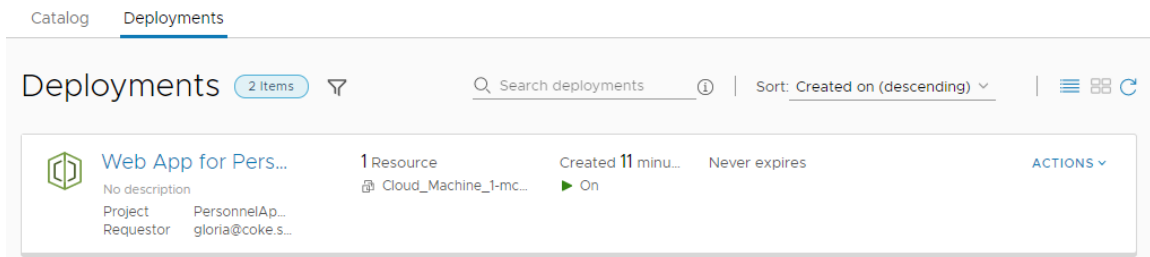
- e Clique em **Salvar**.
- 11 Verifique se o modelo de nuvem está disponível no catálogo do Service Broker para os membros do projeto.
 - a Solicite que um membro do projeto faça login e clique na guia **Catálogo**.



- b Clique em Solicitar no cartão do modelo de nuvem PersonnelApp.
- c Preencha o formulário e clique em **Enviar**.

12 Verifique se o membro do projeto pode monitorar o processo de implantação.

- a Solicite ao membro do projeto para selecionar **Recursos > Implantações** e localizar a solicitação de provisionamento dele.



- b Quando o modelo de nuvem for implantado, verifique se o usuário solicitante acessa o aplicativo.

13 Repita o processo para os projetos adicionais.

Resultados

Neste caso de uso, reconhecendo a necessidade de delegar o desenvolvimento de modelo de nuvem aos desenvolvedores, você adiciona mais membros da organização. Você os transformou em usuários do Cloud Assembly. Em seguida, você os tornou membros de projetos relevantes para que possam criar e implantar modelos de nuvem. Como membros do projeto, eles não podem ver ou alterar a infraestrutura que você continua gerenciando, mas você concedeu a eles permissões de espectador de serviço completo, para que eles pudessem entender as restrições da infraestrutura para a qual estão projetando.

Neste caso de uso, você configura os usuários com várias funções, incluindo o administrador e os usuários do Service Broker. Em seguida, você fornece aos usuários não desenvolvedores o catálogo do Service Broker.

Próximo passo

Para saber como definir e atribuir funções personalizadas aos usuários, consulte [Caso de uso de função de usuário 3: Configurar funções de usuário personalizadas no vRealize Automation para refinar as funções do sistema](#).

Caso de uso de função de usuário 3: Configurar funções de usuário personalizadas no vRealize Automation para refinar as funções do sistema

Como proprietário da organização ou administrador de serviços do vRealize Automation, você gerencia o acesso dos usuários usando as funções da organização e do sistema de serviço. No entanto, você também deseja criar funções personalizadas para os usuários selecionados e realizar tarefas ou ver conteúdo que está fora das funções deles no sistema.

Esse cenário presume que você entenda o usuário e o visualizador de serviço, bem como as funções de membro e visualizador do projeto definidas no caso de uso 2. Você pode ver que elas são mais restritivas do que as funções de administrador de projeto e de serviço usadas no caso de uso 1. Agora você identificou alguns casos de uso locais em que deseja que alguns usuários tenham permissões totais de gerenciamento para alguns recursos, permissões de visualização em outros, e não deseja que eles visualizem outro conjunto de recursos. Você usa funções personalizadas para definir essas permissões.

Esse caso de uso se baseia em três casos de uso locais possíveis. Esse procedimento mostra como criar permissões para as seguintes funções personalizadas.

- **Administrador de infraestrutura restrita.** Você deseja que alguns usuários de serviço, que não são administradores de serviços, tenham permissões de infraestrutura mais amplas. Como administrador, você deseja que eles ajudem a configurar zonas de nuvem, imagens e tipos. Você também deseja que eles estejam integrados e gerenciem os recursos detectados. Observe que eles não podem adicionar contas de nuvem ou integrações; eles podem apenas definir a infraestrutura para esses endpoints.
- **Desenvolvedor de extensibilidade.** Você deseja que alguns usuários do serviço tenham permissões completas para usar as ações de extensibilidade e assinaturas como parte do desenvolvimento do modelo de nuvem para sua equipe de projeto e outros projetos. Eles também desenvolverão tipos de recursos personalizados e ações personalizadas para vários projetos.
- **Desenvolvedor do XaaS.** Você deseja que alguns usuários de serviço tenham permissões totais para desenvolver tipos de recursos personalizados e ações personalizadas para vários projetos.
- **Solução de problemas de implantação.** Você deseja que seus administradores de projeto tenham as permissões necessárias para solucionar problemas e realizar a análise de causa raiz em implantações com falha. Você concede a eles permissões de gerenciamento em categorias não destrutivas ou menos caras, como mapeamentos de imagem e tipo. Você também deseja que os administradores do projeto tenham permissão para definir aprovações e políticas do dia 2 como parte da função de solução de problemas de implantação com falha.

Pré-requisitos

- Reveja as funções de serviço Cloud Assembly e Service Broker e as tabelas de funções de projeto em [Quais são as funções de usuário do vRealize Automation](#). Você precisa entender o que cada função de usuário de serviço pode ver e fazer nesses serviços.
- Analise as descrições de [Personalizar funções de usuário no vRealize Automation](#) para saber mais sobre como é possível refinar as permissões para os seus usuários.
- Analise o primeiro caso de uso para que você entenda as funções da organização e as funções de administrador do serviço. Consulte [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).

- Analise o segundo caso de uso para que você entenda o usuário de serviço e as funções de membro do projeto. Consulte [Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo](#).
- Familiarize-se com o Service Broker . Consulte [Adicionando conteúdo ao catálogo](#).

Procedimentos

- 1 Atribua funções de membro da organização aos seus usuários desenvolvedores de modelo de nuvem.

Se precisar de instruções, consulte o [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).

- 2 Atribua as funções de serviço Cloud Assembly e Service Broker para desenvolvedores de modelos de nuvem e consumidores de catálogos.

Se precisar de instruções, consulte o [Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo](#).

- 3 Crie projetos no Cloud Assembly que você usa para agrupar recursos e usuários.

As etapas abaixo para as funções personalizadas também incluem funções de projeto.

Se você precisar de instruções para criar projetos, consulte o [Caso de uso da função do usuário 2: Configurar funções de usuário no vRealize Automation para oferecer suporte a equipes de desenvolvimento maiores e ao catálogo](#).

- 4 Crie e lance modelos de nuvem para cada equipe de projeto.

Se precisar de instruções, consulte o [Caso de uso de função de usuário 1: Configurar funções de usuário do vRealize Automation para oferecer suporte a uma pequena equipe de desenvolvimento de aplicativos](#).

- 5 Faça login no Cloud Assembly como administrador de serviço e selecione **Infraestrutura > Administração > Funções personalizadas**.

- 6 Crie uma função de Administrador de infraestrutura restrita.

Neste exemplo, há um usuário, Tony, que é especialista na configuração da infraestrutura para vários projetos, mas não deseja dar a ele permissões totais de serviço. Em vez disso,

Tony desenvolve a infraestrutura central que oferece suporte ao trabalho de todos os projetos. Você dá a ele permissões limitadas de gerenciamento de infraestrutura. Tony, ou um prestador externo, também pode ter permissões semelhantes para a integração de máquinas detectadas e colocá-las sob gerenciamento do vRealize Automation.

- a Adicione Tony ao Cloud Assembly como usuário e visualizador de serviço.

Com as permissões de visualizador, ele pode ver as contas de nuvem e as integrações subjacentes, caso precise solucionar problemas em seu trabalho, mas não pode fazer alterações.

- b Crie um projeto e adicione Tony como membro do projeto.

- c Para criar a função personalizada, selecione **Infraestrutura > Administração > Funções personalizadas** e clique em **Nova função personalizada**.

- d Digite o nome **Administrador de infraestrutura restrita** e selecione as seguintes permissões.

| Selecione esta permissão... | Para que os usuários possam... |
|--|---|
| Infraestrutura > Gerenciar zonas de nuvem | Criar, atualizar e excluir zonas de nuvem. |
| Infraestrutura > Gerenciar mapeamentos de tipo | Criar, atualizar e excluir mapeamentos de tipo. |
| Infraestrutura > Gerenciar mapeamentos de imagem | Criar, atualizar e excluir mapeamentos de imagem. |

- e Clique em **Criar**.

- f Na página funções personalizadas, selecione a função de Administrador de infraestrutura restrita e clique em **Atribuir**.

- g Digite a conta de e-mail de Tony e clique em **Adicionar**.

Por exemplo, digite Tony@yourcompany.com.

Você também pode inserir qualquer grupo de usuários do Active Directory definido.

- h Aguarde Tony confirmar se, ao fazer login, ele consegue adicionar, editar e excluir valores nas áreas definidas pela função personalizada.

7 Crie uma função de Desenvolvedor de extensibilidade.

Neste exemplo, você tem vários desenvolvedores de modelo de nuvem, Sylvia e Igor, que sabem como usar ações de extensibilidade e assinaturas para gerenciar tarefas de

desenvolvimento diárias. Eles também têm experiência com vRealize Orchestrator e, portanto, você os incumbe de fornecer recursos e ações personalizadas para vários projetos. Você concede a eles permissões adicionais para gerenciar a extensibilidade administrando recursos e ações personalizadas, bem como ações de extensibilidade e assinaturas.

- a Adicione Sylvia e Igor como usuários do Cloud Assembly.
- b Adicione-os como membros dos projetos aos quais estão contribuindo com suas habilidades de extensibilidade.
- c Crie uma função de usuário personalizada que deve ser nomeada como **Desenvolvedor de extensibilidade** e selecione as seguintes permissões.

| Selecione esta permissão... | Para que os usuários possam... |
|---|--|
| XaaS > Gerenciar recursos personalizados | Criar, atualizar ou excluir recursos personalizados. |
| XaaS > Gerenciar ações de recursos | Criar, atualizar ou excluir ações personalizadas. |
| Extensibilidade > Gerenciar Recursos de Extensibilidade | Criar, atualizar ou excluir ações de extensibilidade e inscrições. Desativar as assinaturas. Cancelar e excluir a execução de ações. |

- d Clique em **Criar**.
 - e Atribua Sylvia e Igor à função de Desenvolvedor de extensibilidade.
 - f Verifique se Sylvia e Igor conseguem gerenciar os recursos e as ações personalizadas e se conseguem gerenciar as várias opções na guia Extensibilidade.
- 8** Crie uma função de solução de problemas de implantação.

Neste exemplo, você dá aos administradores de projeto mais permissões de gerenciamento para que eles possam corrigir falhas de implantação para suas equipes.

- a Adicione seus administradores de projeto, Shauna, Pratap e Wei, como usuários de serviços de Cloud Assembly e Service Broker.
- b Em seus projetos, adicione-os como administradores do projeto.
- c Crie uma função de usuário personalizada que deve ser nomeada como **Solução de problemas de implantação** e selecione as seguintes permissões.

| Selecione esta permissão... | Para que os usuários possam... |
|--|---|
| Infraestrutura > Gerenciar mapeamentos de tipo | Criar, atualizar e excluir mapeamentos de tipo. |
| Infraestrutura > Gerenciar mapeamentos de imagem | Criar, atualizar e excluir mapeamentos de imagem. |
| Implantações > Gerenciar implantações | Visualizar todas as implantações dos projetos e executar todas as ações do dia 2 nas implantações e nos componentes das implantações. |
| Política > Gerenciar políticas | Criar, atualizar ou excluir definições de política. |

- d Clique em **Criar**.
- e Atribua Shauna, Pratap e Wei à função de Solução de problemas de implantação.
- f Verifique se eles conseguem gerenciar mapeamentos de tipo, mapeamentos de imagem e políticas no Service Broker.

Resultados

Nesse caso de uso, você configura diferentes usuários com várias funções, incluindo funções personalizadas que ampliam suas funções de serviço e de projeto.

Próximo passo

Crie funções personalizadas que atendam aos seus casos de uso locais.

Como atribuir a função integrada de Administrador de Infraestrutura do Cloud Assembly a um usuário

A função de administrador de infraestrutura é uma função interna que você pode atribuir a usuários selecionados. Você não pode atribuir a função na interface do usuário.

Quando devo atribuir esta função de usuário

Você pode duplicar as permissões usando as opções de função de usuário personalizadas. No entanto, você pode atribuir essa função integrada a usuários que são administradores limitados.

Permissões de função de administrador de infraestrutura

A tabela a seguir fornece a lista de permissões de gerenciamento e outras permissões de que os administradores de infraestrutura precisam. Essas permissões não podem ser modificadas. "Se quiser que um usuário tenha permissões mais limitadas, use as funções personalizadas para criar uma função de usuário que atenda às suas necessidades específicas."

Tabela 3-15. Permissões fornecidas para a função integrada de Administrador de Infraestrutura

| Permissão para criar, editar, atualizar ou excluir | Outras permissões |
|---|---|
| <ul style="list-style-type: none"> ■ Contas de nuvem ■ Integrações ■ Zonas de nuvem ■ Mapeamentos de tipos ■ Mapeamentos de imagens ■ Perfis de rede ■ Perfis de armazenamento ■ Tags ■ Integração | <ul style="list-style-type: none"> ■ Visualizar e marcar recursos descobertos ■ Visualizar recursos de computação ■ Gerenciar endereços IP ■ Visualizar e marcar balanceadores de carga ■ Visualizar domínios de rede ■ Visualizar a segurança ■ Exibir armazenamento ■ Visualizar e remover solicitações |

Como atribuir a função de Administrador de Infraestrutura

Essa função integrada é atribuída usando a API RBAC. Primeiro, você obtém a função e, em seguida, atribui essa função a um usuário.

Antes de começar:

- Familiarize-se com a API. Consulte o [Guia de Programação de APIs do vRealize Automation](#).
 - Familiarize-se com a API. Consulte o [Guia de Programação de APIs do vRealize Automation 8.6](#).
 - Obtenha um token de portador da API. Consulte o artigo Obter seu token de acesso no [Guia de Programação de APIs do vRealize Automation](#).
 - Obtenha um token de portador da API. Consulte o artigo Obter seu token de acesso no [Guia de Programação de APIs do vRealize Automation 8.6](#)
- 1 Acesse `$vra/project/api/swagger/swagger-ui.html?urls.primaryName=rba` em que `$vra` é a URL base da sua instância.
 - 2 No canto superior direito da página, na lista suspensa **Selecionar uma definição**, selecione **rbac:2020-08-10**.
 - 3 Para recuperar a função do usuário, abra a seção **Função** e execute `GET /rbac-service/api/roles`.

Os resultados serão semelhantes ao exemplo a seguir.

```
"content": [
  {
    "description": "Infrastructure Administrator",
    "hidden": false,
    "id": "infrastructure_administrator",
    "name": "Infrastructure Administrator",
    "orgId": "string",
    "permissions": [
      "string"
    ],
    "projectScope": true
  }
]
```

- 4 Para adicionar um usuário à função, abra a seção **Atribuição de funções** e depois abra e edite o comando `PUT /rbac-service/api/role-assignments` com o nome de usuário incluído.

Por exemplo:

```
{
  "orgId": "string",
  "principalId": "Username@domain",
  "principalType": "user",
  "projectId": "string",
  "rolesToAdd": [
    "infrastructure_administrator"
  ],
}
```

```
"rolesToRemove": [
  "string"
]
```

- 5 Execute o comando PUT modificado.
- 6 Para verificar os resultados, instrua o usuário atribuído a fazer login e garantir que ele tenha as permissões definidas acima.

Como adicionar contas de nuvem ao Cloud Assembly

As contas de nuvem são as permissões configuradas que o Cloud Assembly usa para coletar dados das regiões ou centros de dados e implantar modelos de nuvem nessas regiões.

Os dados coletados incluem as regiões que serão associados posteriormente a zonas de nuvem.

Depois de configurar as zonas de nuvem, os mapeamentos e os perfis, será possível selecionar a conta de nuvem à qual eles estão associados.

Como administrador de nuvem, você cria contas de nuvem para os projetos nos quais os membros da sua equipe trabalham. As informações sobre recursos, como rede e segurança, processamento, armazenamento e tags são coletadas através de dados de suas contas de nuvem.

Observação Se a conta de nuvem tiver máquinas associadas que já foram implantadas na região, será possível colocar essas máquinas no gerenciamento do Cloud Assembly usando um plano de integração. Consulte [O que são planos de integração no Cloud Assembly](#).

Se você remover uma conta de nuvem que é usada em uma implantação, os recursos que fizeram parte dessa implantação se tornarão não gerenciados.

Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation

Para configurar e trabalhar com contas de nuvem em vRealize Automation, verifique se tem as seguintes credenciais.

Credenciais obrigatórias da conta de nuvem

| Para... | Você precisa... |
|--|---|
| Inscrever-se e fazer login no Cloud Assembly | Um ID da VMware. <ul style="list-style-type: none">■ Configure uma conta My VMware usando seu endereço de e-mail corporativo. |
| Conectar ao vRealize Automation Services | <p>A porta HTTPS 443 abre para o tráfego de saída com acesso por meio do firewall para:</p> <ul style="list-style-type: none">■ *.vmwareidentity.com■ gaz.csp-vidm-prod.com■ *.vmware.com <p>Para obter mais informações sobre portas e protocolos, consulte VMware Ports and Protocols.</p> <p>Para obter mais informações sobre portas e protocolos, consulte <i>Requisitos de porta</i> na ajuda da Arquitetura de referência.</p> |

| Para... | Você precisa... |
|---|---|
| Adicionar uma conta de nuvem do vCenter | <p>Privilégios são necessários para o agente do vSphere gerenciar a instância do vCenter Server. Forneça uma conta com os seguintes privilégios de leitura e gravação:</p> <ul style="list-style-type: none"> ■ Endereço IP ou FQDN do vCenter <p>As permissões necessárias para gerenciar contas de nuvem do VMware Cloud on AWS e do vCenter estão listadas. Permissões devem ser ativadas para todos os clusters do vCenter Server, e não apenas para clusters que hospedarão endpoints.</p> <p>Para todas as contas de nuvem baseadas no vCenter Server incluindo NSX-V, NSX-T, vCenter e VMware Cloud on AWS — o administrador deve ter credenciais de endpoint do vSphere ou as credenciais sob as quais o serviço do agente é executado no vCenter, que fornecem acesso administrativo ao host do vCenter Server.</p> <p>Para obter mais informações sobre requisitos do agente do vSphere, consulte a documentação do produto VMware vSphere.</p> <ul style="list-style-type: none"> ■ Repositório de dados <ul style="list-style-type: none"> ■ Alocar espaço ■ Procurar no repositório de dados ■ Operações de arquivo de baixo nível ■ Cluster de Repositório de Dados <ul style="list-style-type: none"> ■ Configurar um cluster de repositório de dados ■ Pasta <ul style="list-style-type: none"> ■ Criar pasta ■ Excluir pasta ■ Global <ul style="list-style-type: none"> ■ Gerenciar atributos personalizados ■ Definir atributo personalizado ■ Rede <ul style="list-style-type: none"> ■ Atribuir rede ■ Permissões <ul style="list-style-type: none"> ■ Modificar permissão ■ Recurso <ul style="list-style-type: none"> ■ Atribuir VM ao Pool de Res ■ Migrar máquina virtual desligada ■ Migrar máquina virtual ligada ■ Armazenamento baseado em perfil <ul style="list-style-type: none"> ■ Exibição Armazenamento baseado em perfil <p>Para retornar uma lista de políticas de armazenamento que podem ser mapeadas para um perfil de armazenamento, conceda o privilégio StorageProfile.View a todas as contas que conectam o vRealize Automation ao vCenter Server.</p> ■ Biblioteca de conteúdo |

| Para... | Você precisa... |
|---------|--|
| | <p>Para atribuir um privilégio em uma biblioteca de conteúdo, um administrador deve conceder o privilégio ao usuário como um privilégio global. Para obter informações relacionadas, consulte Herança hierárquica de permissões para bibliotecas de conteúdo, em <i>Administração de máquinas virtuais vSphere</i>, na Documentação do VMware vSphere.</p> <ul style="list-style-type: none"> ■ Adicionar item de biblioteca ■ Criar biblioteca local ■ Criar biblioteca assinada ■ Excluir item de biblioteca ■ Excluir biblioteca local ■ Excluir biblioteca assinada ■ Baixar arquivos ■ Remover item de biblioteca ■ Informações de assinatura de teste ■ Ler armazenamento ■ Sincronizar item da biblioteca ■ Sincronizar biblioteca assinada ■ Introspecção de tipo ■ Atualizar definições de configuração ■ Atualizar arquivos ■ Atualizar biblioteca ■ Atualizar item de biblioteca ■ Atualizar biblioteca local ■ Atualizar biblioteca assinada ■ Exibir definições de configuração ■ Marcação do vSphere <ul style="list-style-type: none"> ■ Atribuir ou cancelar atribuição de tag do vSphere ■ Atribuir ou cancelar atribuição de tag do vSphere em um objeto ■ Criar uma tag do vSphere ■ Criar uma categoria de tag do vSphere ■ Excluir uma tag do vSphere ■ Excluir uma categoria de tag do vSphere ■ Editar uma tag do vSphere ■ Editar uma categoria de tag do vSphere ■ Modificar campo UsedBy ou uma categoria ■ Modificar campo UsedBy para a tag ■ vApp <ul style="list-style-type: none"> ■ Importar ■ Configuração de aplicativos vApp <p>A configuração de aplicativos vApp.Import é necessária para modelos OVF e para provisionar VMs da biblioteca de conteúdo.</p> <p>A configuração do aplicativo vApp.vApp é necessária ao usar o cloud-init para scripts de configuração de nuvem. Essa configuração permite a modificação da estrutura interna de um vApp, como informações e propriedades do produto.</p> |

| Para... | Você precisa... |
|---------|--|
| | <ul style="list-style-type: none"> ■ Máquina virtual — Inventário <ul style="list-style-type: none"> ■ Criar com base no existente ■ Criar novo ■ Mover ■ Remover ■ Máquina virtual — Interação <ul style="list-style-type: none"> ■ Configurar mídia de CD ■ Interação do console ■ Conexão do dispositivo ■ Desligar ■ Ligar ■ Redefinir ■ Suspende ■ Instalação de ferramentas ■ Máquina virtual — Configuração <ul style="list-style-type: none"> ■ Adicionar disco existente ■ Adicionar novo ■ Remover disco ■ Avançado ■ Alterar contagem de CPU ■ Alterar recurso ■ Estender disco virtual ■ Rastreamento de alterações do dispositivo ■ Memória ■ Modificar configurações do dispositivo ■ Renomear ■ Definir anotação ■ Configurações ■ Posicionamento de Swapfile ■ Máquina virtual — Provisionamento <ul style="list-style-type: none"> ■ Personalizar ■ Clonar modelo ■ Clonar máquina virtual ■ Implantar modelo ■ Ler especificações de personalização ■ Máquina virtual — Estado <ul style="list-style-type: none"> ■ Criar snapshot ■ Remover snapshot ■ Reverter para snapshot |

| Para... | Você precisa... |
|---|---|
| Adicionar uma conta de nuvem do Amazon Web Services (AWS) | <p>Forneça uma conta de usuário avançado com privilégios de leitura e gravação. A conta do usuário deve ser membro da política de acesso avançado (PowerUserAccess) no sistema do AWS Identity and Access Management (IAM).</p> <ul style="list-style-type: none"> ■ ID da chave de acesso de 20 dígitos e Chave secreta de acesso correspondente <p>Se estiver usando um proxy de Internet HTTP externo, este deverá ser configurado para IPv4.</p> <p>A extensibilidade com base em ações (ABX) e integração de IPAM externo do vRealize Automation podem exigir permissões adicionais.</p> <p>As seguintes permissões do AWS são sugeridas para permitir as funções de autodimensionamento:</p> <ul style="list-style-type: none"> ■ Ações de autodimensionamento: <ul style="list-style-type: none"> ■ autodimensionamento: DescribeAutoScalingInstances ■ autodimensionamento: AttachInstances ■ autodimensionamento: DeleteLaunchConfiguration ■ autodimensionamento: DescribeAutoScalingGroups ■ autodimensionamento: CreateAutoScalingGroup ■ autodimensionamento: UpdateAutoScalingGroup ■ autodimensionamento: DeleteAutoScalingGroup ■ autodimensionamento: DescribeLoadBalancers ■ Recursos de autodimensionamento: <ul style="list-style-type: none"> ■ * <p>Forneça todas as permissões de recurso de autodimensionamento.</p> <p>As seguintes permissões são obrigatórias para permitir que as funções do serviço de token de segurança do AWS (AWS STS) ofereçam credenciais temporárias e de privilégio limitado para identidade e acesso ao AWS:</p> <ul style="list-style-type: none"> ■ Recursos do AWS STS: <ul style="list-style-type: none"> ■ * <p>Forneça todas as permissões de recursos do STS.</p> <p>As seguintes permissões do AWS são obrigatórias para permitir funções do EC2:</p> ■ Ações do EC2: <ul style="list-style-type: none"> ■ ec2: AttachVolume ■ ec2: AuthorizeSecurityGroupIngress ■ ec2: DeleteSubnet ■ ec2: DeleteSnapshot ■ ec2: DescribeInstances ■ ec2: DeleteTags ■ ec2: DescribeRegions ■ ec2: DescribeVolumesModifications ■ ec2: CreateVpc ■ ec2: DescribeSnapshots ■ ec2: DescribeInternetGateways ■ ec2: DeleteVolume |

| Para... | Você precisa... |
|---------|--|
| | <ul style="list-style-type: none"> ■ ec2: DescribeNetworkInterfaces ■ ec2: StartInstances ■ ec2: DescribeAvailabilityZones ■ ec2: CreateInternetGateway ■ ec2: CreateSecurityGroup ■ ec2: DescribeVolumes ■ ec2: CreateSnapshot ■ ec2: ModifyInstanceAttribute ■ ec2: DescribeRouteTables ■ ec2: DescribeInstanceTypes ■ ec2: DescribeInstanceTypeOfferings ■ ec2: DescribeInstanceStatus ■ ec2: DetachVolume ■ ec2: RebootInstances ■ ec2: AuthorizeSecurityGroupEgress ■ ec2: ModifyVolume ■ ec2: TerminateInstances ■ ec2: DescribeSpotFleetRequestHistory ■ ec2: DescribeTags ■ ec2: CreateTags ■ ec2: RunInstances ■ ec2: DescribeNatGateways ■ ec2: StopInstances ■ ec2: DescribeSecurityGroups ■ ec2: CreateVolume ■ ec2: DescribeSpotFleetRequests ■ ec2: DescribeImages ■ ec2: DescribeVpcs ■ ec2: DeleteSecurityGroup ■ ec2: DeleteVpc ■ ec2: CreateSubnet ■ ec2: DescribeSubnets ■ ec2: RequestSpotFleet |
| | <p>Observação A permissão de solicitação SpotFleet não é obrigatória para extensibilidade com base em ações (ABX) do vRealize Automation ou integrações IPAM externas.</p> |
| | <ul style="list-style-type: none"> ■ Recursos do EC2: <ul style="list-style-type: none"> ■ * <p>Forneça todas as permissões de recursos do EC2.</p> <p>As seguintes permissões do AWS são obrigatórias para permitir funções do balanceador de carga:</p> <ul style="list-style-type: none"> ■ Ações do balanceador de carga: <ul style="list-style-type: none"> ■ elasticloadbalancing:DeleteLoadBalancer ■ elasticloadbalancing:DescribeLoadBalancers |

| Para... | Você precisa... |
|---------|---|
| | <ul style="list-style-type: none"> ■ elasticloadbalancing:RemoveTags ■ elasticloadbalancing:CreateLoadBalancer ■ elasticloadbalancing:DescribeTags ■ elasticloadbalancing:ConfigureHealthCheck ■ elasticloadbalancing: AddTags ■ elasticloadbalancing: CreateTargetGroup ■ elasticloadbalancing>DeleteLoadBalancerListeners ■ elasticloadbalancing:DeregisterInstancesFromLoadBalancer ■ elasticloadbalancing:RegisterInstancesWithLoadBalancer ■ elasticloadbalancing:CreateLoadBalancerListeners ■ Recursos do balanceador de carga: <ul style="list-style-type: none"> ■ * <p>Forneça todas as permissões de recursos do balanceador de carga. As seguintes permissões do AWS Identity and Access Management (IAM) podem ser habilitadas, embora não sejam necessárias:</p> <ul style="list-style-type: none"> ■ iam: SimulateCustomPolicy ■ iam: GetUser ■ iam: ListUserPolicies ■ iam: GetUserPolicy ■ iam: ListAttachedUserPolicies ■ iam: GetPolicyVersion ■ iam: ListGroupsForUser ■ iam: ListGroupPolicies ■ iam: GetGroupPolicy ■ iam: ListAttachedGroupPolicies ■ iam: ListPolicyVersions |

| Para... | Você precisa... |
|---|--|
| Adicionar uma conta de nuvem do Microsoft Azure | <p>Configure uma instância do Microsoft Azure e obtenha uma assinatura válida do Microsoft Azure na qual você possa usar o ID da assinatura.</p> <p>Crie um aplicativo Active Directory conforme descrito em Como: usar o portal para criar um aplicativo do Azure AD e a entidade de segurança de serviço que pode acessar recursos, na documentação do produto Microsoft Azure.</p> <p>Se estiver usando um proxy de Internet HTTP externo, este deverá ser configurado para IPv4.</p> <p>Anote as seguintes informações:</p> <ul style="list-style-type: none"> ■ ID da assinatura <p>Permite que você acesse suas assinaturas do Microsoft Azure.</p> ■ ID do Tenant <p>O endpoint de autorização para os aplicativos do Active Directory criado na conta do Microsoft Azure.</p> ■ ID do aplicativo cliente <p>Fornece acesso ao Microsoft Active Directory em sua conta individual do Microsoft Azure.</p> ■ Chave secreta do aplicativo cliente <p>A chave secreta exclusiva gerada para emparelhar com o ID do aplicativo cliente.</p> <p>As seguintes permissões são necessárias para criar e validar contas de nuvem do Microsoft Azure:</p> <ul style="list-style-type: none"> ■ Microsoft Compute <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete ■ Microsoft.Compute/virtualMachines/deallocate/action ■ Microsoft.Compute/virtualMachines/delete ■ Microsoft.Compute/virtualMachines/powerOff/action ■ Microsoft.Compute/virtualMachines/read ■ Microsoft.Compute/virtualMachines/restart/action ■ Microsoft.Compute/virtualMachines/start/action ■ Microsoft.Compute/virtualMachines/write ■ Microsoft.Compute/availabilitySets/write ■ Microsoft.Compute/availabilitySets/read ■ Microsoft.Compute/availabilitySets/delete ■ Microsoft.Compute/disks/delete ■ Microsoft.Compute/disks/read ■ Microsoft.Compute/disks/write ■ Microsoft Network <ul style="list-style-type: none"> ■ Microsoft.Network/loadBalancers/backendAddressPools/join/action ■ Microsoft.Network/loadBalancers/delete ■ Microsoft.Network/loadBalancers/read ■ Microsoft.Network/loadBalancers/write ■ Microsoft.Network/networkInterfaces/join/action |

| Para... | Você precisa... |
|---------|--|
| | <ul style="list-style-type: none"> ■ Microsoft.Network/networkInterfaces/read ■ Microsoft.Network/networkInterfaces/write ■ Microsoft.Network/networkInterfaces/delete ■ Microsoft.Network/networkSecurityGroups/join/action ■ Microsoft.Network/networkSecurityGroups/read ■ Microsoft.Network/networkSecurityGroups/write ■ Microsoft.Network/networkSecurityGroups/delete ■ Microsoft.Network/publicIPAddresses/delete ■ Microsoft.Network/publicIPAddresses/join/action ■ Microsoft.Network/publicIPAddresses/read ■ Microsoft.Network/publicIPAddresses/write ■ Microsoft.Network/virtualNetworks/read ■ Microsoft.Network/virtualNetworks/subnets/delete ■ Microsoft.Network/virtualNetworks/subnets/join/action ■ Microsoft.Network/virtualNetworks/subnets/read ■ Microsoft.Network/virtualNetworks/subnets/write ■ Microsoft.Network/virtualNetworks/write ■ Microsoft Resources <ul style="list-style-type: none"> ■ Microsoft.Resources/subscriptions/resourcegroups/delete ■ Microsoft.Resources/subscriptions/resourcegroups/read ■ Microsoft.Resources/subscriptions/resourcegroups/write ■ Microsoft Storage <ul style="list-style-type: none"> ■ Microsoft.Storage/storageAccounts/delete ■ Microsoft.Storage/storageAccounts/listKeys/action ■ Microsoft.Storage/storageAccounts/read ■ Microsoft.Storage/storageAccounts/write ■ Microsoft Web <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action ■ Microsoft.Web/sites/publishxml/action ■ Microsoft.Web/serverfarms/write ■ Microsoft.Web/serverfarms/delete ■ Microsoft.Web/sites/hostruntime/functions/keys/read ■ Microsoft.Web/sites/hostruntime/host/read ■ Microsoft.web/sites/functions/masterkey/read <p>Se você estiver usando o Microsoft Azure com extensibilidade baseada em ação, as seguintes permissões serão necessárias, além das permissões mínimas:</p> <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete |

| Para... | Você precisa... |
|---------|--|
| | <ul style="list-style-type: none"> ■ Microsoft.Web/sites/*/action ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action ■ Microsoft.Web/sites/publishxml/action ■ Microsoft.Web/serverfarms/write ■ Microsoft.Web/serverfarms/delete ■ Microsoft.Web/sites/hostruntime/functions/keys/read ■ Microsoft.Web/sites/hostruntime/host/read ■ Microsoft.Web/sites/functions/masterkey/read ■ Microsoft.Web/apimanagementaccounts/apis/read ■ Microsoft.Authorization/roleAssignments/read ■ Microsoft.Authorization/roleAssignments/write ■ Microsoft.Authorization/roleAssignments/delete ■ Microsoft.Insights/Components/Read ■ Microsoft.Insights/Components/Write ■ Microsoft.Insights/Components/Query/Read <p>Se você estiver usando o Microsoft Azure com extensibilidade baseada em ação com extensões, as seguintes permissões também serão necessárias:</p> <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete <p>Para obter informações relacionadas sobre como criar uma conta de nuvem do Microsoft Azure, consulte Configurar o Microsoft Azure.</p> |

| Para... | Você precisa... |
|---|---|
| Adicionar uma conta de nuvem da Google Cloud Platform (GCP) | <p>A conta de nuvem da Google Cloud Platform interage com o mecanismo de processamento da Google Cloud Platform.</p> <p>As credenciais de Administrador e Proprietário do Projeto são necessárias para criar e validar contas de nuvem da Google Cloud Platform.</p> <p>Se estiver usando um proxy de Internet HTTP externo, este deverá ser configurado para IPv4.</p> <p>O serviço de mecanismo de processamento deve ser ativado. Ao criar a conta de nuvem no vRealize Automation, use a conta de serviço que foi criada quando o mecanismo de processamento foi inicializado.</p> <p>As seguintes permissões do mecanismo de processamento também são necessárias, dependendo das ações que o usuário pode realizar:</p> <ul style="list-style-type: none"> ■ roles/compute.admin <p>Fornece controle total de todos os recursos do mecanismo de computação.</p> ■ roles/iam.serviceAccountUser <p>Fornece acesso a usuários que gerenciam instâncias de máquina virtual configuradas para serem executadas como uma conta de serviço. Conceda acesso aos seguintes recursos e serviços:</p> <ul style="list-style-type: none"> ■ compute.* ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.imageUser <p>Concede permissão para listar e ler imagens sem ter outras permissões na imagem. A concessão da função compute.imageUser no nível do projeto oferece aos usuários a capacidade de listar todas as imagens no projeto. Também permite que os usuários criem recursos, como instâncias e discos permanentes, com base em imagens do projeto.</p> <ul style="list-style-type: none"> ■ compute.images.get ■ compute.images.getFromFamily ■ compute.images.list ■ compute.images.useReadOnly ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.instanceAdmin <p>Concede permissões para criar, modificar e excluir instâncias de máquina virtual. Isso inclui permissões para criar, modificar e excluir discos e também para definir configurações VMBETA protegidas.</p> |

| Para... | Você precisa... |
|---------|--|
| | <p>Para usuários que gerenciam instâncias de máquina virtual (mas não configurações de rede ou segurança ou instâncias executadas como contas de serviço), conceda essa função à organização, pasta ou projeto que contém as instâncias, ou às instâncias individuais.</p> <p>Os usuários que gerenciam instâncias de máquina virtual configuradas para serem executadas como uma conta de serviço também precisam da função <code>roles/iam.serviceAccountUser</code>.</p> <ul style="list-style-type: none"> ■ <code>compute.acceleratorTypes</code> ■ <code>compute.addresses.get</code> ■ <code>compute.addresses.list</code> ■ <code>compute.addresses.use</code> ■ <code>compute.autoscalers</code> ■ <code>compute.diskTypes</code> ■ <code>compute.disks.create</code> ■ <code>compute.disks.createSnapshot</code> ■ <code>compute.disks.delete</code> ■ <code>compute.disks.get</code> ■ <code>compute.disks.list</code> ■ <code>compute.disks.resize</code> ■ <code>compute.disks.setLabels</code> ■ <code>compute.disks.update</code> ■ <code>compute.disks.use</code> ■ <code>compute.disks.useReadOnly</code> ■ <code>compute.globalAddresses.get</code> ■ <code>compute.globalAddresses.list</code> ■ <code>compute.globalAddresses.use</code> ■ <code>compute.globalOperations.get</code> ■ <code>compute.globalOperations.list</code> ■ <code>compute.images.get</code> ■ <code>compute.images.getFromFamily</code> ■ <code>compute.images.list</code> ■ <code>compute.images.useReadOnly</code> ■ <code>compute.instanceGroupManagers</code> ■ <code>compute.instanceGroups</code> ■ <code>compute.instanceTemplates</code> ■ <code>compute.instances</code> ■ <code>compute.licenses.get</code> ■ <code>compute.licenses.list</code> ■ <code>compute.machineTypes</code> ■ <code>compute.networkEndpointGroups</code> ■ <code>compute.networks.get</code> ■ <code>compute.networks.list</code> ■ <code>compute.networks.use</code> ■ <code>compute.networks.useExternalIp</code> ■ <code>compute.projects.get</code> |

| Para... | Você precisa... |
|---------|--|
| | <ul style="list-style-type: none"> ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternalIp ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourceManager.projects.get ■ resourceManager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.instanceAdmin.v1 <p>Fornece controle total de instâncias do mecanismo de processamento, grupos de instâncias, discos, snapshots e imagens. Também fornece acesso de leitura a todos os recursos de rede do mecanismo de computação.</p> <hr/> <p>Observação Se você conceder a um usuário essa função no nível da instância, ele não poderá criar novas instâncias.</p> <hr/> <ul style="list-style-type: none"> ■ compute.acceleratorTypes ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use ■ compute.autoscalers ■ compute.backendBuckets.get ■ compute.backendBuckets.list ■ compute.backendServices.get ■ compute.backendServices.list ■ compute.diskTypes ■ compute.disks ■ compute.firewalls.get ■ compute.firewalls.list ■ compute.forwardingRules.get ■ compute.forwardingRules.list ■ compute.globalAddresses.get ■ compute.globalAddresses.list ■ compute.globalAddresses.use |

| Para... | Você precisa... |
|---------|---|
| | <ul style="list-style-type: none"> ■ compute.globalForwardingRules.get ■ compute.globalForwardingRules.list ■ compute.globalOperations.get ■ compute.globalOperations.list ■ compute.healthChecks.get ■ compute.healthChecks.list ■ compute.httpHealthChecks.get ■ compute.httpHealthChecks.list ■ compute.httpsHealthChecks.get ■ compute.httpsHealthChecks.list ■ compute.images ■ compute.instanceGroupManagers ■ compute.instanceGroups ■ compute.instanceTemplates ■ compute.instances ■ compute.interconnectAttachments.get ■ compute.interconnectAttachments.list ■ compute.interconnectLocations ■ compute.interconnects.get ■ compute.interconnects.list ■ compute.licenseCodes ■ compute.licenses ■ compute.machineTypes ■ compute.networkEndpointGroups ■ compute.networks.get ■ compute.networks.list ■ compute.networks.use ■ compute.networks.useExternalIp ■ compute.projects.get ■ compute.projects.setCommonInstanceMetadata ■ compute.regionBackendServices.get ■ compute.regionBackendServices.list ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.resourcePolicies ■ compute.routers.get ■ compute.routers.list ■ compute.routes.get ■ compute.routes.list ■ compute.snapshots ■ compute.sslCertificates.get ■ compute.sslCertificates.list |

| Para... | Você precisa... |
|---------------------------------------|---|
| | <ul style="list-style-type: none"> ■ compute.sslPolicies.get ■ compute.sslPolicies.list ■ compute.sslPolicies.listAvailableFeatures ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternalIp ■ compute.targetHttpProxies.get ■ compute.targetHttpProxies.list ■ compute.targetHttpsProxies.get ■ compute.targetHttpsProxies.list ■ compute.targetInstances.get ■ compute.targetInstances.list ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.targetSslProxies.get ■ compute.targetSslProxies.list ■ compute.targetTcpProxies.get ■ compute.targetTcpProxies.list ■ compute.targetVpnGateways.get ■ compute.targetVpnGateways.list ■ compute.urlMaps.get ■ compute.urlMaps.list ■ compute.vpnTunnels.get ■ compute.vpnTunnels.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourceManager.projects.get ■ resourceManager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list |
| Adicionar uma conta de nuvem do NSX-T | <p>Forneça uma conta com os seguintes privilégios de leitura e gravação:</p> <ul style="list-style-type: none"> ■ Endereço IP ou FQDN do NSX-T ■ Centro de dados do NSX-T - Credenciais de acesso e função de Administrador Empresarial <p>Os administradores <i>também</i> exigem acesso ao vCenter Server, conforme descrito na seção <i>Adicionar uma conta de nuvem do vCenter</i> desta tabela.</p> |
| Adicionar uma conta de nuvem do NSX-V | <p>Forneça uma conta com os seguintes privilégios de leitura e gravação:</p> <ul style="list-style-type: none"> ■ Credenciais de acesso e função de Administrador Empresarial do NSX-V ■ Endereço IP ou FQDN do NSX-V <p>Os administradores <i>também</i> exigem acesso ao vCenter Server, conforme descrito na seção <i>Adicionar uma conta de nuvem do vCenter</i> desta tabela.</p> |

| Para... | Você precisa... |
|---|--|
| Adicionar uma conta de nuvem do VMware Cloud on AWS (VMC) | <p>Forneça uma conta com os seguintes privilégios de leitura e gravação:</p> <ul style="list-style-type: none"> ■ A conta cloudadmin@vmc.local ou qualquer conta de usuário no grupo CloudAdmin ■ Credenciais de acesso e função de Administrador Empresarial do NSX ■ Acesso de administrador de nuvem do NSX ao ambiente SDDC do VMware Cloud on AWS de sua organização ■ Acesso de administrador ao ambiente SDDC do VMware Cloud on AWS de sua organização ■ O token de API do VMware Cloud on AWS para o seu ambiente do VMware Cloud on AWS no serviço do VMware Cloud on AWS de sua organização ■ Endereço IP ou FQDN do vCenter <p>Os administradores <i>também</i> exigem acesso ao vCenter Server, conforme descrito na seção <i>Adicionar uma conta de nuvem do vCenter</i> desta tabela. Para obter mais informações sobre as permissões necessárias para criar e usar contas de nuvem do VMware Cloud on AWS, consulte <i>Gerenciando o centro de dados do VMware Cloud on AWS</i>, na VMware Cloud on AWS documentação do produto https://docs.vmware.com/br/VMware-Cloud-on-AWS/index.html.</p> |
| Integração com o vRealize Operations Manager | <p>Forneça uma conta de login local ou não local para o vRealize Operations Manager com os seguintes privilégios de leitura.</p> <ul style="list-style-type: none"> ■ Instância de adaptador vCenter Adaptador > Instância de adaptador do VC para <i>vCenter-FQDN</i> <p>Talvez seja necessário importar uma conta não local antes que você possa atribuir sua função somente leitura.</p> |

Configurar o Microsoft Azure para uso com o Cloud Assembly

Você deve coletar algumas informações e executar determinadas configurações para criar uma conta de nuvem do Microsoft Azure no Cloud Assembly.

Procedimentos

- 1 Localize e registre sua assinatura do Microsoft Azure e IDs de tenants.
 - ID da Assinatura - Clique no ícone Assinaturas na barra de ferramentas à esquerda no portal do Azure para exibir o ID da assinatura.
 - ID do Tenant - Clique no ícone Ajuda e selecione Mostrar Diagnóstico no portal do Azure. Pesquise o tenant e registre o ID quando encontrá-lo.

- 2 Você pode criar uma nova conta de armazenamento e um grupo de recursos para começar. Como alternativa, é possível criá-los posteriormente em blueprints.

- Conta de Armazenamento - Use o procedimento a seguir para configurar uma conta.
 - 1 No portal do Azure, localize o ícone Contas de Armazenamento na barra lateral. Certifique-se de que a assinatura correta esteja selecionada e clique em **Adicionar**. Você também pode procurar a conta de armazenamento no campo de pesquisa do Azure.
 - 2 Insira as informações necessárias para a conta de armazenamento. Você precisará do ID da assinatura.
 - 3 Selecione se deseja usar um grupo de recursos existente ou criar um novo. Anote o nome do seu grupo de recursos, pois você precisará dele mais tarde.

Observação Salve a localização da sua conta de armazenamento, pois você precisará dela mais tarde.

- 3 Crie uma rede virtual. Como alternativa, se tiver uma rede existente adequada, você poderá selecioná-la.

Se estiver criando uma rede, você deverá selecionar Usar um Grupo de Recursos Existente e especificar o grupo criado na etapa anterior. Além disso, selecione a mesma localização especificada anteriormente. O Microsoft Azure não implantará máquinas virtuais ou outros objetos se a localização não corresponder a todos os componentes aplicáveis que o objeto consumirá.

- a Localize o ícone Rede Virtual no painel esquerdo e clique nele ou pesquise a rede virtual. Certifique-se de selecionar a assinatura correta e clique em **Adicionar**.
 - b Insira um nome exclusivo para sua nova rede virtual e registre-o para uso posterior.
 - c Insira o endereço IP apropriado para a sua rede virtual no campo **Espaço de endereço**.
 - d Certifique-se de que a assinatura correta esteja selecionada e clique em **Adicionar**.
 - e Insira as informações básicas de configuração restantes.
 - f Você pode modificar as outras opções conforme necessário, mas, para a maioria das configurações, é possível deixar os valores padrão.
 - g Clique em **Criar**.
- 4 Configure um aplicativo do Azure Active Directory para que o vRA possa se autenticar.
- a Localize o ícone do Active Directory no menu esquerdo do Azure e clique nele.
 - b Clique em **Registros de Aplicativos** e selecione **Adicionar**.
 - c Digite um nome para o seu aplicativo que seja compatível com a validação de nomes do Azure.
 - d Deixe Aplicativo Web/API como o Tipo de Aplicativo.

- e A URL de Logon pode ser qualquer coisa apropriada para seu uso.
 - f Clique em **Criar**.
- 5 Crie uma chave secreta para autenticar o aplicativo no Cloud Assembly.
- a Clique no nome do seu aplicativo no Azure.
Anote seu ID de Aplicativo para uso posterior.
 - b Clique **Todas as Configurações** no próximo painel e selecione Chaves na lista de configurações.
 - c Insira uma descrição para a nova chave e escolha uma duração.
 - d Clique em **Salvar** e certifique-se de copiar o valor da chave para um local seguro, pois você não poderá recuperá-lo mais tarde.
 - e No menu esquerdo, selecione **Permissões de API** para o aplicativo e clique em **Adicionar uma Permissão** para criar uma nova permissão.
 - f Selecione Gerenciamento de Serviços do Azure na página Selecionar uma API.
 - g Clique em **Permissões Delegadas**.
 - h Em Selecionar permissões, selecione user_impersonation e clique em **Adicionar Permissões**.
- 6 Autorize seu aplicativo Active Directory a se conectar à sua assinatura do Azure para que você possa implantar e gerenciar máquinas virtuais.
- a No menu à esquerda, clique no ícone Assinaturas e selecione sua nova assinatura.
Talvez seja necessário clicar no texto do nome para que o painel deslize.
 - b Selecione a opção Controle de Acesso (IAM) para ver as permissões da sua assinatura.
 - c Clique em **Adicionar** sob o título Adicionar uma Atribuição de Função.
 - d Escolha Colaborador no menu suspenso Função.
 - e Deixe a seleção padrão no menu suspenso Atribuir Acesso a.
 - f Digite o nome do seu aplicativo na caixa Selecionar.
 - g Clique em **Salvar**.
 - h Adicione outras funções para que seu novo aplicativo tenha as funções Proprietário, Colaborador e Leitor.
 - i Clique em **Salvar**.

Próximo passo

Você deve instalar as ferramentas de interface de linha de comando do Microsoft Azure. Essas ferramentas estão disponíveis gratuitamente para os sistemas operacionais Windows e Mac. Consulte a documentação da Microsoft para obter mais informações sobre como baixar e instalar essas ferramentas.

Quando tiver a interface de linha de comando instalada, você deverá se autenticar na sua nova assinatura.

- 1 Abra uma janela de terminal e digite seu login do Microsoft Azure. Você receberá uma URL e um código de acesso que permitirá a autenticação.
- 2 Em um navegador, insira o código recebido do aplicativo no seu dispositivo.
- 3 Insira seu Código de Autenticação e clique em **Continuar**.
- 4 Selecione sua conta do Azure e faça login.

Se você tiver várias assinaturas, certifique-se de que a correta seja selecionada, usando o comando `azure account set <subscription-name>`.

- 5 Antes de continuar, você deve registrar o provedor Microsoft.Compute na sua nova assinatura do Azure, usando o comando `azure provider register microsoft.compute`.

Se o comando atingir o tempo limite e gerar um erro na primeira vez que você o executar, execute-o novamente.

Quando tiver concluído a configuração, você poderá usar o comando `azure vm image list` para recuperar nomes de imagens de máquinas virtuais disponíveis. É possível escolher a imagem desejada e registrar o URN fornecido para ela e depois usá-la em blueprints.

Criar uma conta de nuvem do Microsoft Azure no vRealize Automation

Como administrador de nuvem, você pode criar uma conta de nuvem da Microsoft Azure para regiões de conta nas quais sua equipe implantará modelos de nuvem do vRealize Automation.

Para ver um exemplo de caso de uso de como a conta em nuvem do Microsoft Azure funciona no vRealize Automation, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se você tem a função de usuário necessária. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Configure uma conta do Microsoft Azure para uso com o vRealize Automation. Consulte [Configurar o Microsoft Azure para uso com o Cloud Assembly](#).
- Se você não tiver acesso externo à Internet, configure um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta do Microsoft Azure e digite as credenciais e outros valores.
- 3 Clique em **Validar**.
As regiões de conta associadas à conta são coletadas.
- 4 Selecione as regiões para as quais deseja provisionar este recurso.
- 5 Para obter eficiência, clique em **Criar uma zona de nuvem para as regiões selecionadas**.
- 6 Se for necessário adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).



Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

- 7 Clique em **Salvar**.

Resultados

A conta é adicionada ao vRealize Automation e as regiões selecionadas estão disponíveis para a zona de nuvem especificada.

Próximo passo

Crie recursos de infraestrutura para esta conta de nuvem.

Ao adicionar uma conta de nuvem do Azure a um modelo de nuvem, você pode optar por reutilizar os conjuntos de disponibilidade, se desejar. Como as assinaturas têm um limite de 2.000 conjuntos de disponibilidade e 25.000 máquinas virtuais, faz sentido reutilizar os conjuntos de disponibilidade quando possível. Existem duas propriedades YAML que você pode usar para controlar como as implantações usam conjuntos de disponibilidade. A propriedade `availabilitySetName` permite que você especifique um conjunto de disponibilidade a ser usado. A segunda propriedade é `doNotAttachAvailabilitySet`, que está definida como `false` por padrão. Se essa propriedade for definida como `true`, o vRealize Automation criará a implantação sem um conjunto de disponibilidade.

Você não poderá criar uma implantação sem um conjunto de disponibilidade se usar um balanceador de carga conectado à máquina virtual.

A tabela a seguir descreve como o vRealize Automation se comporta dependendo de um grupo de recursos e um conjunto de disponibilidade estarem especificados no modelo de nuvem.

Um conjunto de disponibilidade não pode existir sem fazer parte de um grupo de recursos. Os conjuntos de disponibilidade em um determinado grupo de recursos devem ter nomes exclusivos. Os conjuntos de disponibilidade poderão ter o mesmo nome apenas se fizerem parte de diferentes grupos de recursos.

Se você não especificar um nome de grupo de recursos, o vRealize Automation criará um novo grupo de recursos, o que significa que um novo conjunto de disponibilidade também deverá ser criado, mesmo que um nome seja transmitido. O novo conjunto usará o nome que foi transmitido.

Tabela 3-16.

| Grupo de recursos especificado | Conjunto de disponibilidade especificado | Resultado |
|--------------------------------|--|--|
| Não | Não | O vRealize Automation cria um novo grupo de recursos e um novo conjunto de disponibilidade para a máquina virtual. |
| Sim | Não | O vRealize Automation reutiliza o grupo de recursos existente e cria um novo conjunto de disponibilidade para a máquina virtual. |
| Não | Sim | O vRealize Automation cria um novo grupo de recursos e um novo conjunto de disponibilidade com o nome especificado. |
| Sim | Sim | O vRealize Automation reutiliza o grupo de recursos existente. Se já houver um conjunto de disponibilidade com o nome especificado nesse grupo, ele também será reutilizado. Se não houver disponibilidade definida com o nome especificado no grupo, um novo será criado com esse nome. |

O Cloud Assembly oferece suporte a snapshots de disco do Azure para máquinas virtuais implantadas. Consulte [Como trabalhar com snapshots para discos de máquina virtual do Microsoft Azure no vRealize Operations Manager](#) para obter mais informações.

O Cloud Assembly oferece suporte para várias opções de diagnóstico de inicialização para implementações do Azure. O diagnóstico de inicialização oferece suporte à depuração de máquinas virtuais do Azure e inclui a coleta de informações de log e capturas de tela relevantes. Consulte [Usando o diagnóstico de inicialização e análises de log com uma máquina virtual Microsoft Azure](#) para obter mais informações.

Usando o diagnóstico de inicialização e análises de log com uma máquina virtual Microsoft Azure

Você pode invocar e configurar o diagnóstico de inicialização do Microsoft Azure de uma instância do Azure em um modelo de nuvem. Além disso, também pode configurar análises de log para uma instância de máquina virtual do Azure. O diagnóstico de inicialização é um recurso de depuração para máquinas virtuais do Azure que facilita o diagnóstico de falhas de inicialização de máquinas virtuais. Usando o diagnóstico de inicialização, um usuário pode monitorar o estado de uma máquina virtual durante a inicialização, coletando capturas de tela e informações de logs seriais.

Diagnóstico de inicialização

O diagnóstico de inicialização coleta capturas de tela e informações de logs seriais, que precisam ser salvas no disco. O disco pode ser de dois tipos: Disco Não Gerenciado ou Disco Gerenciado do Azure.

A propriedade `bootDiagnostics` YAML é permitida em modelos de nuvem do Azure. Quando essa propriedade está definida como `true`, os diagnósticos de inicialização são ativados na implantação da máquina virtual do Azure aplicável.

O seguinte snippet YAML mostra um exemplo de como a propriedade `bootDiagnostics` é usada.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Azure_Machine_1:
    type: Cloud.Azure.Machine
    metadata:
      layoutPosition:
        - 0
        - 0
    properties:
      image: ubuntu
      flavor: small
      bootDiagnostics: true
```

Diagnósticos de inicialização também podem ser invocados em uma máquina virtual do Azure implantada como uma operação de dia 2. Navegue até a página Implantações no Cloud Assembly e selecione a implantação do Azure. O menu Ações nesta página permite alternar entre Ativar Diagnóstico de Inicialização e Desativar Diagnóstico de Inicialização.

Depois que você implantar um modelo de nuvem com o diagnóstico de inicialização ativado, a página Implantações do Cloud Assembly para a implantação indicará que o diagnóstico de inicialização está ativado. Se quiser desativar o diagnóstico de inicialização, clique no menu Ações da página Implantações e selecione Desativar diagnóstico de inicialização.

Log Analytics

O Log Analytics permite editar e executar consultas de log sobre dados coletados por Logs do Azure Monitor e, em seguida, analisar interativamente os resultados. Você pode usar as consultas do Log Analytics para recuperar registros que correspondem a critérios específicos, para ajudar a identificar tendências e padrões e fornecer uma variedade de insights de dados. Ao ativar o Log Analytics em uma máquina virtual Azure, essa máquina atuará como uma fonte de dados.

Antes de configurar análises de log em um modelo de nuvem do Cloud Assembly, você deve criar e configurar um workspace do Azure Log Analytics. Isso pode ser feito usando a opção Máquinas Virtuais no menu Monitor do Azure. Consulte a documentação do Microsoft Azure para obter mais informações.

Para configurar análises de log, você deve ter o ID do Workspace e a Chave do Workspace do Azure. Eles estão disponíveis na guia Gerenciamento do Agente do Azure, no Workspace do Log Analytics.

O exemplo de modelo de nuvem a seguir mostra como análises de log podem ser configuradas usando extensões.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Azure_Machine_1:
    type: Cloud.Azure.Machine
    properties:
      image: ubuntu
      flavor: small
    extensions:
      - autoUpgradeMinorVersion: true
        name: test-loga
        protectedSettings:
          workspaceKey: xxxxxxxxxx
        publisher: Microsoft.EnterpriseCloud.Monitoring
        settings:
          workspaceId: aaaaaaaaaa
          type: OmsAgentForLinux
          typeHandlerVersion: '1.0'
```

Depois de implantar um modelo de nuvem com Análises de Log ativadas, você pode ativá-lo ou desativá-lo usando as opções do menu Ações na página Implantações do Cloud Assembly para a implantação.

Como trabalhar com snapshots para discos de máquina virtual do Microsoft Azure no vRealize Operations Manager

Você pode criar snapshots completos ou incrementais de discos gerenciados do Microsoft Azure.

A página Implantações do Cloud Assembly para uma implantação do Azure contém um menu Ações que fornece várias opções para criar e excluir snapshots de implantações do Azure em discos gerenciados de máquinas virtuais e em discos gerenciados independentes. A lista a seguir descreve a funcionalidade de snapshot específica com suporte.

- Criar um snapshot de disco: compatível com discos externos e de processamento. Você também pode criar snapshots para um disco em um grupo de recursos diferente.
- Excluir um snapshot de disco: com suporte apenas para discos externos
- Criptografe snapshots usando um conjunto de criptografia de disco do Azure.
- Você pode fornecer pares de chave/valor como tags durante a criação de snapshots.

No momento, não há suporte para snapshots em discos não gerenciados.

Se você usar criptografia, a implementação de snapshot atual oferecerá suporte à criptografia de chave gerenciada por plataforma. Por padrão, a política de rede permite o acesso de qualquer lugar e, portanto, não é possível restringir o acesso a snapshots usando a política de rede.

Para obter mais informações sobre como usar as páginas Ações e Implantações do Cloud Assembly, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Para obter mais informações sobre o suporte a snapshots do Microsoft Azure, consulte [Criar um snapshot de um disco rígido virtual](#) na documentação do produto Microsoft.

Criar uma conta de nuvem do Amazon Web Services no vRealize Automation

Como administrador de nuvem, você pode criar uma conta de nuvem da Amazon Web Services (AWS) para regiões de conta nas quais sua equipe implantará modelos de nuvem do vRealize Automation.

O procedimento a seguir descreve como configurar uma conta de nuvem da AWS.

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se você tem a função de usuário necessária. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se tem credenciais de administrador do AWS necessárias.
- Se você não tiver acesso externo à Internet, configure um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta AWS e digite as credenciais e outros valores.
- 3 Clique em **Validar**.
As regiões de conta associadas à conta são coletadas.
- 4 Selecione as regiões para as quais deseja provisionar este recurso.
- 5 Para obter eficiência, clique em **Criar uma zona de nuvem para as regiões selecionadas**.
- 6 Se for necessário adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).



Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

- 7 Clique em **Adicionar**.

Resultados

A conta é adicionada ao vRealize Automation e as regiões selecionadas estão disponíveis para a zona de nuvem especificada.

Próximo passo

Configure recursos de infraestrutura para esta conta de nuvem.

Criar uma conta de nuvem do Google Cloud Platform no vRealize Automation

Como administrador de nuvem, você pode criar uma conta de nuvem da Google Cloud Platform (GCP) para regiões de conta nas quais sua equipe implantará modelos de nuvem do vRealize Automation.

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se você tem a função de usuário necessária. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem acesso à chave de segurança JSON da Google Cloud Platform.
- Verifique se você tem as informações de segurança necessárias para sua instância da Google Cloud Platform. É possível obter a maioria dessas informações de sua instância ou da documentação do Google.
- Se você não tiver acesso externo à Internet, configure um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).

Procedimentos

- 1 No Cloud Assembly, selecione **Infraestrutura > Conexões > Contas de nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta da Google Cloud Platform e insira as credenciais apropriadas e as informações relacionadas. Use a conta de serviço que foi criada quando o mecanismo de processamento da conta GCP de origem foi inicializado.

Como foi observado na seção **Pré-requisitos** acima, os requisitos de credencial estão disponíveis em [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#). Para criar a conta de nuvem no vRealize Automation com êxito, a conta GCP de origem deve estar com o serviço de mecanismo de processamento ativado.

No vRealize Automation, o ID do projeto faz parte do endpoint do Google Cloud Platform. Especifique-o ao criar a conta de nuvem. Durante a coleta de dados de imagens privadas específicas de projeto, o adaptador GCP do vRealize Automation consulta o API do Google Cloud Platform.

3 Clique em **Validar**.

As regiões de conta associadas à conta são coletadas.

4 Selecione as regiões para as quais deseja provisionar este recurso.**5** Para obter eficiência, clique em **Criar uma zona de nuvem para as regiões selecionadas**.**6** Se precisar de tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).

Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

7 Clique em **Adicionar**.**Resultados**

A conta é adicionada ao vRealize Automations e as regiões selecionadas estão disponíveis para a zona de nuvem especificada.

Próximo passo

Crie recursos de infraestrutura para esta conta de nuvem.

Os parágrafos a seguir fornecem algumas informações sobre a implantação de uma máquina virtual Google Cloud Platform a partir do Cloud Assembly.

Quando você adiciona uma conta de nuvem do Google Cloud Platform a um modelo de nuvem do Cloud Assembly, pode usar a propriedade YAML `useSoleTenant` para indicar que deseja implantar uma máquina virtual em um nó de tenant individual. Essa configuração permite isolar máquinas virtuais para segurança, privacidade ou outros problemas.

Para facilitar essa funcionalidade, rótulos de afinidade de nó do Google Cloud Platform são convertidos em tags no Cloud Assembly, e essas tags são aplicadas em zonas de disponibilidade do vRealize Automation onde os grupos de nós residem. Quando a propriedade `useSoleTenant` é definida como `true`, tags de restrição devem ser um dos rótulos de afinidade de nó. Além disso, para implantar uma máquina no modo de tenant individual, você deve incluir a propriedade `useSoleTenant` no modelo de nuvem, bem como as tags de restrição.

Antes de usar esse recurso, você deve criar o modelo de nó apropriado e os rótulos de afinidade de nó na Google Cloud Platform e, em seguida, criar um grupo de nós.

O seguinte exemplo YAML mostra como a propriedade `useSoleTenant` pode ser usada em modelos de nuvem do Cloud Assembly. As tags de restrição são os rótulos de afinidade de nó que foram coletados automaticamente do seu servidor Google Cloud Platform.

```
resources:
  Cloud_GCP_Machine_1:
    type: Cloud.GCP.Machine
```

```
properties:
  image: ubuntu
  flavor: c2-family
  name: demo-vm
  useSoleTenant: true
  constraints:
    -tag: 'env:prod'
    -tag: 'region:asia-east1'
```

Criar uma conta de nuvem do vCenter no vRealize Automation

Você pode adicionar uma conta de nuvem do vCenter para as regiões de conta nas quais deseja implantar modelos de nuvem do vRealize Automation.

Para fins de rede e segurança, você pode associar uma conta de nuvem vCenter com uma conta de nuvem do NSX-T ou NSX-V.

Uma conta de nuvem NSX-T pode ser associada a uma ou mais contas de nuvem do vCenter. No entanto, uma conta de nuvem NSX-V só pode ser associada a uma conta de nuvem do vCenter.

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você configurou corretamente as portas e os protocolos para oferecer suporte à conta de nuvem. Consulte o tópico *Portas e protocolos para o vRealize Automation* em *Instalar o vRealize Automation com o instalador vRealize Easy* e o tópico *Requisitos da porta* no *Guia de arquitetura de referência do vRealize Automation* na [documentação do produto vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta do vCenter e digite o endereço IP do host do vCenter Server.
- 3 Digite as credenciais de administrador do vCenter Server e clique em **Validar**.

Todos os centros de dados associados à conta são coletados por dados. Os elementos a seguir são coletados por dados, assim como todas as tags vSphere para os seguintes elementos:

- Máquinas
- Clusters e hosts
- Grupos de portas

- Repositórios de dados

- 4 Selecione pelo menos um dos centros de dados disponíveis no vCenter Server especificado para permitir o provisionamento para esta conta de nuvem.
- 5 Para obter eficiência, crie uma zona de nuvem para provisionamento para os centros de dados selecionados.

Também é possível criar zonas de nuvem como uma etapa separada de acordo com a estratégia de nuvem da organização.

Para obter informações sobre zonas de nuvem, consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).

- 6 Selecione uma conta de nuvem do NSX existente.

É possível selecionar a conta do NSX agora ou mais tarde, quando você editar a conta de nuvem.

Para obter informações sobre contas de nuvem do NSX-V, consulte [Criar uma conta de nuvem do NSX-V no vRealize Automation](#).

Para obter informações sobre contas de nuvem do NSX-T, consulte [Criar uma conta de nuvem do NSX-T no vRealize Automation](#).

Para obter informações sobre como fazer alterações de associação depois de implantar um modelo de nuvem, consulte [O que acontecerá se eu remover uma associação de conta de nuvem do NSX no vRealize Automation](#).

- 7 Se quiser adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recursos.

É possível adicionar tags agora ou mais tarde, quando você editar a conta de nuvem. Para obter informações sobre marcação, consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).



Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

- 8 Clique em **Salvar**.

Resultados

A conta de nuvem é adicionada e os centros de dados selecionados estão disponíveis para a zona de nuvem especificada. Os dados coletados, como máquinas, redes, armazenamento e volumes, estão listados na seção **Recursos** da guia **Infraestrutura**.

Próximo passo

Configure os recursos de infraestrutura restantes para essa conta de nuvem. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).

Criar uma conta de nuvem do NSX-V no vRealize Automation

Para fins de rede e segurança, é possível criar e associar uma conta de nuvem do NSX-V a uma conta de nuvem vCenter.

Uma conta de nuvem NSX-V só pode ser associada a uma conta de nuvem do vCenter.

A associação entre o NSX-V e uma conta de nuvem do vCenter deve ser configurada fora do vRealize Automation, especificamente no seu aplicativo NSX. O vRealize Automation não cria a associação entre NSX e vCenter. No vRealize Automation, você especifica uma associação que já existe no NSX.

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se tem uma conta de nuvem do vCenter para usar com esta conta de nuvem do NSX. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- Verifique se você configurou corretamente as portas e os protocolos para oferecer suporte à conta de nuvem. Consulte o tópico *Portas e protocolos para o vRealize Automation* em *Instalar o vRealize Automation com o instalador vRealize Easy* e o tópico *Requisitos da porta* no *Guia de arquitetura de referência do vRealize Automation* na [documentação do produto vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta do NSX-V e digite o endereço IP do host do NSX-V.
- 3 Digite as credenciais de administrador do NSX e clique em **Validar**.

Os ativos associados à conta são coletados.

Se o endereço IP do host do NSX não estiver disponível, a validação falhará.

- 4 Se disponível, selecione o endpoint do vCenter que representa a conta de nuvem do vCenter que foi associada a essa conta do NSX-V.

Somente contas de nuvem do vCenter que não estejam atualmente associadas a uma conta de nuvem do NSX-T ou do NSX-V estão disponíveis para seleção.

Para obter informações sobre como fazer alterações de associação depois de implantar um modelo de nuvem, consulte [O que acontecerá se eu remover uma associação de conta de nuvem do NSX no vRealize Automation](#).

- 5 Se quiser adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recursos.

É possível adicionar ou remover tags de recurso mais tarde. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).



Para obter informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

- 6 Clique em **Salvar**.

Próximo passo

É possível criar ou editar uma conta de nuvem do vCenter para associar a essa conta de nuvem do NSX. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).

Crie e configure uma ou mais zonas de nuvem para uso com os centros de dados que são usados por essa conta de nuvem. Consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).

Configure recursos de infraestrutura para esta conta de nuvem. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).

Criar uma conta de nuvem do NSX-T no vRealize Automation

Para fins de rede e segurança, você pode criar uma conta de nuvem NSX-T e associá-la a uma ou mais contas de nuvem do vCenter.

Uma conta de nuvem NSX-T pode ser associada a uma ou mais contas de nuvem do vCenter. No entanto, uma conta de nuvem NSX-V só pode ser associada a uma conta de nuvem do vCenter.

A associação entre o NSX-T e uma ou mais contas de nuvem do vCenter deve ser configurada fora do vRealize Automation, especificamente no seu aplicativo NSX. O vRealize Automation não cria a associação entre NSX e vCenter. No vRealize Automation, você especifica uma ou mais associações de configuração que já existem no NSX.

Ao criar uma conta de nuvem do NSX-T no vRealize Automation, você especifica um tipo de gerenciador e um modo NSX. Essas seleções não podem ser alteradas após a criação da conta na nuvem.

Você pode se conectar a um NSX-T Global Manager e configurar uma associação entre um NSX-T Global Manager e Local Managers no contexto da federação do NSX-T.

Para obter informações relacionadas sobre opções e recursos do NSX-T em geral, consulte a [Documentação do produto NSX-T Data Center](#).

Para facilitar a tolerância a falhas e a alta disponibilidade em implantações, cada um dos endpoints de centro de dados do NSX-T representa um cluster de três Gerenciadores do NSX.

- O vRealize Automation pode apontar para um dos Managers NSX. Usando essa opção, um Manager NSX recebe as chamadas de API do vRealize Automation.

- O vRealize Automation pode apontar para o IP Virtual do cluster. Usando essa opção, um Manager NSX assume o controle do VIP. Esse NSX Manager recebe as chamadas de API do vRealize Automation. Em caso de falha, outro nó no cluster assumirá o controle do VIP e recebe as chamadas de API do vRealize Automation.

Para obter mais informações sobre a configuração de VIP para NSX, consulte *Configurar um endereço IP virtual (VIP) para um cluster* no *Guia de instalação do NSX-T Data Center* na [documentação do VMware NSX-T Data Center](#).

- O vRealize Automation pode apontar para um VIP do balanceador de carga para balancear a carga das chamadas para os três Managers NSX. Usando essa opção, todos os três Managers NSX recebem chamadas de API do vRealize Automation.

Você pode configurar o VIP em um balanceador de carga de terceiros ou em um balanceador de carga do NSX-T.

Para ambientes de grande escala, considere usar essa opção para dividir as chamadas de API de vRealize Automation entre os três NSX Managers.

Para obter uma visão detalhada do uso do NSX-T 3.2 com o vRealize Automation, consulte a postagem do blog da VMware sobre o [VMware Network Automation com o NSX-T 3.2 e o vRealize Automation](#).

Pré-requisitos

- Verifique se você tem as credenciais de administrador necessárias e se habilitou o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se tem uma conta de nuvem do vCenter para usar com esta conta de nuvem do NSX. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- Verifique se você configurou corretamente as portas e os protocolos para oferecer suporte à conta de nuvem. Consulte o tópico *Portas e protocolos para o vRealize Automation* em *Instalar o vRealize Automation com o instalador vRealize Easy* e o tópico *Requisitos da porta* no *Guia de arquitetura de referência do vRealize Automation* na [documentação do produto vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta do NSX-T e especifique um nome e uma descrição da conta de nuvem.
- 3 Insira o endereço IP do host para a instância ou o VIP do NSX-T Manager (consulte acima para obter informações sobre o comportamento esperado que pertence às opções do NSX Manager e do VIP).

4 Insira suas credenciais de nome de usuário e senha de administrador do NSX.

5 Para **Tipo de Gerente**, selecione **Global** ou **Local** (padrão).

- Global Manager

A configuração Global Manager está disponível apenas para uso com a configuração **Modo NSX** da Política. Ela não está disponível ao usar a configuração **Modo NSX** do Manager.

A configuração Global refere-se aos recursos de federação do NSX-T, incluindo segmentos de rede globais. Somente contas de nuvem do NSX-T com a configuração Global oferecem suporte à federação do NSX-T.

Ao usar a configuração Global Manager, você será solicitado a identificar uma conta de nuvem Local Manager do NSX-T e uma conta de nuvem do vCenter Server associada.

Você não pode associar uma conta de nuvem Global Manager do NSX-T a uma conta de nuvem do vCenter como é possível fazer com uma conta de nuvem Local Manager do NSX-T. Da mesma forma como uma conta de nuvem Local Manager do NSX-T pode ser associada a várias contas de nuvem do vCenter, uma conta de nuvem Global Manager do NSX-T pode ser associada a várias contas de nuvem Local Manager do NSX-T.

- Local Manager

Use a configuração Local para definir uma conta de nuvem do NSX-T tradicional, que pode ser associada a uma ou mais contas de nuvem do vSphere. Você pode associar uma conta de nuvem Global Manager do NSX-T a uma conta de nuvem Local do NSX-T. Observe que essa também é a configuração a ser usada se você estiver criando uma conta de nuvem do NSX-T de destino nova e vazia para migração do NSX-V para o NSX-T.

Não será possível alterar a configuração **Tipo do Manager** depois que você criar a conta de nuvem.

6 Para **Modo NSX**, selecione **Política** ou **Manager**.

- Modo de Política (padrão)

O modo de Política está disponível para o NSX-T 3.0, o NSX-T 3.1 e versões posteriores. Essa opção permite que o vRealize Automation use os recursos adicionais disponíveis na API da Política do NSX-T.

Se estiver usando o NSX-T com uma conta de nuvem do VMware Cloud on AWS em um modelo de nuvem, a conta de nuvem NSX-T deve usar o **modo NSX** de Política.

A configuração de Política faz referência ao formato de API de Política do NSX-T do NSX-T.

- Modo do Manager

Endpoints ou contas de nuvem existentes do NSX-T que são atualizados de uma versão anterior do vRealize Automation que não fornecia uma opção de Política são tratados como contas de nuvem do NSX-T no modo do Manager.

O modo do Manager é compatível com o NSX-T 2.4, NSX-T 3.0, e NSX-T 3.1 e versões posteriores.

Se você especificar o modo do Manager, use a opção do modo Manager para outras contas de nuvem do NSX-T até o vRealize Automation apresentar um caminho de migração do modo Manager para o modo de Política.

Alguns vRealize Automation opções para o NSX-T exigem o NSX-T 3.0 ou superior, incluindo a adição de tags a componentes NIC de máquina virtual no modelo de nuvem.

A configuração do Manager faz referência ao formato de API NSX-T Manager do NSX-T.

Se você tiver contas de nuvem do NSX-T existentes que foram criadas antes da introdução do método de Política no vRealize Automation 8.2, elas usarão o método de API do Manager. Recomenda-se aguardar até que a API do Manager para a ferramenta de migração da API da Política seja disponibilizada no vRealize Automation. Se preferir não aguardar, substitua as contas de nuvem do NSX-T existentes por novas contas de nuvem do NSX-T que especificam o método da API da Política.

Não será possível alterar o valor do **modo NSX** depois de criar a conta de nuvem.

- 7 Clique em **Validar** para confirmar as credenciais em relação ao tipo do NSX Manager e o modo do NSX selecionados.

Os ativos associados à conta são coletados.

Se o endereço IP do host do NSX não estiver disponível, a validação falhará.

- 8 Em **Associações**, adicione uma ou mais contas de nuvem do vCenter a serem associadas a esta conta de nuvem do NSX-T. Você também pode remover associações existentes da conta de nuvem do vCenter.

Somente contas de nuvem do vCenter que não estejam atualmente associadas no vRealize Automation a uma conta de nuvem do NSX-T ou do NSX-V estão disponíveis para seleção.

Consulte [O que posso fazer com o mapeamento do NSX-T para vários vCenters no vRealize Automation](#).

Para obter informações sobre como fazer alterações de associação depois de implantar um modelo de nuvem ou excluir a conta de nuvem depois de implantar um modelo de nuvem, consulte [O que acontecerá se eu remover uma associação de conta de nuvem do NSX no vRealize Automation](#).

- 9 Se quiser adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recursos.

É possível adicionar ou remover tags de recurso mais tarde. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).



Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

10 Clique em **Salvar**.

Próximo passo

É possível criar ou editar uma conta de nuvem do vCenter para associar a essa conta de nuvem do NSX. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).

Crie e configure uma ou mais zonas de nuvem para uso com os centros de dados que são usados por essa conta de nuvem. Consulte [Saiba mais sobre as zonas de nuvem do Cloud Assembly](#).

Configure recursos de infraestrutura para esta conta de nuvem. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).

Para amostras do uso de opções do NSX-T em modelos de nuvem do vRealize Automation, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation

Como administrador de nuvem, você pode criar uma conta de nuvem da VMware Cloud on AWS para regiões de conta nas quais sua equipe implantará modelos de nuvem do vRealize Automation.

O VMware Cloud on AWS exige alguns procedimentos de configuração exclusivos no vRealize Automation. Para configurar corretamente o vRealize Automation para VMware Cloud on AWS, incluindo a configuração de valores de um token de API para a conta de nuvem e a configuração de regras de firewall do gateway para o proxy de nuvem, consulte o fluxo de trabalho do [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#).

Pré-requisitos

- Verifique se você tem as credenciais de administrador do VMware Cloud on AWS necessárias, incluindo credenciais CloudAdmin do VMware Cloud on AWS para o SDDC de destino no vCenter, e que você tenha ativado o acesso HTTPS na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Se você não tiver acesso externo à Internet, configure um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).
- Verifique se você configurou as regras de acesso e firewall necessárias no SDDC. Consulte [Preparar seu VMware Cloud on AWS SDDC para se conectar a contas de nuvem do VMware Cloud on AWS no vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem**, clique em **Adicionar Conta de Nuvem** e selecione o tipo de conta do VMware Cloud on AWS.

- 2 Adicione o **Token de API do VMC** para sua organização acessar os SDDCs disponíveis.

É possível criar um novo token ou usar um token existente para a sua organização na página vinculada **Tokens de API**. Para obter detalhes, consulte [Criar uma conta de nuvem do VMware Cloud on AWS no vRealize Automation em um fluxo de trabalho de amostra](#).

- 3 Selecione o SDDC a ser disponibilizado para implantações.

Os SDDCs do NSX-V não são compatíveis e não aparecem na lista.

Os valores de endereço IP/FQDN do Gerenciador do vCenter e do NSX-T são preenchidos automaticamente com base no SDDC.

- 4 Digite o nome do usuário e senha do vCenter para o SDDC especificado, se for diferente do valor padrão de cloudadmin@vmc.local.

- 5 Clique em **Validar** para confirmar seus direitos de acesso ao vCenter especificado e verifique se o vCenter está em execução.

Os centros de dados associados à conta são coletados.

- 6 Para obter eficiência, crie uma zona de nuvem de provisionamento para o SDDC selecionado.

Também é possível criar zonas de nuvem como uma etapa separada de acordo com a estratégia de nuvem da organização.

- 7 Se quiser adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recursos.

É possível adicionar ou remover tags de recurso mais tarde. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).



Para obter mais informações sobre como as tags de capacidade e as tags de restrição ajudam a controlar os posicionamentos de implantação, confira o tutorial de vídeo [Tags de capacidade e posicionamento](#).

Assim como acontece com as VMs implantadas no vSphere, você pode configurar tags de máquina para que uma VM seja implantada no VMware Cloud on AWS. Você também pode atualizar a tag da máquina após a implantação inicial. Essas tags de máquina permitem que o vRealize Automation atribua dinamicamente uma VM a um grupo de segurança apropriado do NSX-T durante a implantação. Para obter informações relacionadas, consulte [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#).

- 8 Clique em **Salvar**.

Resultados

A conta de nuvem é adicionada e o SDDC selecionado está disponível para a zona de nuvem especificada.

Próximo passo

Para configurar corretamente o vRealize Automation para VMware Cloud on AWS, consulte [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#).

Para obter informações relacionadas sobre o VMware Cloud on AWS fora do vRealize Automation, consulte a [documentação do VMware Cloud on AWS](#).

Criar uma conta de nuvem do VMware Cloud Foundation

Você pode configurar um VMware Cloud Foundation (VCF) como uma conta de nuvem no Cloud Assembly para usar domínios de carga de trabalho.

Uma conta de nuvem do VCF permite que você incorpore uma carga de trabalho do VCF no Cloud Assembly para facilitar uma solução de gerenciamento de nuvem híbrida abrangente. O Cloud Assembly oferece vários pontos de entrada dos quais você pode ativar a página de configuração da conta de nuvem do VCF. Se você acessar essa página usando o botão **Adicionar Conta de Nuvem** na guia Domínio da Carga de Trabalho da integração com o SDDC, a carga de trabalho será pré-selecionada, incluindo as informações básicas para o vCenter e o NSX Manager.

Pré-requisitos

Você deve ter uma instância do VMware SDDC Manager 4.1 ou superior configurada como uma integração do Cloud Assembly para uso com essa conta de nuvem. Para obter mais informações, consulte [Configurar uma integração do VMware SDDC Manager](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.

- 2 Selecione o Tipo de conta da nuvem do VCF e insira um **Nome** e uma **Descrição**.

- 3 Insira o FQDN e as credenciais para a instância do SDDC Manager que você está usando com essa conta de nuvem.

Você poderá pular essa etapa se já tiver configurado a instância do SDDC Manager que usará com essa conta.

- 4 Selecione um ou mais domínios de carga de trabalho que você deseja usar com essa conta de nuvem do VCF.
- 5 Se quiser que o Cloud Assembly use credenciais de serviços gerenciados do Cloud Foundation para o vCenter e o NSX, selecione **Criar credenciais de serviço automaticamente**. Mais tarde, se quiser alterar essas credenciais, você deverá usar o mecanismo VCF para o gerenciamento de senhas.

Se você selecionar essa opção, poderá ignorar as etapas 7 e 8.

- 6 Insira as credenciais necessárias para acessar o vCenter associado a essa conta de nuvem.

- 7 No cabeçalho do NSX Manager, insira as credenciais do NSX se quiser inserir manualmente as credenciais da conta de nuvem do VCF ou clique em Criar e Validar Credenciais de Serviço se quiser que o Cloud Assembly crie e valide as credenciais do NSX.
- 8 Insira as credenciais necessárias para acessar a rede NSX-T associada a essa conta de nuvem.
- 9 Se for o caso, selecione o modo NSX.
- 10 Clique em **Validar** para confirmar uma conexão com o SDDC Manager.
- 11 Se aplicável, selecione os centros de dados que você deseja provisionar sob o título Configuração. Clique na caixa de seleção se quiser criar uma zona de nuvem para os centros de dados selecionados.
- 12 Se você usar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly e Criação de uma estratégia de marcação](#).
- 13 Clique em **Salvar**.

Resultados

Essa conta de nuvem traz o domínio de carga de trabalho selecionado associado ao SDDC Manager especificado para o Cloud Assembly para uso.

Se quiser gerenciar domínios de carga de trabalho adicionais usando o vRealize Automation, você deverá repetir esse processo para cada domínio.

Próximo passo

Depois de configurar a conta da nuvem do VCF, você poderá selecionar a conta na página principal da conta da nuvem e clicar em **Configurar Nuvem** para iniciar o assistente de Início Rápido do VMware Cloud Foundation que configurará sua nuvem.

Para obter mais informações sobre o assistente de Início Rápido, consulte [Como começar a trabalhar com o vRealize Automation usando o Início Rápido do VMware Cloud Foundation](#), em Introdução.

Criar uma conta de nuvem do VMware Cloud Director no vRealize Automation

Você pode criar uma conta de VMware Cloud Director cloud no vRealize Automation para implantar máquinas virtuais do Cloud Director usando objetos independentes de nuvem. O Cloud Director aceita o provisionamento flexível de recursos de rede, armazenamento e processamento e oferece uma experiência baseada em portal para gerenciar os vCenters, seus dispositivos de rede NSX-T e NSX-V e os centros de dados virtuais associados por meio de um catálogo.

A conta de nuvem VMware Cloud Director oferece suporte à criação de máquinas virtuais independentes do Cloud Director sem vApp. Há suporte para três cenários de provisionamento de máquinas virtuais do Cloud Director por meio de modelos de nuvem do Cloud Assembly:

- Máquinas virtuais

- Redes conectadas a máquinas virtuais
- Máquinas virtuais com disco/s adicionais

Para obter mais informações sobre como trabalhar com o VMware Cloud Director, incluindo informações sobre como configurar vários servidores para alta disponibilidade, consulte a documentação oficial do <https://docs.vmware.com/br/VMware-Cloud-Director/index.html>.

A conta de nuvem VMware Cloud Director suporta até 1000 máquinas virtuais com vRealize Automation no modo de sustentação.

O procedimento a seguir descreve como configurar uma conta de nuvem do VMware Cloud Director no vRealize Automation Cloud Assembly.

Pré-requisitos

- Configure uma implantação do VMware Cloud Director 10.2.0, 10.2.1, 10.2.2, 10.3 ou 10.3.1 com uma ou mais organizações apropriadas.
- Os usuários especificados para essa integração devem ter privilégios de Administrador da Organização para ler modelos aplicáveis e criar máquinas virtuais, bem como para visualizar outros recursos, como políticas de processamento, discos, centros de dados virtuais, etc. A conta de nuvem do VCD para vRealize Automation funciona em um contexto de tenant no Cloud Director para você se conectar a uma organização individual no Cloud Director com suas credenciais de tenant. Para obter mais informações sobre as credenciais necessárias, consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Você deve configurar o armazenamento, a rede, a imagem e os tipos apropriados ou a política de dimensionamento, na sua instância do VMware Cloud Director e mapear esses objetos no vRealize Automation Cloud Assembly antes ou depois de configurar sua integração. A lista a seguir explica como objetos virtuais do VMware Cloud Director devem ser mapeados para objetos do vRealize Automation no Cloud Assembly.
 - Redes (isoladas, diretas, roteadas) da organização do VMware Cloud Director: mapeamento para redes do vRealize Automation. Nenhum pool de IPs estáticos pode ser definido para o adaptador de rede.
 - Políticas de dimensionamento de máquina virtual do VMware Cloud Director: mapeamento para tipos do vRealize Automation.
 - Políticas de armazenamento do VMware Cloud Director: mapeamento para perfis de armazenamento do vRealize Automation.
 - Imagens (mídia de inicialização OVF ou ISO) do VMware Cloud Director: mapeamento para imagens do vRealize Automation. As imagens podem ser modelo ou mídia de vApp, como arquivos ISO. Se você usar ISO, uma máquina virtual "vazia" será criada e a mídia será anexada como mídia de inicialização.
 - Máquinas virtuais do VMware Cloud Director: mapeamento para processamentos do vRealize Automation.

- Discos de máquinas virtuais do VMware Cloud Director: mapeamento para volumes de nuvem do vRealize Automation.

Mapeie esses objetos do VMware Cloud Director para os objetos do vRealize Automation usando as opções nas páginas **Configurar > Infraestrutura >** no Cloud Assembly. Consulte os tópicos relevantes em [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#) para obter informações detalhadas sobre o mapeamento de objetos no vRealize Automation.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Contas de Nuvem** e clique em **Adicionar Conta de Nuvem**.
- 2 Selecione o tipo de conta de nuvem do VMware Cloud Director e insira um **Nome** e uma **Descrição**.
- 3 Insira as informações de conta apropriadas necessárias para acessar o servidor VMware Cloud Director.
- 4 Insira a URL base que será usada para se conectar ao servidor VMware Cloud Director.
- 5 Insira um **Nome de usuário** e uma **Senha** adequados para uma conta válida que possa acessar a instância especificada do Cloud Director.
- 6 Insira o nome desejado da **Organização** que será usado com esta integração.
No vCloud Director, uma organização contém usuários, os vApps que eles criam e os recursos que os vApps usam.
- 7 Clique em **Validar**.
Durante a validação, você pode ser solicitado a aceitar um certificado. Quando a conexão é validada, você pode selecionar configurações adicionais.
- 8 Se você usar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 9 Após a sua validação, a página exibirá uma lista de centros de dados virtuais do Cloud Director disponíveis para você pode selecionar. Selecione o centro de dados apropriado. Essa seleção determina as regiões do Director nas quais você pode implantar.
- 10 Clique em **Adicionar** para adicionar a conta de nuvem do VMware Cloud Director ao vRealize Automation.

Resultados

A conta de nuvem do VMware Cloud Director está disponível para configuração no vRealize Automation. As redes associadas à instância do Cloud Director estão disponíveis para configuração na página **Recursos > Redes** do Cloud Assembly. Você pode configurar os perfis de armazenamento apropriados e usar a conta de nuvem para criar implantações nos modelos de nuvem. Além disso, certifique-se de que um projeto apropriado esteja configurado no Cloud Assembly para uso com a instância do Cloud Director.

Próximo passo

A conta de nuvem do VMware Cloud Director está pronta para uso nos modelos de nuvem do Cloud Assembly.

Veja a seguir um exemplo de modelo de nuvem de uma implantação básica do VMware Cloud Director.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      constraints:
        - tag: net1:isolated
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 2
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: image1
      flavor: small
      storage:
        constraints:
          - tag: storage:development
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
      networks:
        - network: '${resource.Cloud_Network_1.id}'
```

As seguintes ações de dia 2 são permitidas em máquinas virtuais implantadas do VMware Cloud Director:

- Ligar
- Desligar
- Suspendar
- Criar snapshot

- Reverter para snapshot
- Remover snapshot
- Adicionar disco
- Remover disco
- Redimensionar disco (observação: é permitido somente aumentar o tamanho do disco)
- Redimensionar disco de inicialização

Quando que um blueprint é implantado, os usuários podem aplicar tags em máquinas recém-provisionadas no vRealize Automation. Essas tags do vRealize Automation são mapeadas para metadados do VMware Cloud Director, que podem ser recuperados usando a API do VMware Cloud Director. Os usuários também podem marcar outros recursos do vRealize Automation, mas apenas as máquinas no lado do VMware Cloud Director são atualizadas, pois este é o único tipo de recurso compatível com essa funcionalidade.

Quando que um blueprint é implantado, os usuários podem redimensionar o disco de inicialização de uma máquina virtual. Além disso, não há suporte para discos regulares. Nesse caso, os clientes só precisam anexar um recurso de disco a um recurso de máquina. Quando tudo estiver implantado, você poderá usar a opção "atualizar o disco de inicialização" ou "atualizar o disco" para aumentar, mas não diminuir, o tamanho do disco desejado.

Quando um blueprint é implantado, os usuários podem alterar uma política de dimensionamento de máquina virtual usando a opção de redimensionamento da configuração de tipo do vRealize Automation. Uma vez selecionada, a máquina virtual do VMware Cloud Director usará a política de dimensionamento fornecida.

Esse recurso requer que o **Pacote de Direitos Padrão** atribuído à função de Administrador da Organização contenha o direito "Alterar políticas de processamento", cujo código interno é `VAPP_EDIT_VM_COMPUTE_POLICY`. Em seguida, esse direito deve ser ativado para o Administrador da Organização. Caso contrário, a operação de redimensionamento falhará com um erro 403: `Either you need some or all of the following rights [VAPP_EDIT_VM_COMPUTE_POLICY] to perform operations.`

Você pode redimensionar o disco de inicialização de uma máquina virtual do VMware Cloud Director como uma operação de dia 2 selecionando a máquina virtual na página Implantações. No entanto, você deve desativar o Provisionamento rápido antes de tentar redimensionar o disco de inicialização, ou o seguinte erro poderá ocorrer:

```
Request timed out after 120 minutes. Please configure project request timeout
parameter for long running resource requests.
```

Observe que esse requisito aplica-se somente a máquinas virtuais criadas a partir de discos de Modelo de vApp. Ele não se aplica a máquinas virtuais criadas a partir de arquivos ISO.

O procedimento a seguir descreve como desativar o provisionamento rápido.

- 1 Faça login no VMware Cloud Director como administrador do sistema: `https://vcd_url/provider with the system user`

- 2 Clique em VDCs de organização.
- 3 Selecione a organização de destino.
- 4 Clique em Armazenamento (em Políticas).
- 5 Desative **Provisionamento rápido**.

Usando logs e outros recursos para solucionar problemas de contas de nuvem VMware Cloud Director no vRealize Automation

Se você encontrar problemas ao configurar ou usar uma conta de nuvem do VMware Cloud Director no vRealize Automation, poderá consultar logs e outros recursos, conforme descritos abaixo.

Solução de problemas de conexão da conta na nuvem do VMware Cloud Director

Se o adaptador VMware Cloud Director não estiver listado na tela de criação da conta na nuvem ou não estiver respondendo, você pode usar o seguinte comando para verificar o status fazendo login no host kubernetes do vRealize Automation e verificando o status do pod do adaptador:

```
root@host [ ~ ]# kubectl -n prelude get pods | grep adapter-host-service-app
adapter-host-service-app-65f5c945bb-p6hpn      1/1      Running    0          4dlh
```

Se o adaptador VMware Cloud Director não puder se comunicar com a máquina física do Cloud Director, um erro será exibido na tela da conta de nuvem com instruções sobre exceções de conexão e processamento. O erro também aparece nos logs.

Trabalhando com logs VMware Cloud Director

O arquivo de log principal do adaptador do VMware Cloud Director reside sob o local (pod) `dir /var/log/adapter-host-service-app.log` e no caso do adaptador em execução dentro do host do dispositivo do vRealize Automation, esse log também é copiado para o `/services-logs/prelude/adapter-host-service-app/file-logs/`. Por padrão, a maioria do log é restrita a níveis de DEBUG ou INFO. Você pode alterar a configuração dos seguintes agentes de log para permitir um registro mais detalhado para fins de depuração:

- `org.apache.cxf.services=INFO` - este agente fornece informações detalhadas para a comunicação entre o adaptador e o VMware Cloud Director.
- `com.vmware.vra.vcloud.director.adapter=TRACE` - este agente fornece informações detalhadas para a comunicação entre o adaptador e o vRealize Automation.

Há três maneiras de acessar os logs:

- log de acesso por login no pod do adaptador

```
root@host [ ~ ]# kubectl -n prelude exec -ti adapter-host-service-app-65f5c945bb-p6hpn --
bash
root [ / ]# less /var/log/adapter-host-service-app.log
```

- acessar log usando kubectl

```
root@host [ ~ ]# kubectl -n prelude get logs adapter-host-service-app-65f5c945bb-p6hpn
```

- log de acesso usando a cópia local do host kubernetes do adaptador

```
root@host [ ~ ]# less /services-logs/prelude/adapter-host-service-app/file-logs/adapter-host-service-app.log
```

Você pode consultar ou alterar a configuração do agente de log por meio do /actuator/loggers REST API endpoint.

- Exemplo de ativação do rastreamento de comunicação do cliente VMware Cloud Director via curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "INFO"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Exemplo de desativação do rastreamento de comunicação do cliente VMware Cloud Director via curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "OFF"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Exemplo de obtenção da configuração atual para a comunicação do cliente VMware Cloud Director via curl:

```
curl http://{adapter-url}/actuator/loggers/org.apache.cxf.services
...
{"configuredLevel":"OFF","effectiveLevel":"INFO"}
```

Há outros parâmetros que podem ser ajustados para alterar o desempenho do VMware Cloud Director.

- `vcd.max.thread.count` - este parâmetro determina o grau máximo de paralelismo ao executar chamadas de API do VMware Cloud Director. O padrão é 128.

Observação Diminuir o valor desse parâmetro reduzirá a tensão no back-end do VMware Cloud Director ao executar a enumeração, mas poderá diminuir o desempenho da enumeração.

- `VCD_ADAPTER_PAGINATION_SIZE_IMAGES` - esse parâmetro determina o tamanho da página ao executar a enumeração da imagem. O padrão é 50.

Observação Diminua esse parâmetro se ocorrerem erros de tempo limite do adaptador durante a enumeração da imagem.

Como integrar o vRealize Automation a outros aplicativos

Integrações permitem adicionar sistemas externos ao vRealize Automation.

As integrações incluem o vRealize Orchestrator, o gerenciamento de configuração e outros sistemas externos, como GitHub, Ansible, Puppet, e os provedores de IPAM externos, como Infoblox.

Observação Se você não tiver acesso externo à internet e sua integração exigir, poderá configurar um proxy de servidor de internet. Consulte [Como configurar um servidor proxy de Internet para o vRealize Automation](#).

Como usar a integração do Git no Cloud Assembly

O Cloud Assembly oferece suporte à integração com vários tipos de repositórios Git, para que você possa gerenciar VMware Cloud Templates e scripts de ação sob controle de origem. Essa funcionalidade facilita a auditoria e a responsabilidade dos processos em torno da implantação.

O Cloud Assembly oferece suporte a diferentes tipos de integração Git, conforme descrito na lista a seguir. Cada uma dessas opções é uma integração separada.

- Nuvem do GitHub, GitHub Enterprise no local
- Nuvem do GitLab, GitLab Enterprise no local
- BitBucket no local

É necessário ter um repositório Git local apropriado configurado com acesso a todos os usuários designados para configurar a integração do Git ao Cloud Assembly. Além disso, você deve salvar seus modelos de nuvem em uma estrutura específica para que eles sejam detectados pelo Git. Para criar uma integração com o GitLab ou GitHub, selecione **Infraestrutura > Conexões > Integrações** no Cloud Assembly e, em seguida, faça a seleção apropriada. Será necessário a URL e o token do repositório de destino.

Quando a integração do Git é configurada com um repositório existente, todos os modelos de nuvem associados aos projetos selecionados ficam disponíveis para usuários qualificados. É possível usar esses modelos com uma implantação existente ou como base para uma nova implantação. Quando você adicionar um projeto, é necessário selecionar algumas propriedades referentes ao local e como elas são armazenadas no Git.

É possível salvar ações em um repositório Git diretamente do Cloud Assembly. Você pode criar scripts de ação de versão diretamente para o Git ou pode criar versões no Cloud Assembly. Se você criar uma versão de uma ação no Cloud Assembly, ela será automaticamente salva no Git como uma versão. Modelos de nuvem são um pouco mais complicados, pois você não pode adicioná-los diretamente a uma integração com o Git a partir do Cloud Assembly. Você deve salvá-los diretamente em uma instância do Git e, em seguida, poderá recuperá-los do Git ao trabalhar com a página de gerenciamento de modelo de nuvem no Cloud Assembly.

Antes de começar

É necessário criar e salvar seus modelos de nuvem em uma estrutura específica para que eles sejam detectados pelo GitLab ou GitHub.

- Configure e armazene modelos de nuvem a serem integrados corretamente ao GitLab. Somente modelos válidos são importados para o GitLab.
 - Crie uma ou mais pastas designadas para os modelos de nuvem.
 - Todos os modelos de nuvem devem ser armazenados em arquivos `blueprint.yaml`.
 - Certifique-se de que a parte superior de seus modelos inclua as propriedades `name:` e `version:.`
- Extraia uma chave de API para o repositório aplicável. Na sua conta do Git, selecione seu login no canto superior direito e navegue até o menu Configurações. Selecione **Tokens de Acesso** e, em seguida, nomeie seu token e defina uma data de expiração. Depois selecione API e crie o token. Copie o valor resultante e salve-o.

As diretrizes a seguir devem ser observadas para todos os modelos de nuvem usados com a integração do Git.

- Cada modelo de nuvem deve residir em uma pasta separada.
- Todos os modelos de nuvem devem ser nomeados como `blueprint.yaml`.
- Todos os arquivos YAML de modelo de nuvem devem usar campos `name` e `version`.
- Somente modelos de nuvem válidos são importados.
- Se você atualizar um modelo de nuvem de rascunho importado do Git e seu conteúdo for diferente daquele na versão superior, o rascunho não será atualizado em sincronizações subsequentes, e uma nova versão será criada. Se você deseja atualizar um modelo e também permitir a sincronização adicional do Git, deverá criar uma nova versão após as alterações finais.
- [Configurar a integração de modelos de nuvem com o GitLab no Cloud Assembly](#)
Este procedimento demonstra como configurar a integração com o GitLab no Cloud Assembly, para que você possa trabalhar com modelos de nuvem no repositório e baixar automaticamente os modelos salvos que estão associados a projetos designados. Para usar modelos de nuvem com o GitLab, é necessário criar uma conexão com uma instância apropriada do GitLab e, em seguida, salvar os modelos desejados nessa instância.
- [Configurar a integração do GitHub no Cloud Assembly](#)
É possível integrar o serviço de hospedagem de repositórios com base na nuvem do GitHub no Cloud Assembly
- [Configurar a integração do bitbucket no Cloud Assembly](#)
O Cloud Assembly é compatível com a integração com o bitbucket para uso como um repositório baseado em git para scripts de ação do ABX e VMware Cloud Templates.

Configurar a integração de modelos de nuvem com o GitLab no Cloud Assembly

Este procedimento demonstra como configurar a integração com o GitLab no Cloud Assembly, para que você possa trabalhar com modelos de nuvem no repositório e baixar automaticamente os modelos salvos que estão associados a projetos designados. Para usar modelos de nuvem com o GitLab, é necessário criar uma conexão com uma instância apropriada do GitLab e, em seguida, salvar os modelos desejados nessa instância.

Quando a integração do GitLab é configurada com um repositório existente, todos os modelos de nuvem associados aos projetos selecionados ficam disponíveis aos usuários qualificados. É possível usar esses modelos com uma implantação existente ou como base para uma nova implantação. Quando você adicionar um projeto, é necessário selecionar algumas propriedades referentes ao local e como elas são armazenadas no GitLab.

Observação Não é possível forçar modelos de nuvem novos ou atualizados para o repositório Git a partir do Cloud Assembly. Além disso, não é possível forçar novos modelos para o repositório a partir do Cloud Assembly. Para adicionar modelos de nuvem a um repositório, os desenvolvedores devem usar a interface do Git.

Se você atualizar um modelo de nuvem de rascunho importado do Git e seu conteúdo for diferente daquele na versão superior, o rascunho não será atualizado em sincronizações subsequentes, e uma nova versão será criada. Se quiser atualizar um modelo de nuvem e também permitir a sincronização adicional do Git, você deverá criar uma nova versão após as alterações finais.

Depois de configurar seus modelos de nuvem para uso com o GitLab e coletar as informações necessárias, você deverá configurar a integração com a instância do GitLab. Em seguida, será possível importar os modelos de nuvem designados para o GitLab. É possível visualizar uma demonstração em vídeo desse procedimento em <https://www.youtube.com/watch?v=h0vqo63Sdgg>.

Pré-requisitos

- Extraia uma chave de API para o repositório aplicável. Na sua conta do GitLab, selecione seu login no canto superior direito e navegue até o menu Configurações. Selecione Tokens de Acesso, dê um nome para seu token e defina uma data de expiração. Depois selecione API e crie o token. Copie o valor resultante e salve-o.

É necessário ter um repositório Git local apropriado configurado com acesso a todos os usuários designados para configurar a integração do Git ao Cloud Assembly. Além disso, é necessário criar e salvar seus modelos de nuvem em uma estrutura específica para que eles sejam detectados pelo GitLab.

- Configure e armazene modelos de nuvem a serem integrados corretamente ao GitLab. Somente modelos válidos são importados para o GitLab. Consulte [Como usar a integração do Git no Cloud Assembly](#).

Procedimentos

- 1 Configurar a integração com seu ambiente do GitLab no Cloud Assembly.
 - a Selecione **Infraestrutura > Integrações > Adicionar Novo** e escolha GitLab.
 - b Insira a **URL** da sua instância do GitLab. Para uma instância do GitLab de software como serviço, na maioria dos casos, ela será gitlab.com.
 - c Insira o **Token**, também conhecido como chave de API, para a instância do GitLab especificada. Consulte os pré-requisitos acima para obter informações sobre como extrair o token da sua instância do GitLab.
 - d Adicione um nome e uma descrição apropriados.
 - e Clique em **Validar** para verificar a conexão.
 - f Adicione tags de recurso, se desejado. Consulte [Como usar tags de capacidade no Cloud Assembly](#) para informações adicionais.
 - g Clique em **Adicionar**.
- 2 Configure a conexão do GitLab para aceitar modelos de nuvem em um repositório apropriado.
 - a Selecione **Infraestrutura > Integrações** e escolha a integração GitLab apropriada.
 - b Selecione **Projetos**.
 - c Selecione **Novo Projeto** e crie um nome para o projeto.
 - d Insira o caminho do **Repositório** no GitLab. Normalmente, esse é o nome do usuário da conta principal acrescentada ao nome do repositório.
 - e Insira a **Ramificação** do GitLab apropriada que você deseja usar.
 - f Se apropriado, digite o nome da **Pasta**. Se deixado em branco, todas as pastas estarão disponíveis.
 - g Digite um **Tipo** apropriado. Se apropriado, digite o nome da pasta. Se deixado em branco, todas as pastas estarão disponíveis.
 - h Clique em **Avançar** para concluir a adição do repositório.

Quando você clicar em **Seguinte**, será iniciada uma tarefa de sincronização automatizada que importa modelos de nuvem para a plataforma.

Quando as tarefas de sincronização estiverem concluídas, uma mensagem indicará que os modelos de nuvem foram importados.

Resultados

Agora, você pode recuperar modelos de nuvem do GitLab.

Configurar a integração do GitHub no Cloud Assembly

É possível integrar o serviço de hospedagem de repositórios com base na nuvem do GitHub no Cloud Assembly

É necessário um token do GitHub válido para configurar a integração do GitHub no Cloud Assembly. Consulte a documentação do GitHub para obter informações sobre como criar e localizar o token.

Pré-requisitos

- É necessário ter acesso ao GitHub.
- Configure e armazene modelos de nuvem a serem integrados corretamente ao GitHub. Somente modelos de nuvem válidos são importados para o GitHub. Consulte [Como usar a integração do Git no Cloud Assembly](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione GitHub.
- 3 Digite as informações necessárias na página de configuração do GitHub.
- 4 Clique em **Validar** para verificar a integração.
- 5 Se for necessário adicionar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 6 Clique em **Adicionar**.
- 7 Configure a conexão do GitHub para aceitar modelos de nuvem em um repositório apropriado.
 - a Selecione **Infraestrutura > Integrações** e escolha a integração do GitHub apropriada.
 - b Selecione **Projetos**.
 - c Selecione **Novo Projeto** e crie um nome para o projeto.
 - d Digite o caminho do **Repositório** no GitHub. Normalmente, esse é o nome do usuário da conta principal acrescentada ao nome do repositório.
 - e Digite a **Ramificação** do GitHub apropriada que deseja usar.
 - f Se apropriado, digite o nome da **Pasta**. Se deixado em branco, todas as pastas estarão disponíveis.
 - g Digite um **Tipo** apropriado.
 - h Clique em **Avançar** para concluir a adição do repositório.

Será iniciada uma tarefa de sincronização automatizada que importa modelos de nuvem para a plataforma.

Quando as tarefas de sincronização estiverem concluídas, uma mensagem indicará que os modelos de nuvem foram importados.

Resultados

O GitHub está disponível para uso em blueprints do Cloud Assembly.

Próximo passo

Agora, você pode recuperar modelos de nuvem do GitHub.

Configurar a integração do bitbucket no Cloud Assembly

O Cloud Assembly é compatível com a integração com o bitbucket para uso como um repositório baseado em git para scripts de ação do ABX e VMware Cloud Templates.

No Cloud Assembly, você pode trabalhar com dois tipos de itens de repositório usando a integração do bitbucket: VMware Cloud Templates ou scripts de ação do ABX. Você deve sincronizar projetos com os quais deseja trabalhar antes de usar uma integração do bitbucket. As ações do ABX oferecem suporte de write-back para o repositório do bitbucket, mas não é possível gravar novamente os modelos de nuvem a partir da integração. Se você quiser criar novas versões de arquivos de modelo de nuvem, deverá criar manualmente.

Pré-requisitos

- Configure uma implantação do Bitbucket Server no local com um ou mais projetos baseados em modelos de ABX ou nuvem que você deseja usar com suas implantações. No momento, não há suporte para o Bitbucket Cloud.
- Crie ou designe o projeto do Cloud Assembly ao qual associar sua integração do bitbucket.
- Arquivos de modelo de nuvem a serem sincronizados com uma integração do Bitbucket devem se chamar `blueprint.yaml`.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione o bitbucket.
- 3 Digite as informações de resumo e as credenciais do bitbucket na página de resumo da nova integração do bitbucket.
- 4 Para verificar a integração, clique em **Validar**.
- 5 Se usar adição de tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 6 Clique em **Adicionar**.
- 7 Selecione a guia Projetos na página principal para a integração do bitbucket associar um projeto a ela.
- 8 Selecione o projeto a ser associado com essa integração do bitbucket.

9 Clique em **Avançar** para adicionar um repositório ao projeto do bitbucket e indicar o tipo de repositório que você está adicionando e, em seguida, especifique o nome do **Repositório**, a **Ramificação** e a **Pasta**.

10 Clique em **Adicionar**.

Se desejar adicionar um ou mais repositórios a um projeto, clique em **Adicionar repositório**.

Resultados

A integração do bitbucket está configurada com a configuração do repositório especificado e você pode visualizar e trabalhar com ações do ABX e o modelo de nuvem contidos nos repositórios configurados. Quando você adiciona um projeto a uma integração do bitbucket, uma operação de sincronização é executada para extrair as versões mais recentes dos scripts de ação do ABX e os arquivos de modelo de nuvem do repositório designado. A guia Histórico na página de integração do bitbucket mostra registros de todas as operações de sincronização para a integração. Por padrão, os arquivos são sincronizados automaticamente a cada 15 minutos, mas é possível sincronizar manualmente um arquivo, basta selecioná-lo e clicar em **SINCRONIZAR** a qualquer momento.

Próximo passo

Você pode trabalhar com ações do ABX na página Extensibilidade do Cloud Assembly e com blueprints, na página Design. Se você salvar uma versão alterada de uma ação do ABX na área de extensibilidade do Cloud Assembly, a nova versão do script será criada e gravada novamente no repositório.

Como configurar uma integração externa de IPAM no vRealize Automation

Você pode criar um ponto de integração de IPAM externo específico de provedor para gerenciar os endereços IP usados nas suas implantações de modelo de nuvem. Ao usar um ponto de integração de IPAM externo, os endereços IP são obtidos e gerenciados pelo provedor de IPAM designado, e não a partir do vRealize Automation.

Você pode criar um ponto de integração de IPAM específico de provedor para gerenciar endereços IP e configurações de DNS de implantações de modelos de nuvem e VMs no vRealize Automation.

Para obter informações sobre como configurar os pré-requisitos e um exemplo de como criar um ponto de integração de IPAM externo específico do provedor no contexto de um fluxo de trabalho de amostra, consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#). Observe que esse fluxo de trabalho é para uma integração de IPAM Infoblox, mas pode ser usado como referência para qualquer fornecedor de IPAM externo.

Para obter informações sobre como criar os ativos necessários para permitir que fornecedores e parceiros de IPAM externos integrem suas soluções de IPAM ao vRealize Automation, consulte [Como usar o SDK de IPAM para criar um pacote de integração de IPAM externo específico do provedor para o vRealize Automation](#).

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o [Infoblox](#) ou o [Bluecat](#), e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM.
- Verifique se você tem acesso a um pacote de integração implantado para o provedor de IPAM, como o Infoblox ou o BlueCat. O pacote implantado é obtido inicialmente como um download de .zip do provedor de IPAM ou do [VMware Marketplace](#), em seguida, implantado no vRealize Automation.
- Verifique se você tem acesso a um ambiente de execução configurado para o provedor de IPAM.
- Se você estiver usando um ambiente de execução de extensibilidade baseada em ações (ABX) incorporado localmente, verifique se você tem um servidor proxy HTTP na rede vRealize Automation que é capaz de passar o tráfego de saída para sites externos, como gcr.io e storage.googleapis.com. Para obter detalhes, consulte [Extrair imagens do Docker atrás do proxy no vRealize Automation 8.x \(75180\)](#).
- Verifique se você tem as credenciais de usuário necessárias para acessar e usar o produto de fornecedor IPAM. Consulte a documentação do produto do fornecedor de integração para obter informações sobre as permissões de usuário necessárias.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Clique em **IPAM**.
- 3 No menu suspenso **Provedor**, selecione um pacote de provedor de IPAM configurado na lista.
Se a lista estiver vazia, clique em **Importar Pacote do Provedor**, navegue até um arquivo .zip de pacote de provedor existente e selecione-o. Se você não tiver o arquivo .zip, poderá obtê-lo no [VMware Marketplace](#).
- 4 Insira suas credenciais de nome de usuário e senha de administrador da sua conta com o provedor de IPAM externo, juntamente com todos os outros campos obrigatórios (se houver), como o nome de host do seu provedor.
- 5 Na lista suspensa **Ambiente em Execução**, selecione um ambiente de execução existente, como o ponto de integração local de extensibilidade com base em ações.
O ambiente de execução oferece suporte à comunicação entre o vRealize Automation e o provedor de IPAM.

A estrutura de IPAM só é compatível com um ambiente de execução incorporado de extensibilidade com base em ações (ABX) no local.

Observação Se você usar uma conta de nuvem do Amazon Web Services ou Microsoft Azure como o ambiente de execução da integração, certifique-se de que o dispositivo do provedor de IPAM esteja acessível na Internet, não esteja atrás de um NAT ou firewall e tenha um nome DNS que possa ser resolvido publicamente. Se o provedor de IPAM não estiver acessível, o Amazon Web Services Lambda ou o Microsoft Azure Functions não conseguirão se conectar a ele, e a integração falhará.

6 Clique em **Validar**.

7 Quando solicitado a confiar no certificado autoassinado do provedor de IPAM externo, clique em **Aceitar**.

Depois que você aceitar o certificado autoassinado, a ação de validação poderá continuar até ser concluída.

8 Insira um nome para esse ponto de integração de IPAM e clique em **Adicionar** para salvar o novo ponto de integração de IPAM.

Uma ação de coleta de dados é iniciada. As redes e os endereços IP são coletados por dados do provedor de IPAM externo.

Como fazer upgrade para um pacote de integração de IPAM externo mais recente no vRealize Automation

Você pode atualizar um ponto de integração de IPAM externo existente para originar uma versão mais recente do pacote de integração de IPAM específico do fornecedor.

Um provedor de IPAM externo ou a VMware pode fazer upgrade de um pacote de integração de IPAM de origem para um determinado fornecedor. Por exemplo, o pacote de integração de IPAM externo para o Infoblox foi atualizado várias vezes. Para preservar as configurações de infraestrutura de vRealize Automation existentes que usam um ponto de integração de IPAM nomeado, é possível editar um ponto de integração de IPAM para originar o pacote de integração de IPAM atualizado, em vez de criar um novo ponto de integração de IPAM.

Pré-requisitos

Esse procedimento pressupõe que você já tenha criado um ponto de integração de IPAM externo e queira fazer upgrade desse ponto de integração para usar uma versão mais recente do pacote de integração de IPAM do fornecedor.

Para obter informações sobre como criar um ponto de integração de IPAM externo, consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).

- Verifique se você tem uma conta com o provedor de IPAM externo e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM.
- Verifique se você tem acesso a um pacote de integração implantado para o seu provedor de IPAM. O pacote implantado é obtido inicialmente como um download de arquivo .zip do site do provedor de IPAM ou no [VMware Marketplace](#) e, em seguida, implantado no vRealize Automation.

Para obter informações sobre como baixar e implantar o arquivo .zip do pacote do provedor e torná-lo disponível como um valor de **Provedor** na página Integração com o IPAM, consulte [Baixar e implantar um pacote de provedor de IPAM externo para uso no vRealize Automation](#).

- Verifique se você tem acesso a um ambiente de execução configurado para o provedor de IPAM. O ambiente de execução é em geral um ponto de integração incorporado no local de extensibilidade com base em ações (ABX).

Para obter informações sobre as características do ambiente de execução, consulte [Criar um ambiente em execução para um ponto de integração de IPAM no vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações IPAM** e abra o ponto de integração de IPAM existente.
- 2 Clique **Gerenciar Provedores**.
- 3 Navegue até o pacote de integração de IPAM atualizado e importe-o.
- 4 Clique em **Validar** e clique em **Salvar**.

Configurar a integração do My VMware no Cloud Assembly

Você pode integrar o My VMware ao Cloud Assembly para permitir ações e recursos relacionados à VMware e associados aos componentes que podem ser baixados e exigem uma conta.

É possível criar apenas uma integração do My VMware para cada organização.

Pré-requisitos

Você deve ter uma conta de usuário com as permissões apropriadas para o MyVMware.

- Para obter informações sobre como convidar um usuário para uma conta MyVMware, consulte o [KB 2070555](#).
- Para obter informações sobre como atribuir permissões de usuário em uma conta My VMware, consulte o [KB 2006977](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione My VMware.
- 3 Digite as informações necessárias na página de configuração do My VMware.

- 4 Se você precisar de tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 5 Clique em **Adicionar**.

Resultados

O My VMware está disponível para uso.

Próximo passo

Acesse os componentes do My VMware conforme necessário.

Configurar uma integração do vRealize Orchestrator no Cloud Assembly

É possível configurar uma ou mais integrações do vRealize Orchestrator para poder usar fluxos de trabalho como parte dos modelos de extensibilidade e de nuvem.

O vRealize Automation inclui uma instância pré-configurada do vRealize Orchestrator incorporado. Você pode acessar o cliente do vRealize Orchestrator incorporado do Console do vRealize Automation Cloud Services.

Observação É possível acessar o Centro de Controle do vRealize Orchestrator incorporado navegando até https://seu_vRA_FQDN/vco-controlcenter e fazendo login como **root**.

Também é possível integrar uma instância externa do vRealize Orchestrator para uso em suas assinaturas de extensibilidade do vRealize Automation e operações do XaaS (Qualquer coisa como serviço) usadas para modelos de nuvem.

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Faça upgrade ou migre para o vRealize Orchestrator 8.3. Consulte *Fazendo upgrade e migrando o VMware vRealize Orchestrator*.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações**.
- 2 Clique em **Adicionar integração**.
- 3 Selecione **vRealize Orchestrator**.
- 4 Insira um nome para a integração do vRealize Orchestrator.
- 5 (Opcional) Insira uma descrição para a integração do vRealize Orchestrator.

- 6 Em **URL do vRealize Orchestrator**, insira o nome de domínio totalmente qualificado (FQDN) da sua instância externa do vRealize Orchestrator.
Por exemplo, `https://my_vRO_FQDN.com:443`.
- 7 Para validar a integração, clique em **Validar**.
- 8 (Opcional) Se você for solicitado a fazer isso, revise as informações do certificado e clique em **Aceitar**.
- 9 (Opcional) Adicione tags de recurso. Para obter mais informações sobre tags de capacidade, consulte [Como usar tags de capacidade no Cloud Assembly](#).

Observação Tags de capacidade podem ser usadas para gerenciar várias integrações do vRealize Orchestrator. Consulte [Gerenciamento de várias integrações do vRealize Orchestrator com restrições de projeto](#).

- 10 Clique em **Adicionar**.
A integração do vRealize Orchestrator é salva.
- 11 Para verificar se a integração está configurada e se os fluxos de trabalho foram adicionados, selecione **Extensibilidade > Biblioteca > Fluxos de Trabalho**.

Próximo passo

Acesse o cliente do vRealize Orchestrator externo incorporado:

- 1 Navegue até o Console do Cloud Services do vRealize Automation.
- 2 Selecione **Orchestrator**.
- 3 Selecione a guia que corresponde à instância do vRealize Orchestrator integrada.

Observação Os usuários do Cloud Assembly sem credenciais de administrador de nuvem não podem ver a guia da instância integrada do vRealize Orchestrator.

Desativar ou ativar integrações do vRealize Orchestrator

Você pode desativar ou ativar manualmente sua integração com o vRealize Orchestrator para poder fazer uma manutenção enquanto a integração ainda está em execução.

Você pode desativar sua integração com o vRealize Orchestrator para fazer essa manutenção. Enquanto estiver desativada, sua integração com o vRealize Orchestrator ainda estará em um estado **EM EXECUÇÃO** e, portanto, você pode continuar a realizar tarefas como monitoramento de recursos e coleta de dados.

Observação Além da desativação manual, o Serviço de gateway do vRealize Orchestrator executa verificações periódicas de status de integridade para confirmar se as suas integrações com o vRealize Orchestrator estão ativas ou não. Todas as integrações com o vRealize Orchestrator inativas são desativadas automaticamente e definidas para o estado **DESCONECTADO**. Você não poderá realizar tarefas como coleta de dados ou monitoramento de recursos em integrações desconectadas.

Depois de desativar uma integração com o vRealize Orchestrator ou fazer com que essa integração seja desconectada pelo verificador de status de integridade, os fluxos de trabalho apenas serão executados nas integrações restantes que estiverem ativadas. Se o seu ambiente incluir várias integrações com o vRealize Orchestrator ativadas que não são gerenciadas por meio de restrições de projeto ou tags de capacidade, uma integração com o vRealize Orchestrator aleatória será selecionada para executar seu fluxo de trabalho.

Observação Como a integração com o vRealize Orchestrator é selecionada aleatoriamente, você deve garantir que as informações necessárias para executar uma determinada operação estejam disponíveis em todas as integrações. Para entidades de conteúdo, como fluxos de trabalho, isso significa que elas devem ser sincronizadas em todas as integrações. Para objetos de inventário, não há garantia de que eles terão o mesmo identificador de objeto em todas as integrações, portanto, a tentativa de executar um fluxo de trabalho que inclui esse objeto de inventário como um parâmetro de entrada pode falhar.

Para obter informações sobre como gerenciar várias integrações com o vRealize Orchestrator usando restrições de projeto e tags de capacidade, consulte [Gerenciamento de várias integrações do vRealize Orchestrator com restrições de projeto](#) e [Gerenciamento de várias integrações do vRealize Orchestrator com tags de capacidade da conta de nuvem](#).

Pré-requisitos

Configure uma ou mais integrações do vRealize Orchestrator no Cloud Assembly. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).

Procedimentos

- 1 Desative sua integração com o vRealize Orchestrator.
 - a Navegue até **Infraestrutura > Conexões > Integrações**.
 - b Selecione a integração com o vRealize Orchestrator que você deseja desativar.
 - c Em **Credenciais do vRealize Orchestrator Server**, desative a opção **Ativar endpoint**.
 - d Clique em **Validar**.
 - e Após a validação bem-sucedida, clique em **Salvar**.
- 2 Realize as tarefas de manutenção necessárias na integração com o vRealize Orchestrator desativada.
- 3 Ative sua integração com o vRealize Orchestrator.
 - a Navegue até **Infraestrutura > Conexões > Integrações**.
 - b Selecione a integração com o vRealize Orchestrator desativada anteriormente.
 - c Em **Credenciais do vRealize Orchestrator Server**, ative a opção **Ativar endpoint**.
 - d Clique em **Validar**.
 - e Após a validação bem-sucedida, clique em **Salvar**.

Gerenciamento de várias integrações do vRealize Orchestrator com restrições de projeto

Você pode usar restrições de projeto para gerenciar quais integrações do vRealize Orchestrator são usadas em assinaturas de fluxo de trabalho.

O Cloud Assembly é compatível com a integração de vários servidores vRealize Orchestrator que podem ser usados em assinaturas de fluxo de trabalho. Você pode gerenciar quais integrações do vRealize Orchestrator são usadas em modelos de nuvem provisionados pelo seu projeto com restrições de projeto rígidas ou flexíveis. Para obter mais informações sobre restrições de projeto, consulte [Usando tags de projeto e propriedades personalizadas do Cloud Assembly](#).

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Configure duas ou mais integrações do vRealize Orchestrator no Cloud Assembly. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).
- Adicione tags de capacidade às suas integrações do vRealize Orchestrator. Consulte [Como usar tags de capacidade no Cloud Assembly](#).

Procedimentos

- 1 Navegue para **Infraestrutura > Administração > Projetos** e selecione o projeto.
- 2 Selecione a guia **Provisionamento**.
- 3 Insira as tags de capacidade das suas integrações do vRealize Orchestrator na caixa de texto **Restrições de extensibilidade** e defina-as como restrições de projeto fixas ou flexíveis.
- 4 Clique em **Salvar**.

Resultados

Quando você implanta um modelo de nuvem, o Cloud Assembly usa as restrições do projeto para gerenciar quais integrações do vRealize Orchestrator são usadas em inscrições de fluxo de trabalho.

Próximo passo

Como alternativa, você pode usar tags de capacidade para gerenciar várias integrações do vRealize Orchestrator em um nível de conta de nuvem. Para obter mais informações, consulte [Gerenciamento de várias integrações do vRealize Orchestrator com tags de capacidade da conta de nuvem](#).

Gerenciamento de várias integrações do vRealize Orchestrator com tags de capacidade da conta de nuvem

Você pode usar tags de capacidade para gerenciar quais integrações do vRealize Orchestrator são usadas em assinaturas de fluxos de trabalho.

O Cloud Assembly é compatível com a integração de vários servidores vRealize Orchestrator que podem ser usados em assinaturas de fluxo de trabalho. Você pode gerenciar quais integrações do vRealize Orchestrator são usadas em assinaturas de fluxo de trabalho adicionando tags de capacidade à sua conta de nuvem.

Pré-requisitos

- Verifique se tem credenciais de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Configure duas ou mais integrações do vRealize Orchestrator no Cloud Assembly. Para obter mais informações, consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).
- Adicione tags de capacidade às suas integrações do vRealize Orchestrator. Consulte [Como usar tags de capacidade no Cloud Assembly](#).

Procedimentos

- 1 Navegue até **Infraestrutura > Conexões > Contas de Nuvem**.
- 2 Selecione sua conta de nuvem.
- 3 Insira as tags de capacidade das integrações do vRealize Orchestrator que você deseja usar.

As tags de capacidade são automaticamente convertidas em restrições flexíveis. Para usar as restrições fixas no gerenciamento das suas integrações, você deve usar as restrições do projeto. Para obter mais informações, consulte [Gerenciamento de várias integrações do vRealize Orchestrator com restrições de projeto](#).
- 4 Clique em **Salvar**.

Resultados

Quando você implanta um modelo de nuvem, o Cloud Assembly usa a marcação na conta de nuvem associada para gerenciar quais integrações do vRealize Orchestrator são usadas em inscrições de fluxo de trabalho.

Coleta de dados para integrações do vRealize Orchestrator

O vRealize Automation realiza a coleta periódica de dados para as suas integrações do vRealize Orchestrator.

Eventos de coleta de dados para integrações do vRealize Orchestrator são acionados a cada 10 minutos. A coleta de dados reúne dados sobre os fluxos de trabalho incluídos na biblioteca de cada integração do vRealize Orchestrator.

Importante Certifique-se de criar uma versão de um fluxo de trabalho quando terminar de editá-lo. Alterações em fluxos de trabalho sem versão não são capturadas pelo coletor de dados.

Você pode encontrar informações sobre a última coleta de dados realizada em uma integração do vRealize Orchestrator navegando até **Infraestrutura > Conexões > Integrações** e selecionando a integração específica. Também pode acionar um evento de coleta manual de dados clicando em **Iniciar Coleta de Dados**.

Para obter mais informações sobre a coleta de dados do vRealize Automation, consulte [Como a coleta de dados funciona no vRealize Automation](#).

Como trabalhar com o Kubernetes no Cloud Assembly

O Cloud Assembly oferece várias opções para configurar, gerenciar e implantar cargas de trabalho virtuais do Kubernetes.

Há duas opções para trabalhar com recursos do Tanzu Kubernetes no Cloud Assembly. Você pode criar uma configuração do vSphere with Tanzu Kubernetes, que requer apenas uma conta de nuvem do vCenter adequada e um plano de cluster para acessar os recursos nativos do vSphere with Tanzu Kubernetes. Com essa opção, você pode aproveitar uma conta de nuvem do vCenter para acessar namespaces de supervisor para implantar cargas de trabalho baseadas no vSphere Kubernetes. Você também pode integrar recursos externos do Kubernetes ao Cloud Assembly.

Como alternativa, você pode integrar o VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), o antigo PKS. Esse tipo de implementação do Kubernetes requer uma integração do PKS no Cloud Assembly. Ele não requer um plano de cluster do Cloud Assembly.

Por fim, você também pode criar uma integração do Red Hat OpenShift com o Cloud Assembly para configurar, gerenciar e implantar recursos do Kubernetes.

Trabalhando com clusters do vSphere with Tanzu Kubernetes

O vSphere 7.x conta com melhorias significativas que permitem que você trabalhe com o Kubernetes de forma nativa para gerenciar máquinas virtuais e contêineres em uma única interface. O Cloud Assembly permite que os usuários aproveitem os recursos do vSphere with Tanzu Kubernetes incorporados ao vSphere. Você pode acessar a funcionalidade do vSphere with Tanzu Kubernetes por meio de uma conta de nuvem do vCenter com uma implementação do vSphere que contém clusters de supervisor. Essa implementação permite que você gerencie máquinas virtuais convencionais e clusters Kubernetes no vCenter.

Para namespaces de supervisor Tanzu Kubernetes, os usuários devem ter acesso a um SSO do vSphere aplicável para que possam fazer login em um link fornecido para os detalhes do namespace de supervisor. Em seguida, eles podem baixar um Kubectl personalizado com autenticação do vSphere, para poderem usar seus namespaces de supervisor.

Para usar essa funcionalidade, você deve ter um vCenter com uma conta de nuvem do vSphere que tenha namespaces de supervisor configurados. Depois que um usuário fizer login, ele poderá começar a trabalhar com namespaces aplicáveis.

Trabalhando com integrações do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) ou Openshift

Para configurações do TKGI, de clusters externos ou do Openshift, o Cloud Assembly fornece acesso a uma Kubeconfig que permite aos usuários acessar clusters Kubernetes aplicáveis.

Depois de criar uma integração do TKGI ou do OpenShift, os clusters Kubernetes aplicáveis ficam disponíveis no Cloud Assembly, e você pode adicionar e criar componentes do Kubernetes para o Cloud Assembly para oferecer suporte ao gerenciamento de aplicativos de cluster e de contêiner. Esses aplicativos formam a base das implantações de autoatendimento disponíveis a partir do catálogo do Service Broker.

- [Configurar a integração com o VMware Tanzu Kubernetes Grid Integrated Edition no Cloud Assembly](#)

Você pode configurar uma conexão de recurso do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), o antigo PKS, no local e na nuvem para oferecer suporte a recursos de integração e gerenciamento do Kubernetes no Cloud Assembly.

- [Provisionar uma implantação do vSphere with Tanzu Kubernetes no vRealize Automation](#)

O vRealize Automation permite que você provisione uma implantação do vSphere with Tanzu Kubernetes pelo Cloud Assembly para aproveitar os recursos nativos do vSphere 7.x com o objetivo de implantar e gerenciar clusters Tanzu Kubernetes, fornecendo uma camada independente de infraestrutura para o provisionamento e o gerenciamento da infraestrutura virtual.

- [Configurar a integração com o Red Hat OpenShift no Cloud Assembly](#)

Você pode configurar uma conexão de recurso do Red Hat OpenShift no local e na nuvem para oferecer suporte a recursos de integração e gerenciamento do Kubernetes em nível empresarial no Cloud Assembly.

- [Configurar uma zona do Kubernetes no Cloud Assembly](#)

As zonas do Kubernetes permitem que os administradores de nuvem definam o posicionamento baseado em políticas de clusters e namespaces do Kubernetes e namespaces de supervisor usados em implantações do Cloud Assembly. Um administrador pode usar essa página para especificar quais clusters estão disponíveis para o provisionamento de namespaces do Kubernetes e quais propriedades são aceitáveis para clusters.

- [Criar um plano de cluster no vRealize Automation Cloud Assembly para uso com uma implantação do vSphere with Tanzu Kubernetes](#)

Você deve criar um plano de cluster para uso com implantações do vSphere with Tanzu Kubernetes no vRealize Automation. Um plano de cluster funciona como um modelo de configuração para o provisionamento de instâncias de cluster Tanzu Kubernetes em uma instância de conta de nuvem do vSphere específica.

- [Usar clusters e namespaces de supervisor do Tanzu no Cloud Assembly](#)

Os administradores podem disponibilizar namespaces de supervisor em uma integração do vSphere habilitada para Tanzu, para que eles possam adicionar esses namespaces a implantações do Kubernetes por meio de modelos de nuvem ou para solicitá-los no catálogo do Service Broker.

- [Trabalhando com clusters e namespaces do Kubernetes no Cloud Assembly](#)

Os administradores de nuvem podem adicionar, exibir e gerenciar a configuração de clusters e namespaces implantados do Kubernetes, tanto genéricos quanto baseados no Pacific, no Cloud Assembly.

- [Adicionando componentes Kubernetes a modelos de nuvem no Cloud Assembly](#)

Ao adicionar componentes do Kubernetes a um modelo de nuvem do Cloud Assembly, você pode optar por adicionar clusters ou permitir que os usuários criem namespaces em várias configurações. Normalmente, essa escolha depende dos seus requisitos de controle de acesso, de como você configurou seus componentes do Kubernetes e dos seus requisitos de implantação.

- [Usando a extensibilidade do Cloud Assembly com o Kubernetes](#)

O Cloud Assembly fornece um conjunto de tópicos de eventos que correspondem a ações típicas relacionadas à implantação do namespace e do cluster Kubernetes. Os usuários podem assinar esses tópicos conforme desejado, e eles serão executados no momento apropriado. Os usuários recebem uma notificação quando ocorre o evento relacionado ao tópico inscrito. Você também pode configurar fluxos de trabalho do vRO para serem executados com base em notificações de eventos.

Configurar a integração com o VMware Tanzu Kubernetes Grid Integrated Edition no Cloud Assembly

Você pode configurar uma conexão de recurso do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), o antigo PKS, no local e na nuvem para oferecer suporte a recursos de integração e gerenciamento do Kubernetes no Cloud Assembly.

As integrações com o TKGI permitem gerenciar instâncias do TKGI no local e na nuvem e os clusters do Kubernetes provisionados no TKGI e em clusters externos. Você deve criar um perfil do Kubernetes e associá-lo a um projeto para oferecer suporte ao posicionamento de recursos com base em políticas.

Pré-requisitos

- Você deve ter um servidor TKGI devidamente configurado com autenticação UAA.
- Verifique se tem credenciais de administrador de nuvem. Para obter mais informações, consulte [Quais são as funções de usuário do vRealize Automation](#).

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione VMware Tanzu Kubernetes Grid Integrated Edition.

- 3 Insira o endereço IP ou o FQDN, bem como o endereço TKGI da conta de nuvem do TKGI que você está criando.
 - O endereço IP é o FQDN ou o endereço IP do servidor de autenticação de usuários do TKGI.
 - O endereço TKGI é o FQDN ou o endereço IP do servidor TKGI principal.
- 4 Selecione se esse servidor TKGI é local ou se está localizado na nuvem pública ou em uma nuvem privada.
- 5 Insira um **Nome de Usuário** e uma **Senha** apropriados para o servidor TKGI e outras informações relacionadas.
- 6 Se você usar tags para oferecer suporte a uma estratégia de marcação, adicione tags de recurso. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 7 Clique em **Adicionar**.

Resultados

É possível criar zonas do Kubernetes e atribuí-las a um projeto ou descobrir clusters do Kubernetes externos e atribuir esses clusters a projetos. Além disso, você pode adicionar ou criar namespaces do Kubernetes que facilitam o gerenciamento de clusters entre grupos grandes e organizações.

Próximo passo

Crie ou selecione as zonas do Kubernetes apropriadas e, em seguida, selecione um ou mais clusters ou namespaces e atribua-os a um projeto. Depois disso, você poderá criar e publicar modelos de nuvem para permitir que os usuários gerem implantações de autoatendimento que usam o Kubernetes.

Provisionar uma implantação do vSphere with Tanzu Kubernetes no vRealize Automation

O vRealize Automation permite que você provisione uma implantação do vSphere with Tanzu Kubernetes pelo Cloud Assembly para aproveitar os recursos nativos do vSphere 7.x com o objetivo de implantar e gerenciar clusters Tanzu Kubernetes, fornecendo uma camada independente de infraestrutura para o provisionamento e o gerenciamento da infraestrutura virtual.

A funcionalidade do vSphere with Tanzu Kubernetes aproveita o recurso Kubernetes nativo do vSphere 7.x e não requer uma integração do vRealize Automation PKS para operar.

Pré-requisitos

- Para provisionar uma implantação do vSphere with Tanzu Kubernetes com o Cloud Assembly, você deve ter acesso ao vSphere 7.x. No vRealize Automation, o vSphere está disponível como parte de uma conta de nuvem do vCenter do Cloud Assembly. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).

- O Tanzu deve estar habilitado na conta de nuvem do vSphere e deve conter namespaces de supervisor apropriados.
- Você deve ter um plano de cluster apropriado para usar com a integração. Consulte [Criar um plano de cluster no vRealize Automation Cloud Assembly para uso com uma implantação do vSphere with Tanzu Kubernetes](#).

Procedimentos

- 1 Se uma conta de nuvem do vCenter adequada ainda não existir no Cloud Assembly, crie uma. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- 2 Selecione **Infraestrutura > Configurar > Zona do Kubernetes** para criar ou selecionar uma zona do Kubernetes no vRealize Automation Cloud Assembly.

Você poderá usar uma zona do Kubernetes existente se tiver uma apropriada já configurada, mas um administrador deverá adicionar um ou mais namespaces de supervisor à zona. Esses namespaces servem como recursos de processamento nos quais os clusters Tanzu Kubernetes provisionados são criados dentro da zona. Consulte [Configurar uma zona do Kubernetes no Cloud Assembly](#) para obter mais informações sobre zonas Kubernetes.
- 3 Navegue até a guia Provisionamento do Kubernetes na página **Infraestrutura > Administração > Projetos** no Cloud Assembly e associe a Zona do Kubernetes ao projeto apropriado.
- 4 Crie ou selecione um plano de cluster para uma conta de nuvem do vSphere 7.x apropriada. Consulte [Criar um plano de cluster no vRealize Automation Cloud Assembly para uso com uma implantação do vSphere with Tanzu Kubernetes](#) para obter mais informações.
- 5 Selecione **Projetar > Modelos de Nuvem** e crie um modelo de nuvem para um projeto que tenha acesso a uma zona apropriada do Kubernetes. Em seguida, arraste um componente de cluster K8s no esquema de modelo de nuvem e especifique seu nome e plano de cluster.

Você também tem a opção de especificar o número de nós de trabalho.
- 6 Execute o modelo de nuvem e, quando ele estiver concluído, localize o endereço do cluster Tanzu provisionado na implantação, nas propriedades de recursos da página Implantações do Cloud Assembly.
- 7 Encontre e explore o cluster Tanzu na página **Infraestrutura > Configurar > Kubernetes** do Cloud Assembly.

Resultados

O cluster Tanzu Kubernetes é provisionado conforme especificado no modelo de nuvem.

Próximo passo

Depois de implantar o cluster Tanzu, você tem várias opções para trabalhar com ele.

- Navegue até a página **Recursos > Implantações** no Cloud Assembly, localize e baixe o arquivo Kubeconfig relacionado para acessar o cluster Tanzu provisionado. Você pode usar o arquivo Kubeconfig para gerenciar o cluster Tanzu Kubernetes implantado como qualquer outro cluster Kubernetes em conformidade.
- Você pode encontrar e explorar o cluster Tanzu na página **Infraestrutura > Recursos > Kubernetes** do Cloud Assembly.
- Para criar um novo namespace, navegue até a guia Namespaces na página **Infraestrutura > Recursos > Kubernetes** do Cloud Assembly e clique em **Novo Namespace** para criar um namespace no cluster Tanzu aplicável. Você pode conferir se o namespace foi criado verificando se ele está listado na guia Namespaces da página Kubernetes.

Configurar a integração com o Red Hat OpenShift no Cloud Assembly

Você pode configurar uma conexão de recurso do Red Hat OpenShift no local e na nuvem para oferecer suporte a recursos de integração e gerenciamento do Kubernetes em nível empresarial no Cloud Assembly.

O Cloud Assembly oferece suporte à integração com o OpenShift versões 3.x.

Pré-requisitos

- É necessário ter uma implementação do Red Hat OpenShift devidamente configurada.
- Verifique se tem credenciais de administrador de nuvem. Para obter mais informações, consulte [Quais são as funções de usuário do vRealize Automation](#).
- A VMware fornece recursos que você pode usar para criar um cluster do OpenShift com um modelo de nuvem na seguinte localização: <https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>. É possível usar clusters criados com esses recursos como clusters globais nas zonas do Kubernetes para criar namespaces de autoatendimento.

Procedimentos

1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.

2 Selecione Red Hat OpenShift.

3 Insira o **Endereço** e a **Localização** para o servidor OpenShift.

4 Selecione o **Tipo de Credencial** apropriado e insira as credenciais corretas.

A integração com o OpenShift oferece suporte à autenticação de nome de usuário/senha OAuth, chave pública ou token de portador.

5 Insira um **Nome** e uma **Descrição** apropriados para a integração com o OpenShift.

- 6 Se você usar tags para oferecer suporte a uma estratégia de marcação, insira as tags de recurso apropriadas. Consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#) e [Criação de uma estratégia de marcação](#).
- 7 Clique em **Adicionar**.

Resultados

Quando uma integração é criada, novos clusters do Kubernetes aparecem na seção relevante da página Kubernetes. Você pode criar zonas do Kubernetes e atribuí-las a um projeto. Além disso, você pode configurar namespaces do Kubernetes que facilitam o gerenciamento de clusters entre grupos grandes e organizações.

Próximo passo

Crie ou selecione as zonas do Kubernetes apropriadas e, em seguida, selecione um ou mais clusters ou namespaces e atribua-os a um projeto. Depois disso, você poderá criar e publicar modelos de nuvem para permitir que os usuários gerem implantações de autoatendimento que usam o Kubernetes.

Configurar uma zona do Kubernetes no Cloud Assembly

As zonas do Kubernetes permitem que os administradores de nuvem definam o posicionamento baseado em políticas de clusters e namespaces do Kubernetes e namespaces de supervisor usados em implantações do Cloud Assembly. Um administrador pode usar essa página para especificar quais clusters estão disponíveis para o provisionamento de namespaces do Kubernetes e quais propriedades são aceitáveis para clusters.

Os administradores de nuvem podem associar zonas do Kubernetes a contas de nuvem do TKGI configuradas para o Cloud Assembly ou a clusters do Kubernetes externos que não estão associados a um projeto.

Ao criar uma zona do Kubernetes, você pode atribuir a ela vários recursos específicos do provedor, e esses recursos determinarão quais propriedades podem ser definidas para os clusters recém-provisionados em termos do número de trabalhadores, mestres, CPU disponível, memória e outras definições de configuração. Para provedores de TKGI, eles correspondem a planos de TKGI. Um administrador também pode atribuir vários clusters a uma zona do Kubernetes, que serão usados para o posicionamento de namespaces do Kubernetes recém-provisionados. O administrador só pode atribuir clusters que não estejam integrados, ou que não sejam gerenciados pelo CMX, e que sejam provisionados por meio do provedor de cluster selecionado. O administrador pode atribuir várias zonas do Kubernetes a um único projeto, tornando-as assim disponíveis para operações de posicionamento que acontecem nesse projeto.

Um administrador de nuvem pode atribuir prioridades em vários níveis.

- Prioridade de zonas do Kubernetes dentro de um projeto.
- Prioridade de recursos dentro de uma zona do Kubernetes.
- Prioridade de clusters dentro de uma zona do Kubernetes.

O administrador da nuvem também pode atribuir tags em vários níveis:

- Tags de capacidade por zona do Kubernetes.
- Tags por atribuição de recurso.
- Tags por atribuição de cluster.

Você pode criar zonas do Kubernetes com namespaces de supervisor no vSphere da mesma forma que trabalha com namespaces do Kubernetes genéricos. Para adicionar um namespace de supervisor a uma zona do Kubernetes, você deve associar a zona a um endpoint do vSphere 7 que contém os recursos de namespace do Pacífico desejados.

O Service Broker contém uma versão da página Zona do Kubernetes para permitir que os administradores do Service Broker acessem zonas do Kubernetes existentes para criar políticas de posicionamento para namespaces e clusters do Kubernetes provisionados a partir do catálogo.

Pré-requisitos

Configure a integração com uma implantação adequada do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). Consulte [Configurar a integração com o VMware Tanzu Kubernetes Grid Integrated Edition no Cloud Assembly](#)

Procedimentos

- 1 Selecione **Infraestrutura > Configurar > Zona do Kubernetes** e clique em **Nova Zona do Kubernetes**.
- 2 Insira o nome da **Conta** da integração com o TKGI à qual você deseja que essa zona seja aplicada.

Isso define a conta de nuvem ou o endpoint que está associado à zona. Você pode atribuir apenas um endpoint a cada zona. Se você estiver trabalhando com um namespace de Supervisor no vSphere, só poderá selecionar instâncias do vSphere aqui que contenham namespaces de supervisor.
- 3 Adicione um **Nome** e uma **Descrição** para a Zona do Kubernetes.
- 4 Adicione tags de capacidade, se apropriado. Consulte [Como usar tags de capacidade no Cloud Assembly](#) para informações adicionais.
- 5 Clique em **Salvar**.
- 6 Clique na guia Sob demanda e adicione planos do TKGI conforme apropriado para a zona usar no provisionamento de clusters.

Você pode selecionar um ou mais planos e atribuir prioridades a eles. Números mais baixos representam maior prioridade. Atribuições de prioridade são secundárias à seleção baseada em tags.

- 7 Clique na guia Cluster e, em seguida, clique no botão **Adicionar processamento** para adicionar clusters de kubernetes ou de supervisor à zona. Se estiver trabalhando com um cluster externo, ele será integrado automaticamente ao Cloud Assembly quando você o selecionar.

É possível adicionar namespaces do Kubernetes ao cluster na página Clusters do Kubernetes do Cloud Assembly.

Resultados

Zonas do Kubernetes são configuradas para uso com implantações do Cloud Assembly.

Próximo passo

Atribua a zona do Kubernetes a um projeto.

- 1 Selecione **Infraestrutura > Administração > Projetos** e, em seguida, selecione o projeto que você deseja associar à zona do kubernetes.
- 2 Clique na guia Provisionamento do Kubernetes, na página Projeto.
- 3 Clique em **Adicionar Zona do Kubernetes** e adicione a zona que você acabou de criar. Você pode criar várias zonas, se aplicável, e também definir a prioridade nas zonas.
- 4 Clique em **Salvar**.

A guia Provisionamento do Kubernetes na página Projeto do Cloud Assembly permite que você defina limites para o tipo e o número de namespaces que os usuários podem provisionar para uma zona do kubernetes. Você também pode selecionar o tipo de namespaces que podem ser provisionados para uma zona: namespaces regulares ou namespaces de supervisor. A tabela Zonas do Kubernetes na guia Provisionamento do Kubernetes contém colunas que mostram as configurações de limite atuais. Para definir limites, clique na zona aplicável na tabela para abrir uma caixa de diálogo que permite escolher limites de namespace e namespace de supervisor.

Clique na coluna Suporte na tabela Zonas do Kubernetes para selecionar que tipo de namespace pode ser provisionado para a zona.

Depois de atribuir uma zona do Kubernetes a um projeto, você poderá usar a página Modelos de Nuvem na guia Design do Cloud Assembly para provisionar uma implantação com base na zona do Kubernetes e na configuração do projeto. Essa página Modelos de nuvem inclui opções para adicionar um Cluster K8S, um Namespace K8S e um Namespace de Supervisor. Selecione a opção apropriada para o recurso de kubernetes com o qual você está trabalhando.

Criar um plano de cluster no vRealize Automation Cloud Assembly para uso com uma implantação do vSphere with Tanzu Kubernetes

Você deve criar um plano de cluster para uso com implantações do vSphere with Tanzu Kubernetes no vRealize Automation. Um plano de cluster funciona como um modelo de configuração para o provisionamento de instâncias de cluster Tanzu Kubernetes em uma instância de conta de nuvem do vSphere específica.

Um plano de cluster define um mapeamento de configuração, semelhante a um mapeamento de tipo, para um conjunto de instâncias da conta de nuvem do vSphere. Geralmente, o plano de cluster codifica um conjunto significativo de propriedades de configuração, como classes de máquina virtual, classes de armazenamento etc., que são usadas para provisionar clusters Tanzu Kubernetes em uma conta de nuvem de servidor vSphere específica.

Observe que um único plano de cluster pode ter um mapeamento de propriedade de configuração específico em uma conta de nuvem do vSphere e outro mapeamento de configuração em outra instância do vSphere. Por exemplo, se você tiver duas contas de nuvem do vSphere qualificadas, uma com muitos recursos e outra com recursos limitados, o plano de cluster `large` poderá especificar `guaranteed-xlarge` para o servidor vSphere de alto perfil e `best-effort-medium` para a instância limitada do vSphere. Em geral, a especificação `large` mapeia um conjunto de propriedades de configuração diferente para cada instância do servidor vSphere qualificado.

Depois que um plano de cluster é criado para uma ou mais instâncias do vSphere, todos os namespaces de supervisor elegíveis, que um administrador atribui para hospedar um cluster Tanzu Kubernetes usando uma atribuição de zona Kubernetes, devem ser alinhados em relação à configuração definida na especificação do plano de cluster. Por exemplo, a política de armazenamento especificada no plano de cluster deve ser adicionada como uma classe de armazenamento a todos os namespaces de supervisor do vSphere dedicados para o provisionamento de clusters Tanzu.

Pré-requisitos

- Para criar uma implantação do vSphere with Tanzu Kubernetes no Cloud Assembly, você deve ter acesso ao vSphere 7.x, que está disponível como parte de uma conta de nuvem do vCenter. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- O Tanzu deve estar ativado na conta de nuvem do vSphere com um ou mais namespaces de supervisor.
- Todos os clusters de supervisor na conta de nuvem do vSphere registrada que são elegíveis para provisionamento de Clusters Tanzu devem ser adicionados como entidades gerenciadas na página **Infraestrutura > Kubernetes > Clusters de Supervisor** do Cloud Assembly usando a opção **Adicionar Cluster de Supervisor**.

Procedimentos

- 1 Selecione **Infraestrutura > Configurar > Plano de Cluster** e clique em **Novo Plano de Cluster**.
- 2 Insira uma **Conta**, um **Nome** e uma **Descrição** para o plano de cluster. A conta define a conta de nuvem à qual esse plano de cluster se aplica.
- 3 Insira os detalhes das informações do cluster, incluindo as **Versões Kubernetes** e o **Plano de controle**. Essas informações incluem alocações para nós, classe de máquina e classe de armazenamento.
 - Insira a versão do Kubernetes que é aplicável a este plano de cluster. Esta é a versão Kubernetes dos clusters Tanzu Kubernetes provisionados: por exemplo, 1.19 ou 1.20.

- A contagem de planos de controle define a especificação para os nós do servidor de API do Kubernetes.
 - Uma classe de máquina virtual é uma solicitação de reservas na máquina virtual para poder de processamento. Existem várias classes de máquina predefinidas, que representam diferentes níveis de poder de processamento. Consulte [Classes de máquina virtual para clusters Tanzu Kubernetes](#) para obter mais informações.
 - Trabalhadores especificam os nós de trabalhador do Tanzu Kubernetes a serem implantados com esse plano.
- 4 Digite e selecione Configurações Adicionais para o plano de cluster.
- Digite a **Classe de armazenamento PVC padrão** a ser usada com esse cluster.
 - Use os botões de opção para indicar o comportamento em relação ao uso de classes de armazenamento e configurações de rede.
- 5 Clique em **Criar**.

Resultados

O plano de cluster é criado e fica disponível para uso em modelos de nuvem do Cloud Assembly.

Próximo passo

Depois de criar um plano de cluster, você pode usá-lo para criar uma implantação do vSphere with Tanzu Kubernetes no Cloud Assembly. Consulte [Provisionar uma implantação do vSphere with Tanzu Kubernetes no vRealize Automation](#).

Usar clusters e namespaces de supervisor do Tanzu no Cloud Assembly

Os administradores podem disponibilizar namespaces de supervisor em uma integração do vSphere habilitada para Tanzu, para que eles possam adicionar esses namespaces a implantações do Kubernetes por meio de modelos de nuvem ou para solicitá-los no catálogo do Service Broker.

Esta tarefa descreve como adicionar clusters de supervisor do Tanzu com o Cloud Assembly para uso em implantações e como criar ou adicionar namespaces que definem quais projetos e usuários do Cloud Assembly podem acessar recursos específicos do Kubernetes. Essa funcionalidade depende de uma conta de nuvem do vSphere adequada, e não de uma integração, como o VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) ou o Openshift. Os clusters de supervisor são clusters kubernetes personalizados associados ao vSphere. Eles expõem APIs do Kubernetes aos usuários finais e usam o ESXI como plataforma para nós de trabalho em vez do Linux. Os namespaces de supervisor facilitam o controle do acesso aos recursos do Kubernetes, pois geralmente é mais fácil aplicar políticas a namespaces do que a máquinas virtuais individuais. Você pode criar vários namespaces para cada cluster de supervisor.

As implantações habilitadas pelo Tanzu também podem usar clusters guest gerados pelo vSphere. Um cluster guest é um cluster Kubernetes executado dentro de máquinas virtuais no cluster de supervisor. Um cluster guest é totalmente compatível com o Kubernetes e, portanto, é possível ter a garantia de que funcionará com todos os aplicativos do Kubernetes. Os clusters guest no vSphere usam o projeto de API de Cluster de código aberto para gerenciar o ciclo de vida dos clusters Kubernetes, que, por sua vez, usam o operador da VM para gerenciar as máquinas virtuais que compõem um guest.

Quando usadas com instâncias do vSphere ativadas para o Tanzu, as zonas do Kubernetes definem quais clusters de supervisor estão disponíveis para o provisionamento de um namespace de supervisor. Namespaces de supervisor são específicos para instâncias do vSphere ativadas para o Tanzu. Você não pode provisionar um recurso do Kubernetes genérico para uma instância do vSphere ativada para o Tanzu.

Os usuários do Cloud Assembly designados como espectadores de projeto têm acesso somente exibição a namespaces, enquanto membros de projetos podem editá-los.

Você poderá configurar os clusters de supervisor associados namespaces, se desejar.

Pré-requisitos

- Para usar clusters e namespaces de supervisor com o Cloud Assembly, você deve ter um endpoint do vSphere 7.x configurado. No vRealize Automation, o vSphere é instalado como parte de uma conta do vCenter Cloud. Consulte [Criar uma conta de nuvem do vCenter no vRealize Automation](#).
- O Tanzu deve estar habilitado na conta de nuvem do vSphere e deve conter namespaces de supervisor apropriados.
- O vCenter e a sua implantação do vRealize Automation devem usar o mesmo Active Directory para que os usuários sejam sincronizados. Embora o provisionamento ainda funcione se esse não for o caso, os usuários do vRealize Automation não terão acesso automático ao namespace.

Procedimentos

- 1 Selecione **Infraestrutura > Configurar > Zona de kubernetes** no Cloud Assembly.
Essa página mostra os clusters gerenciados que estão disponíveis para uso e permite que você adicione outros clusters. Você pode clicar em qualquer um dos clusters para exibir os respectivos detalhes.
- 2 Selecione **Nova zona do kubernetes**.
- 3 Especifique os detalhes da **conta** para a conta de nuvem do vSphere pretendida.
- 4 Clique no ícone de pesquisa na caixa de texto para exibir todas as contas do vSphere ou procurar uma conta por nome.
- 5 Digite um **Nome** e uma **Descrição** para a nova zona.

- 6 Adicione tags de capacidade, se apropriado. Consulte [Como usar tags de capacidade no Cloud Assembly](#) para informações adicionais.
- 7 Clique na guia provisionamento para selecionar o cluster do supervisor que será associado aos namespaces.
- 8 Clique em **Adicionar processamento** para exibir e selecionar os clusters de supervisor disponíveis.
- 9 Clique em **Adicionar**.
- 10 Selecione **Infraestrutura > Administração > Projetos** e, em seguida, selecione o projeto que você deseja associar à zona do kubernetes.
- 11 Clique na guia Provisionamento do Kubernetes, na página Projeto.
- 12 Clique em **Adicionar Zona do Kubernetes** e adicione a zona que você acabou de criar. Você pode criar várias zonas, se aplicável, e também definir a prioridade nas zonas.
- 13 Clique em **Salvar**.

Próximo passo

Após a configuração de um namespace, a página **Infraestrutura > Recursos > Kubernetes** no Cloud Assembly para usuários aplicáveis exibe o namespace. Os usuários podem clicar no link de Endereço da guia Resumo para abrir as Ferramentas de CLI Kubernetes do vSphere para gerenciar o namespace. Os usuários devem ser administradores de nuvem ou membros do namespace do projeto designado para acessar um link para os detalhes do Namespace de supervisor. Além disso, os usuários podem baixar um Kubectl personalizado para usar o Namespace de supervisor. Os usuários podem fazer login no namespace do supervisor, usá-lo como fariam com qualquer outro namespace e, em seguida, criar modelos de nuvem e implantar aplicativos.

Para adicionar o namespace a um modelo de nuvem, selecione **Projetar > Modelo de Nuvem** e selecione um modelo de nuvem existente ou crie um novo. Em seguida, você pode selecionar o item namespace do supervisor no menu à esquerda e arrastá-lo para a tela.

É possível atribuir políticas de armazenamento a um namespace de supervisor usando tags. É possível adicionar tags, como `location:local`, para especificar a zona Kubernetes que você deseja usar com a implantação e outras tags nos seus perfis de armazenamento, como `speed:fast` e `speed:slow`.

```
formatVersion: 1
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: 'a'
      storage:
        -profile:
          constraints:
            - tag: 'speed:fast'
        -profile:
```

```

limitMB:1000
constraints:
  -tag: 'speed:slow'

```

Esse modelo de nuvem solicita um namespace de supervisor sem restrições e especifica dois perfis de armazenamento com ele.

Depois que você implantar modelos de nuvem contendo um namespace de supervisor, os usuários também poderão solicitar namespaces de supervisor ao catálogo do Service Broker. Além disso, é possível clicar na página implantações no Cloud Assembly para visualizar informações sobre a implantação e acessar um link que contém o comando para executar o `kubectl` para o namespace no vSphere.

Você pode especificar classes de máquina virtual para namespaces de supervisor em um modelo de nuvem usando a propriedade `vmclasses`, que permite especificar um nome de classe. Consulte o exemplo de modelo de nuvem a seguir.

```

resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: demo-vmclass1
      vmclasses:
        - name: vmclass1

```

Trabalhando com clusters e namespaces do Kubernetes no Cloud Assembly

Os administradores de nuvem podem adicionar, exibir e gerenciar a configuração de clusters e namespaces implantados do Kubernetes, tanto genéricos quanto baseados no Pacific, no Cloud Assembly.

Usuários com privilégios de administrador de nuvem podem visualizar, adicionar e gerenciar clusters e namespaces do Kubernetes aos quais tem direito de acesso na página **Infraestrutura > Recursos > Kubernetes**. Essa página contém guias para Clusters, Namespaces, Clusters de Supervisor e Namespaces de Supervisor. Você pode selecionar uma dessas guias para visualizar e gerenciar os recursos análogos. Normalmente, essa página facilita o gerenciamento de clusters e namespaces implantados.

- **Cluster:** um cluster é um grupo de nós do Kubernetes distribuídos em uma ou mais máquinas físicas. Essa página mostra os clusters provisionados e não implantados que foram configurados para uso na sua instância do Cloud Assembly. Você pode clicar em um cluster para exibir informações sobre seu status atual. Quando você implanta um cluster, ele inclui um link para um arquivo `Kubconfig` que é acessível apenas para administradores de nuvem. Esse arquivo concede privilégios totais de administrador sobre o cluster, incluindo uma lista de namespaces.

Os clusters de supervisor são exclusivos para instâncias do vSphere e usam o ESXI como nós de trabalhador no lugar do Linux.

- **Namespaces:** namespaces são clusters virtuais que fornecem aos administradores uma maneira de agrupar ou separar os recursos do cluster. Elas facilitam o gerenciamento de recursos entre grandes grupos de usuários e organizações. Como um formulário de controle de acesso baseado em função, um administrador de nuvem pode permitir que os usuários adicionem namespaces a um projeto quando solicitam uma implantação e, em seguida, gerenciam esses namespaces na página Clusters do Kubernetes. Quando você implanta um namespace, ele inclui um link para um arquivo kubeconfig que permite que usuários válidos, como desenvolvedores, visualizem e gerenciem alguns aspectos desse namespace.

Clusters de supervisor e namespaces de supervisor existem apenas em instâncias do vSphere e fornecem acesso semelhante ao Kubernetes a objetos do vSphere.

Um administrador de nuvem pode alterar o projeto associado a um namespace ou cluster Kubernetes nesta página, para poder provisionar recursos Kubernetes de modelos de nuvem e do Service Broker e, em seguida, atribuí-los a projetos específicos para consumo. O administrador pode alterar o escopo de um cluster para torná-lo global ou específico do projeto. Clusters globais aparecem na guia Clusters para todas as zonas Kubernetes e estão disponíveis para seleção e provisionamento. Se um cluster for global, ele poderá ser adicionado a uma zona do Kubernetes e, em seguida, usado para provisionar namespaces do catálogo.

Se você estiver configurando um cluster novo ou existente, deverá selecionar se deseja se conectar a um endereço IP primário ou a um nome de host primário.

Trabalhar com clusters de kubernetes genéricos no Cloud Assembly

Você pode adicionar clusters novos, existentes ou externos ao Cloud Assembly usando as opções dessa página.

- 1 Selecione **Infraestrutura > Recursos > Kubernetes** e confirme se a guia Clusters está ativa.

Se houver clusters configurados no momento para a sua instância do Cloud Assembly, eles aparecerão nessa página.

- Se você estiver adicionando um cluster novo ou existente ou implantando um cluster, selecione a opção apropriada de acordo com a tabela a seguir.

| Opção | Descrição | Detalhes |
|---------------------|---|--|
| Implantar | Adicionar novos clusters ao Cloud Assembly | Você deve especificar a conta de nuvem do TKGI na qual esse cluster será implantado, bem como o plano desejado e o número de nós. |
| Adicionar Existente | Configure um cluster existente para funcionar com o seu projeto. | Você deve especificar a conta de nuvem do TKGI, o cluster a ser usado e o projeto apropriado para o desenvolvedor pretendido. Além disso, precisa especificar o escopo de compartilhamento. Se quiser compartilhar globalmente, deverá configurar suas zonas e namespaces do Kubernetes apropriadamente. |
| Adicionar Externo | Adicione um cluster do Kubernetes vanilla, que pode não estar associado ao TKGI, ao Cloud Assembly. | Você deve designar um projeto ao qual o cluster esteja associado, inserir o endereço IP do cluster desejado e selecionar um proxy de nuvem e as informações de certificado necessárias para se conectar a esse cluster. |

- Clique em **Adicionar** para disponibilizar o cluster no Cloud Assembly.

Trabalhando com namespaces do Kubernetes no Cloud Assembly

Se você for um administrador de nuvem, namespaces o ajudarão a agrupar e gerenciar recursos de clusters do Kubernetes. Se você for um usuário, namespaces serão a área nos clusters do Kubernetes para suas implantações. Administradores e usuários podem acessar namespaces usando a guia Namespaces localizada na página **Infraestrutura > Recursos > Kubernetes**.

Existem várias maneiras de adicionar namespaces do Kubernetes a recursos no Cloud Assembly. O procedimento a seguir descreve um método típico.

- Selecione **Infraestrutura > Recursos > Kubernetes** e clique na guia Namespaces.
- Para adicionar um novo namespace, clique em **Novo Namespace**. Para adicionar um namespace existente, clique em **Adicionar Namespace**.

- Insira um **Nome** e uma **Descrição** para o namespace.

Nesse ponto, você adicionou um namespace para uso com os recursos do Kubernetes, mas ele não está associado a nada em particular.

- Especifique o **Cluster** que você deseja associar a esse namespace.
- Clique em **Criar** para adicionar o namespace ao Cloud Assembly.

Você pode adicionar propriedades personalizadas aos namespaces Kubernetes para oferecer suporte à extensibilidade de várias maneiras diferentes. Você adiciona propriedades personalizadas ao provisionar um namespace criando um modelo de nuvem do Cloud Assembly. Ao especificar um namespace Kubernetes em um modelo de nuvem, você pode adicionar

propriedades a esse namespace. Primeiro, é possível clicar com o botão direito nas propriedades do modelo para acessar as propriedades padrão que fazem parte do esquema do modelo de nuvem. Como segunda opção, é possível adicionar propriedades definidas pelo usuário na seção de propriedades do namespace no modelo de nuvem.

Após a implantação, essas propriedades personalizadas aparecem na página Implantações do Cloud Assembly para a implantação aplicável.

Por fim, você também pode adicionar propriedades personalizadas a um namespace usando ações configuradas na página **Extensibilidade > Ações** do Cloud Assembly.

Trabalhar com clusters de supervisor e namespaces de supervisor

Os administradores de nuvem podem visualizar e alterar a configuração de clusters de supervisor e namespaces na página Kubernetes do Cloud Assembly.

- 1 Selecione **Infraestrutura > Recursos > Kubernetes** no Cloud Assembly.
- 2 Selecione **Adicionar Cluster de Supervisor**.
- 3 Especifique os detalhes da Conta para a conta de nuvem do vSphere pretendida.
- 4 Clique no ícone Pesquisar na caixa de texto Cluster de supervisor para exibir todos os clusters de supervisor ou procure um cluster por nome.
- 5 Selecione o cluster desejado e clique em **Adicionar**.
- 6 Selecione a guia Namespaces de Supervisor e clique no botão **Novo Namespace de Supervisor** para adicionar um novo namespace.
- 7 Selecione a guia Namespaces de Supervisor e clique no botão **Novo Namespace de Supervisor** para adicionar um novo namespace.
 - a Se estiver criando um novo namespace, adicione um **Nome** e uma **Descrição**.
 - b Selecione a **Conta** de nuvem apropriada a ser associada ao namespace.
 - c Selecione o **Cluster de supervisor** a ser associado a esse namespace.
 - d Selecione o **Projeto** a ser associado ao namespace.
 - e Use a seleção de **Políticas de armazenamento disponíveis** para adicionar políticas de armazenamento para uso com o namespace.

Você pode adicionar todas as políticas de armazenamento disponíveis ou selecionar políticas específicas para uso com o namespace de supervisor. Além disso, existe a opção de definir um limite no tamanho de armazenamento disponível com cada política de armazenamento disponível.
 - f Clique em **Criar**.
- 8 Revise os detalhes relevantes para o novo namespace. Você poderá alterar a configuração da política de armazenamento se necessário.

Os usuários e grupos que atualmente têm acesso ao namespace no vSphere estão listados na guia **Usuários**. Se novos usuários ou grupos forem adicionados ao projeto, clique no botão **Atualizar usuários** nessa guia para atualizar a lista. A lista não é atualizada automaticamente e, portanto, você deve usar o botão para atualizar.

Observação A sincronização de usuários fará sentido apenas se o Cloud Assembly e o vCenter estiverem configurados com um serviço do Active Directory/LDAP em comum.

Depois que um cluster ou namespace é configurado, a página **Infraestrutura > Recursos > Kubernetes** no Cloud Assembly exibirá os clusters e namespaces disponíveis para o usuário. Você pode clicar em um namespace ou cluster individual para abrir uma página que contém uma série de guias que mostram estatísticas e outras informações para o recurso e que permite configurar várias opções.

A guia **Resumo** para clusters na página **Kubernetes** permite que os administradores visualizem e, em alguns casos, atualizem a configuração de um cluster, incluindo a alteração do escopo. Os botões de opção **Compartilhamento** permitem que você selecione **Global** (compartilhável na Zona do Kubernetes) ou **Projeto** (acesso limitado a um único projeto). Se você selecionar **Projeto**, também deverá especificar o projeto aplicável na seleção de **Projeto** a seguir.

Observação Alterar a configuração de compartilhamento pode afetar os namespaces que estão disponíveis no cluster.

Os usuários podem clicar no link de **Endereço** da guia **Resumo** para abrir as Ferramentas de CLI Kubernetes do vSphere para gerenciar o namespace. Os usuários devem ser administradores de nuvem ou membros do namespace do projeto designado para acessar um link para os detalhes do Namespace de supervisor. Além disso, os usuários podem baixar um Kubectl personalizado para usar o Namespace de supervisor. Os usuários podem fazer login no namespace do supervisor, usá-lo como fariam com qualquer outro namespace e, em seguida, criar modelos de nuvem e implantar aplicativos.

Adicionando componentes Kubernetes a modelos de nuvem no Cloud Assembly

Ao adicionar componentes do Kubernetes a um modelo de nuvem do Cloud Assembly, você pode optar por adicionar clusters ou permitir que os usuários criem namespaces em várias configurações. Normalmente, essa escolha depende dos seus requisitos de controle de acesso, de como você configurou seus componentes do Kubernetes e dos seus requisitos de implantação.

Para adicionar um componente do Kubernetes a um modelo de nuvem no Cloud Assembly, clique em **Design > Modelos de Nuvem**, clique em **Novo** e localize e expanda a opção **Kubernetes** no menu à esquerda. Em seguida, faça a seleção desejada, **Cluster** ou **Namespace KBS**, arrastando-a até a tela.

Adicionar um cluster do Kubernetes associado a um projeto até um modelo de nuvem é o método mais simples de disponibilizar recursos do Kubernetes para usuários válidos. Você pode usar tags em clusters para controlar onde eles são implantados, como você faz com outros recursos do Cloud Assembly. É possível usar tags para selecionar uma zona e um plano do VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) durante a fase de alocação da implantação do cluster.

Ao adicionar um cluster dessa maneira, ele é disponibilizado automaticamente para todos os usuários válidos.

Exemplos de modelos de nuvem

O primeiro exemplo de modelo de nuvem mostra um modelo para uma implantação simples do Kubernetes que é controlada por marcação. Uma zona do Kubernetes foi criada com dois planos de implantação, configurados na página Nova Zona do Kubernetes. Nesse caso, uma tag chamada `placement:tag` foi adicionada como recurso na zona e foi usada para corresponder à restrição análoga no modelo de nuvem. Se houver mais de uma zona configurada com a tag, aquela com o número de prioridade mais baixa será selecionada.

```
formatVersion: 1
inputs: {}
resources:
  Cluster_provisioned_from_tag:
    type: Cloud.K8S.Cluster
    properties:
      hostname: 109.129.209.125
      constraints:
        -tag: 'placement tag'
      port: 7003
      workers: 1
      connectBy: hostname
```

Os segundo exemplo de modelo de nuvem mostra como configurar um modelo com uma variável chamada `$(input.hostname)`, para que os usuários possam inserir o nome do host do cluster desejado ao solicitar uma implantação. Tags também podem ser usadas para selecionar uma zona e um plano do TKGI durante a fase de alocação de recursos da implantação do cluster.

```
formatVersion: 1
inputs:
  hostname:
    type: string
    title: Cluster hostname
resources:
  Cloud_K8S_Cluster_1:
    type: Cloud.K8S.Cluster
    properties:
      hostname: ${input.hostname}
      port: 8443
      connectBy: hostname
      workers: 1
```

Se quiser usar namespaces para gerenciar o uso do cluster, você poderá configurar uma variável no modelo de nuvem chamada `name: ${input.name}` para substituir o nome do namespace que um usuário insere ao solicitar uma implantação. Para esse tipo de implantação, crie um modelo semelhante ao exemplo a seguir:

```
1 formatVersion: 1
2 inputs:
```

```

3 name:
4   type: string
5   title: "Namespace name"
6 resources:
7   Cloud_K8S_Namespace_1:
8     type: Cloud.K8S.Namespace
9     properties:
10      name: ${input.name}

```

Os usuários podem gerenciar clusters implantados por meio de arquivos kubeconfig acessíveis na página **Infraestrutura > Recursos > Clusters do Kubernetes**. Localize o cartão na página para o cluster desejado e clique em **Kubeconfig**.

Namespaces de Supervisor em VMware Cloud Templates

Veja a seguir o esquema para um namespace de supervisor básico em um modelo de nuvem do Cloud Assembly.

```

{
  "title": "Supervisor namespace schema",
  "description": "Request schema for provisioning of Supervisor namespace resource",
  "type": "object",
  "properties": {
    "name": {
      "title": "Name",
      "description": "Alphabetic (a-z and 0-9) string with maximum length of 63 characters. The character '-' is allowed anywhere except the first or last position of the identifier.",
      "type": "string",
      "pattern": "^[a-z0-9]([a-z0-9-]{1,63})$",
      "ignoreOnUpdate": true
    },
    "description": {
      "title": "Description",
      "description": "An optional description of this Supervisor namespace.",
      "type": "string",
      "ignoreOnUpdate": true
    },
    "content": {
      "title": "Content",
      "description": "Kubernetes Yaml Content",
      "type": "string",
      "maxLength": 65000
    },
    "constraints": {
      "title": "Constraints",
      "description": "To target the correct resources, blueprint constraints are matched against infrastructure capability tags. Constraints must include the key name. Options include value, negative [!], and hard or soft requirement.",
      "type": "array",
      "recreateOnUpdate": true,
      "items": {
        "type": "object",
        "properties": {
          "tag": {

```

```

        "title": "Tag",
        "description": "Constraint definition in syntax `[!]tag_key[:tag_value]`  

[:hard|:soft]` \nExamples:\n```\n!location:eu:hard\n location:us:soft\n!pci\n```,",
        "type": "string",
        "recreateOnUpdate": true
    }
}
},
"limits": {
    "title": "Limits",
    "description": "Defines namespace resource limits such as pods, services, etc.",
    "type": "object",
    "properties": {
        "stateful_set_count": {
            "title": "stateful_set_count",
            "description": "This represents the new value for 'statefulSetCount' option which  

is the maximum number of StatefulSets in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "deployment_count": {
            "title": "deployment_count",
            "description": "This represents the new value for 'deploymentCount' option which is  

the maximum number of deployments in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "cpu_limit_default": {
            "title": "cpu_limit_default",
            "description": "This represents the new value for the default CPU limit (in Mhz)  

for containers in the pod. If specified, this limit should be at least 10 MHz.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "config_map_count": {
            "title": "config_map_count",
            "description": "This represents the new value for 'configMapCount' option which is  

the maximum number of ConfigMaps in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "pod_count": {
            "title": "pod_count",
            "description": "This represents the new value for 'podCount' option which is the  

maximum number of pods in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        },
        "job_count": {
            "title": "job_count",
            "description": "This represents the new value for 'jobCount' option which is the  

maximum number of jobs in the namespace.",
            "type": "integer",
            "recreateOnUpdate": false
        }
    }
}

```

```

    },
    "secret_count": {
      "title": "secret_count",
      "description": "This represents the new value for 'secretCount' option which is the
maximum number of secrets in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "cpu_limit": {
      "title": "cpu_limit",
      "description": "This represents the new value for 'limits.cpu' option which is
equivalent to the maximum CPU limit (in MHz) across all pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "cpu_request_default": {
      "title": "cpu_request_default",
      "description": "This represents the new value for the default CPU request (in Mhz)
for containers in the pod. If specified, this field should be at least 10 MHz.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_limit_default": {
      "title": "memory_limit_default",
      "description": "This represents the new value for the default memory limit (in
mebibytes) for containers in the pod.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_limit": {
      "title": "memory_limit",
      "description": "This represents the new value for 'limits.memory' option which is
equivalent to the maximum memory limit (in mebibytes) across all pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_request_default": {
      "title": "memory_request_default",
      "description": "This represents the new value for the default memory request (in
mebibytes) for containers in the pod.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "service_count": {
      "title": "service_count",
      "description": "This represents the new value for 'serviceCount' option which is
the maximum number of services in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "replica_set_count": {
      "title": "replica_set_count",
      "description": "This represents the new value for 'replicaSetCount' option which is
the maximum number of ReplicaSets in the namespace.",
      "type": "integer",

```

```

    "recreateOnUpdate": false
  },
  "replication_controller_count": {
    "title": "replication_controller_count",
    "description": "This represents the new value for 'replicationControllerCount'
option which is the maximum number of ReplicationControllers in the namespace.",
    "type": "integer",
    "recreateOnUpdate": false
  },
  "storage_request_limit": {
    "title": "storage_request_limit",
    "description": "This represents the new value for 'requests.storage' which is the
limit on storage requests (in mebibytes) across all persistent volume claims from pods in the
namespace.",
    "type": "integer",
    "recreateOnUpdate": false
  },
  "persistent_volume_claim_count": {
    "title": "persistent_volume_claim_count",
    "description": "This represents the new value for 'persistentVolumeClaimCount'
option which is the maximum number of PersistentVolumeClaims in the namespace.",
    "type": "integer",
    "recreateOnUpdate": false
  },
  "daemon_set_count": {
    "title": "daemon_set_count",
    "description": "This represents the new value for 'daemonSetCount' option which is
the maximum number of DaemonSets in the namespace.",
    "type": "integer",
    "recreateOnUpdate": false
  }
},
"additionalProperties": false
},
"vm_classes": {
  "title": "VM classes",
  "description": "Defines set of Virtual Machine classes to be assigned to the namespace",
  "type": "array",
  "recreateOnUpdate": false,
  "items": {
    "type": "object",
    "properties": {
      "name": {
        "title": "Name",
        "description": "Name of the Virtual Machine class.",
        "type": "string",
        "recreateOnUpdate": false
      }
    }
  }
},
"storage": {
  "title": "Storage policies",
  "description": "Defines set of storage profiles to be used to assign storage policies
to the namespace.",

```

```

    "type": "array",
    "recreateOnUpdate": false,
    "items": {
      "type": "object",
      "properties": {
        "profile": {
          "type": "object",
          "title": "Storage profile",
          "description": "Defines storage policies to be assigned to the namespace",
          "recreateOnUpdate": false,
          "properties": {
            "constraints": {
              "title": "Constraints",
              "description": "To target the correct storage profiles, blueprint constraints
are matched against storage profile capability tags.",
              "type": "array",
              "recreateOnUpdate": false,
              "items": {
                "type": "object",
                "properties": {
                  "tag": {
                    "title": "Tag",
                    "description": "Constraint definition in syntax `[!]  
[:hard|:soft]` \nExamples:\n```\nlocation:eu:hard\n location:us:soft\n```\n",
                    "type": "string",
                    "recreateOnUpdate": false
                  }
                }
              },
              "minItems": 1
            },
            "limitMb": {
              "title": "Limit",
              "description": "The maximum amount of storage (in mebibytes) which can be
utilized by the namespace for this storage policy. Optional. If unset, no limits are placed.",
              "type": "integer"
            }
          },
          "required": [
            "constraints"
          ]
        }
      }
    },
    "required": [
      "name"
    ]
  }
}

```

Os VMware Cloud Templates oferecem suporte ao uso de limites com namespaces de supervisor. Os limites permitem que você controle o uso de recursos para CPUs e memória, bem como o número máximo de pods permitidos no namespace por máquinas implantadas.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: '${env.deploymentName}'
      limits:
        - cpu_limit: 1000
          cpu_request_default: 800
          memory_limit: 2000
          memory_limit_default: 1500
          pod_count: 200
```

O exemplo a seguir mostra como você pode especificar uma política de armazenamento usando tags.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: 'ns-with-storage-policy'
      description: 'sample'
      storage:
        - profile:
            limitMb: 1000
            constraints:
              - tag: 'storage:fast'
          - profile:
            constraints:
              - tag: 'storage:cheap'
```

Usando YAMLS arbitrários com VCTs de cluster ou namespace de autoatendimento

Como parte da criação de um cluster ou namespace, os usuários geralmente desejam executar personalizações adicionais. Por exemplo, você pode querer adicionar usuários (associação de função/ função) ou criar uma política de segurança de pod ou instalar agentes. Usando a propriedade YAML `content`, os usuários podem definir pacotes personalizados que desejam provisionar nesse cluster/namespaces /namespace de supervisor.

Cada pacote de conteúdo YAML associado à propriedade `content` deve ser separado com um traço triplo (---). Além disso, as informações de conteúdo devem ser uma cadeia de caracteres de várias linhas. Consulte o exemplo YAML a seguir para ver como os pacotes de conteúdo podem ser configurados.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Tanzu_Cluster_1:
    type: Cloud.Tanzu.Cluster
    properties:
      name: ddonchev-tkc
      plan: small
      content: |-
        apiVersion: rbac.authorization.k8s.io/v1
        kind: ClusterRoleBinding
        metadata:
          name: psp:authenticated-from-yaml
        subjects:
        - apiGroup: rbac.authorization.k8s.io
          kind: Group
          name: system:authenticated
        roleRef:
          apiGroup: rbac.authorization.k8s.io
          kind: ClusterRole
          name: psp:vmware-system-privileged
        ---
        apiVersion: apiextensions.k8s.io/v1
        kind: CustomResourceDefinition
        metadata:
          # name must match the spec fields below, and be in the form: <plural>.<group>
          name: crontabs.stable.example.com
        spec:
          # group name to use for REST API: /apis/<group>/<version>
          group: stable.example.com
          # list of versions supported by this CustomResourceDefinition
          versions:
            - name: v1
              # Each version can be enabled/disabled by Served flag.
              served: true
              # One and only one version must be marked as the storage version.
              storage: true
              schema:
                openAPIV3Schema:
                  type: object
                  properties:
                    spec:
                      type: object
                      properties:
                        cronSpec:
                          type: string
                        image:
                          type: string
                        replicas:
```

```

        type: integer
# either Namespaced or Cluster
scope: Namespaced
names:
  # plural name to be used in the URL: /apis/<group>/<version>/<plural>
  plural: crontabs
  # singular name to be used as an alias on the CLI and for display
  singular: crontab
  # kind is normally the CamelCased singular type. Your resource manifests use this.
  kind: CronTab
  # shortNames allow shorter string to match your resource on the CLI
  shortNames:
    - ct

```

O YAML definido na propriedade de conteúdo também aparece na guia Propriedades da implantação.

O Cloud Assembly apenas pode criar recursos de conteúdo no escopo do recurso que está sendo implantado. Por exemplo: se você provisionar um namespace do Kubernetes, o Cloud Assembly não poderá criar uma implantação dentro de um namespace diferente. Os usuários têm os mesmos direitos como se estivessem usando o kubeconfig com kubectl.

Depois que a máquina virtual for provisionada, uma instalação dos objetos Kubernetes dentro da propriedade `content` será iniciada. Se o provisionamento de um dos recursos referenciados na propriedade de conteúdo YAML falhar, o Cloud Assembly reverterá e excluirá todos os objetos Kubernetes anteriores desse recurso, e a implantação terá um status de Falha. O recurso ainda estará provisionado e visível. Além disso, você ainda pode usar ações de dia 2, incluindo tentar aplicar o conteúdo novamente.

Você pode aprimorar a propriedade `content` com entradas do modelo de nuvem, como mostra o exemplo a seguir.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: sv-namespace-with-vm-classes
      vm_classes:
        - name: best-effort-2xlarge
        - name: best-effort-4xlarge
        - name: best-effort-8xlarge

```

Além disso, você pode provisionar recursos personalizados, como `TanzuKubernetesCluster`. Isso falharia como uma operação de dia 1, pois o namespace do supervisor não conterá as classes de máquina virtual e as classes de armazenamento necessárias. Quando as classes de máquina virtual e as classes de armazenamento estão vinculadas ao namespace de supervisor, você pode criar `TanzuKubernetesCluster` (ou outro recurso) usando a ação de dia 2.

Observação: você pode provisionar um recurso sem conteúdo e ainda poderá adicionar objetos Kubernetes como YAML com a ação de dia 2.

O conteúdo que aparece na propriedade YAML define o que é provisionado no recurso. Quando você edita esse conteúdo, a tabela a seguir mostra os resultados possíveis:

| Ação | Resultado |
|---|---|
| Se adicionar um objeto Kubernetes e enviar. | O objeto especificado é criado no recurso. |
| Se remover um objeto Kubernetes e enviar. | O objeto especificado é excluído do recurso. |
| Se modificar um objeto Kubernetes e enviar. | O objeto especificado é corrigido no recurso. |

É importante esclarecer quais ações são consideradas como uma modificação no objeto atual. Por exemplo: se você modificar o campo de namespace de um objeto, um novo objeto será criado no lugar do antigo que está sendo corrigido.

A exclusividade de um recurso é definida pelos seguintes campos: `apiVersion`, `kind`, `metadata.name` e `metadata.namespace`

Usando a extensibilidade do Cloud Assembly com o Kubernetes

O Cloud Assembly fornece um conjunto de tópicos de eventos que correspondem a ações típicas relacionadas à implantação do namespace e do cluster Kubernetes. Os usuários podem assinar esses tópicos conforme desejado, e eles serão executados no momento apropriado. Os usuários recebem uma notificação quando ocorre o evento relacionado ao tópico inscrito. Você também pode configurar fluxos de trabalho do vRO para serem executados com base em notificações de eventos.

Os tópicos a seguir estão disponíveis para assinatura na página **Extensibilidade > Biblioteca > Tópicos de Evento** do Cloud Assembly. Para visualizar esses tópicos, procure Kubernetes na caixa de texto de pesquisa de Tópicos de Evento.

- Alocação do cluster do Kubernetes
- Pós-provisionamento do cluster do Kubernetes
- Remoção do cluster do Kubernetes
- Provisão do cluster do Kubernetes
- Remoção de cluster do Kubernetes
- Alocação de namespaces do Kubernetes
- Pós-provisionamento de namespaces do Kubernetes
- Pós-remoção de namespaces do Kubernetes
- Remoção de namespaces do Kubernetes
- Alocação de namespaces do Kubernetes
- Alocação de namespaces de supervisor do Kubernetes
- Pós-provisionamento de namespaces de supervisor do Kubernetes
- Pós-remoção de namespaces de supervisor do Kubernetes

- Remoção de namespaces de supervisor do Kubernetes
- Alocação de namespaces de supervisor do Kubernetes

Clique em um dos tópicos para exibir o esquema desse tópico que mostra todas as informações coletadas e transmitidas. Existem tópicos de namespace para namespaces do Kubernetes e namespaces de supervisor. Você pode usar qualquer uma dessas informações de esquema para configurar várias tarefas de gerenciamento e notificações.

É possível configurar scripts de ação para ações relacionadas ao CMX na página **Extensibilidade > Biblioteca > Ações**. Scripts de ação podem ser usados para vários fins: por exemplo, para criar um registro de DNS do provisionamento de clusters do Kubernetes. Se você estiver criando um registro de DNS, poderá usar o campo `masternodeips` do tópico de pós-provisionamento de clusters do Kubernetes com um comando REST em um script de Ação para criar um registro de DNS.

A página Assinaturas define a relação entre os tópicos de evento e os scripts de ação. É possível visualizar e gerenciar esses componentes na página Assinaturas do Cloud Assembly

Consulte a documentação sobre extensibilidade do Cloud Assembly em [Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade](#) para obter mais informações.

O que é o gerenciamento de configuração no Cloud Assembly

O Cloud Assembly oferece suporte à integração com o Puppet Enterprise, o Ansible Open Source e o Ansible Tower para poder gerenciar configuração e descompasso das implantações.

Integração com o Puppet

Para integrar o gerenciamento de configuração baseado no Puppet, é necessário ter uma instância válida do Puppet Enterprise instalada em uma nuvem pública ou privada com uma carga de trabalho do vSphere. É necessário estabelecer uma conexão entre este sistema externo e sua instância do Cloud Assembly. Em seguida, é possível tornar o gerenciamento de configuração do Puppet disponível para o Cloud Assembly adicionando-o aos blueprints apropriados.

O provedor Puppet do serviço de blueprint do Cloud Assembly instala, configura e executa o agente Puppet em um recurso de processamento implantado. O provedor Puppet oferece suporte a conexões SSH e WinRM com os seguintes pré-requisitos:

- Conexões SSH:
 - O nome de usuário deve ser um super usuário ou um usuário com permissões sudo para executar comandos com `NOPASSWD`.
 - Desativar `requiretty` para o usuário especificado.
 - O cURL deve estar disponível no recurso de processamento na implantação.
- Conexões WinRM:
 - O PowerShell 2.0 deve estar disponível no recurso de processamento de implantação.

- Configure o modelo do Windows conforme descrito na documentação do vRealize Orchestrator.

O administrador do DevOps é responsável por gerenciar as conexões a um Puppet mestre e por aplicar funções de Puppets ou regras de configuração a implantações específicas. Após a implantação, as máquinas virtuais configuradas para oferecer suporte ao gerenciamento de configuração são registradas com o Puppet mestre designado.

Quando as máquinas virtuais são implantadas, os usuários podem adicionar ou excluir um Puppet mestre como um sistema externo ou atualizar projetos atribuídos ao Puppet mestre. Por fim, os usuários apropriados podem cancelar o registro de máquinas implantadas do Puppet Master quando essas máquinas são desativadas.

Integração do Ansible Open Source

Ao configurar uma integração do Ansible, instale o Ansible Open Source de acordo com as instruções de instalação do Ansible. Consulte a documentação do Ansible para obter mais informações sobre a instalação.

O Ansible habilita a verificação de chave de host por padrão. Se um host for reinstalado com uma chave diferente no arquivo `known_hosts`, uma mensagem de erro será exibida. Se um host não estiver listado no arquivo `known_hosts`, você deverá fornecer a chave na inicialização. É possível desativar a verificação da chave de host com a seguinte configuração no arquivo `/etc/ansible/ansible.cfg` ou `~/.ansible.cfg`:

```
[defaults]
host_key_checking = False
localhost_warning = False

[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null
```

Para evitar os erros de verificação da chave de host, defina `host_key_checking` e `record_host_keys` como `False`, incluindo a adição de uma opção extra `UserKnownHostsFile=/dev/null` definida no `ssh_args`. Além disso, se o inventário estiver vazio inicialmente, o Ansible avisará que a lista de hosts está vazia. Isso faz com que a verificação de sintaxe do playbook falhe.

O Ansible Vault permite armazenar informações confidenciais, como senhas ou chaves, em arquivos criptografados ao invés de texto simples. O cofre é criptografado com uma senha. No Cloud Assembly, o Ansible usa o Cofre para criptografar dados, como senhas SSH para máquinas de host. Ele assume que o caminho para a senha do cofre foi definido.

É possível modificar o arquivo `ansible.cfg` para especificar a localização do arquivo de senha usando o seguinte formato.

```
vault_password_file = /path to/file.txt
```

Também é possível definir a variável de ambiente `ANSIBLE_VAULT_PASSWORD_FILE` para que o Ansible pesquise a senha automaticamente. Por exemplo,

```
ANSIBLE_VAULT_PASSWORD_FILE=~/.vault_pass.txt
```

O Cloud Assembly gerencia o arquivo de inventário do Ansible, portanto, é necessário garantir que o usuário o Cloud Assembly tenha acesso ao arquivo de inventário.

```
cat ~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1)/log.txt
```

Se quiser usar um usuário não root com a integração de código-fonte aberto do Cloud Assembly, os usuários precisarão de um conjunto de permissões para executar os comandos usados pelo provedor de código-fonte aberto do Cloud Assembly. Os seguintes comandos devem ser definidos no arquivo `sudoers` do usuário.

```
Defaults:myuser !requiretty
```

Se o usuário não fizer parte de um grupo de administradores que não tenha um aplicativo `askpass` especificado, defina o seguinte comando no arquivo `sudoers` do usuário.

```
myuser ALL=(ALL) NOPASSWD: ALL
```

Se você encontrar erros ou outros problemas ao configurar a integração com o Ansible, consulte o arquivo `log.txt` em `'cat~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1)/'` na máquina de controle do Ansible.

Integração com o Ansible Tower

Tipos de sistemas operacionais com suporte

- O Red Hat Enterprise Linux 8.0 ou posterior de 64 bits (x86) apenas oferece suporte ao Ansible Tower 3.5 e versões superiores.
- Red Hat Enterprise Linux 7.4 ou posterior de 64-bit (x86).
- CentOS 7.4 ou posterior de 64 bits (x86).

Esta é uma amostra de arquivo de inventário que é gerada durante uma instalação do Ansible Tower. Talvez seja necessário modificá-la para usos de integração com o Cloud Assembly.

```
[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# pwd

/root/ansible-tower-install/ansible-tower-setup-bundle-3.5.2-1.el8

[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# cat inventory

[tower]

localhost ansible_connection=local
```

```
[database]

[all:vars]
admin_password='VMware1!'

pg_host=''
pg_port=''

pg_database='awx'
pg_username='awx'
pg_password='VMware1!'

rabbitmq_port=5672
rabbitmq_vhost=tower
rabbitmq_username=tower
rabbitmq_password='VMware1!'
rabbitmq_cookie=cookiemonster

# Needs to be true for fqdns and ip addresses
rabbitmq_use_long_name=false

# Isolated Tower nodes automatically generate an RSA key for authentication;
# To deactivate this behavior, set this value to false
# isolated_key_generation=true
```

Configurar a integração com o Puppet Enterprise no Cloud Assembly

O Cloud Assembly oferece suporte à integração com o gerenciamento de configuração do Puppet Enterprise.

Quando você adiciona o Puppet Enterprise ao Cloud Assembly como um sistema externo, por padrão, ele é disponibilizado em todos os projetos. Você pode restringi-lo a projetos específicos.

Para adicionar uma integração com o Puppet Enterprise, é necessário ter o nome do mestre Puppet e o nome do host ou endereço IP do mestre.

Você pode encontrar os logs do Puppet na seguinte localização, caso precise verificá-los em busca de erros ou para fins de informações.

| Descrição | Localização do Log |
|---|--|
| Log para criar e instalar eventos relacionados | Os logs estão na máquina implantada, em <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`</code> . Consulte o arquivo log.txt para obter logs completos. Para logs de agentes Puppet detalhados, consulte https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging |
| Log para tarefas relacionadas a exclusão e execução do Puppet | Os logs estão no PE em <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`</code> . Consulte o arquivo log.txt para obter logs completos. |

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione Puppet.
- 3 Digite as informações necessárias na página de configuração do Puppet.

Para que a integração com o Puppet funcione adequadamente, as credenciais fornecidas devem ser válidas para o SSH e para a conta de API. Além disso, as contas de usuário do SO e do aplicativo especificadas devem ter o mesmo nome de usuário e a mesma senha.
- 4 Clique em **Validar** para verificar a integração.
- 5 Clique em **Adicionar**.

Resultados

O Puppet está disponível para uso com modelos de nuvem.

Próximo passo

Adicione componentes do Puppet aos modelos de nuvem desejados.

- 1 Em Modelos de nuvem, no Cloud Assembly, selecione Puppet sob o título Gerenciamento de Conteúdo no menu do modelo de nuvem e arraste o componente Puppet até a tela.

2 Digite as propriedades do Puppet no painel à direita.

| Propriedade | Descrição |
|---------------------------------|--|
| Mestre | Insira o nome da máquina primária Puppet a ser usada com esse modelo de nuvem. |
| Ambiente | Selecione o ambiente da máquina primária do Puppet. |
| Função | Selecione a função Puppet a ser usada com esse modelo de nuvem. |
| Intervalo de execução do agente | A frequência com que você deseja que o agente Puppet faça sondagens na máquina primária Puppet em busca de detalhes de configuração a serem aplicados a máquinas virtuais implantadas relacionadas a esse modelo de nuvem. |

3 Clique na guia Código no painel à direita para visualizar o código YAML para as propriedades de configuração do Puppet.

Quando você adiciona um componente do Puppet a um modelo de nuvem, pode adicionar a propriedade `installMaster` ao arquivo YAML para apontar a um mestre de instalação do Puppet, também conhecido como mestre de compilação. O valor dessa propriedade pode ser o endereço IP ou o nome do host do mestre de compilação do Puppet. Usar essa propriedade fornece acesso a capacidades aprimoradas para máquinas virtuais Puppet implantadas e também oferece suporte a ações de dia 2 adicionais.

```
Puppet_Agent:
  type: Cloud.Puppet
  properties:
    account: PEIntegrationAccount
    environment: production
    role: 'role::linux_webserver'
    host: '${CentOS-Puppet.*}'
    username: root
    password: password123!
    installMaster: my-pe-compile-master.example.com
    agentConfiguration:
      certName: '${CentOS-Puppet.address}'
    osType: linux
    count: 1
```

Observação Embora o usuário definido aqui seja root, o modelo de nuvem pode ser configurado com qualquer usuário que esteja incluído na lista de sudoers.

Em alguns casos, o vRealize Automation transmite, por padrão, algumas informações relacionadas à máquina para as máquinas virtuais do Puppet como fatos. Fatos personalizados não são aceitos em máquinas Windows. Em máquinas Linux, algumas informações são transmitidas por padrão, e os usuários podem transmitir informações adicionais usando propriedades personalizadas.

Existem algumas limitações sobre o que é transmitido às máquinas Puppet no Linux. Propriedades personalizadas nos recursos de host e no agente Puppet são transmitidas a máquinas virtuais Puppet. Propriedades personalizadas em recursos de rede não são transmitidas à máquina virtual. Os itens passados incluem propriedades simples, propriedades booleanas, bem como nomes personalizados e tipos complexos, como mapas aninhados com matrizes.

O exemplo a seguir mostra como vários recursos personalizados podem ser chamados em recursos de host:

```
resources:
  Puppet-Host:
    type: Cloud.AWS.EC2.Instance
    properties:
      customer_specified_property_on_ec2_resource: "property"

customer_specified_property_on_network_resource_that_should_also_be_a_fact_and_is_boolean:
true
  CustomerNameStuff: "zone A"
  try_map:
    key: value
    keytwo: value
  nested_array:
    - one
    - two
    - true
  try_array:
    - one
    - two
    -three:
      inner_key: value
```

Se um comando de expurgação do Puppet resultar em erros, na maioria dos casos, o vRealize Automation ignorará os erros de eliminação dos nós e prosseguirá com a exclusão do nó. Mesmo que um certificado não seja encontrado para um nó específico, o vRealize Automation prosseguirá com a exclusão. Se o vRealize Automation não puder prosseguir com a exclusão do nó por algum motivo, você poderá clicar em Excluir no menu Ações da página Implementações para abrir uma caixa de diálogo que permitirá que você prossiga com a exclusão do nó. Um fluxo de trabalho semelhante é executado quando você remove uma integração do Puppet de um modelo de nuvem e, em seguida, aplica o modelo à implantação. Esse fluxo de trabalho aciona uma operação de limpeza de nó que é tratada conforme descrito acima.

A integração com o Puppet Enterprise requer um endereço IP público. Se não houver nenhum endereço IP público configurado para a máquina do Puppet Enterprise, o endereço IP da primeira NIC será usado.

Se o NIC de uma máquina provisionada Puppet em execução em uma máquina vSphere tem vários endereços IP, você pode usar a propriedade YAML `primaryAddress` nos modelos de nuvem para especificar qual endereço IP será usado para conexões. Quando a propriedade `primaryAddress` é atribuída a um NIC, o Puppet usa o endereço IP desse NIC. Apenas uma NIC pode ser designada como primária. Veja um exemplo de como a propriedade `primaryAddress` é usada no snippet YAML a seguir.

```
BaseVM:
  type: Cloud.vSphere.Machine
  properties:
    image: photon
    count: 2
    customizationSpec: Linux
    cpuCount: 1
    totalMemoryMB: 1024
    networks:
      - network: '${resource.dev.id}'
        deviceIndex: 0
        primaryAddress: true
        assignment: static
      - network: '${resource.prod.id}'
        deviceIndex: 1
        assignment: static
```

Se a propriedade `primaryAddress` não foi definida para nenhum NIC de máquina virtual, a lógica do modelo de nuvem é padronizada para o comportamento atual de seleção de endereço IP.

Configurar a integração do Ansible Open Source no Cloud Assembly

O Cloud Assembly oferece suporte à integração com o gerenciamento de configuração do Ansible Open Source. Depois de configurar a integração, é possível adicionar componentes do Ansible a implantações novas ou existentes.

Quando você integra o Ansible Open Source ao Cloud Assembly, é possível configurá-lo para executar uma ou mais guias estratégicos do Ansible em uma determinada ordem quando uma nova máquina é provisionada para automatizar o gerenciamento de configuração. Especifique os playbooks desejados para uma implantação no modelo de nuvem.

Ao configurar uma integração do Ansible, é necessário especificar a máquina host do Ansible Open Source, bem como o caminho do arquivo de inventário que define informações para gerenciar recursos. Além disso, é necessário fornecer um nome e uma senha para acessar a instância do Ansible Open Source. Posteriormente, quando você adicionar um componente Ansible a uma implantação, será possível atualizar a conexão para usar a autenticação baseada em chave.

Por padrão, o Ansible usa SSH para se conectar às máquinas físicas. Se estiver usando máquinas Windows conforme especificado no modelo de nuvem com a propriedade `osType Windows`, a variável `connection_type` será automaticamente definida como `winrm`.

Inicialmente, a integração do Ansible usa as credenciais de usuário/senha ou usuário/chave fornecidas na integração para se conectar à máquina de controle do Ansible. Assim que a conexão for bem-sucedida, os playbooks fornecidos no modelo de nuvem serão validados quanto à sintaxe.

Se a validação for bem-sucedida, uma pasta de execução será criada na máquina de controle do Ansible em `~/var/tmp/vmware/provider/user_defined_script/`. Esse é o local de onde os scripts são executados para adicionar o host ao inventário, criar os arquivos VARs do host, incluindo a configuração do modo de autenticação para se conectar ao host e, por fim, executar os guias estratégicos. Nesse ponto, as credenciais fornecidas no modelo de nuvem são usadas para conexão com o host a partir da Máquina de controle Ansible.

A integração com o Ansible oferece suporte a máquinas físicas que não usam um endereço IP. Para máquinas provisionadas em nuvens públicas, como a AWS, o Azure e a GCP, a propriedade de endereço no recurso criado é preenchida com o endereço IP público da máquina somente quando a máquina está conectada a uma rede pública. Para máquinas não conectadas a uma rede pública, a integração do Ansible procura o endereço IP da rede conectada à máquina. Se houver várias redes conectadas, a integração do Ansible procurará a rede com o menor valor de `deviceIndex`; ou seja, o índice da Placa de interface de rede (NIC) conectada à máquina. Se a propriedade `deviceIndex` não estiver especificada no blueprint, a integração usará a primeira rede conectada.

Consulte [O que é o gerenciamento de configuração no Cloud Assembly](#) para obter mais detalhes sobre como configurar o Ansible Open Source para integração no Cloud Assembly.

Pré-requisitos

- A máquina de controle Ansible deve usar uma versão do Ansible. Consulte a [Matriz de Suporte do vRealize Automation](#) para obter informações sobre as versões com suporte.
- O detalhamento do log do Ansible deve ser definido como o padrão de zero.
- O usuário deve ter acesso de leitura/gravação ao diretório onde o arquivo de inventário do Ansible está localizado. Além disso, o usuário deve ter acesso de leitura/gravação ao arquivo de inventário, se ele já existir.
- Se estiver usando um usuário não raiz com a opção `sudo`, certifique-se de que o seguinte esteja definido no arquivo `sudoers`:

```
Defaults:user_name !requiretty
e
username ALL=(ALL) NOPASSWD: ALL
```

- Certifique-se de que a verificação de chaves de host esteja desativada, definindo `host_key_checking = False` em `/etc/ansible/ansible.cfg` ou `~/ansible.cfg`.

- Certifique-se de que a senha do cofre esteja definida, adicionando a seguinte linha ao arquivo `/etc/ansible/ansible.cfg` ou `~/.ansible.cfg`:

```
vault_password_file = /path/to/password_file
```

O arquivo de senha de cofre contém a senha em texto sem formatação e é usado apenas quando os modelos de nuvem ou as implantações fornecem a combinação de nome de usuário e senha a ser usada entre o ACM e o nó, como mostra o exemplo a seguir.

```
echo 'myStr0ng9@88w0rd' > ~/.ansible_vault_password.txt
echo 'ANSIBLE_VAULT_PASSWORD_FILE=~/.ansible_vault_password.txt' > ~/.profile
# Instead of this way, you can also set it setting
'vault_password_file=~/.ansible_vault_password.txt' in either /etc/ansible/ansible.cfg or
~/.ansible.cfg
```

- Para evitar falhas de chaves de host ao tentar executar os playbooks, é recomendável incluir as seguintes configurações em `/etc/ansible/ansible config`.

```
[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null # If you already have any
options set for ssh_args, just add the additional option shown here at the end.
```

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Clique no Ansible.
A página de configuração do Ansible é exibida.
- 3 Digite o nome do host, o caminho do arquivo de inventário e outras informações necessárias para a instância do Ansible Open Source.
- 4 Clique em **Validar** para verificar a integração.
- 5 Clique em **Adicionar**.

Resultados

O Ansible está disponível para uso com modelos de nuvem.

Próximo passo

Adicione componentes do Ansible aos modelos de nuvem desejados.

- 1 Na página da tela do modelo de nuvem, selecione Ansible sob o título Gerenciamento da Configuração no menu de opções do modelo de nuvem e arraste o componente Ansible até a tela.

- 2 Use o painel à direita para configurar as propriedades apropriadas do Ansible, como especificar os guias estratégicos a serem executados.

No Ansible, os usuários podem atribuir uma variável a um único host e, em seguida, usá-la mais tarde em playbooks. A integração com o Ansible Open Source permite que você especifique essas variáveis de host em modelos de nuvem. A propriedade `hostVariables` deve estar no formato YAML apropriado, conforme o esperado pela máquina de controle Ansible, e esse conteúdo será colocado no seguinte local:

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

A localização padrão do arquivo de inventário do Ansible é definido na conta do Ansible, conforme adicionado na página Integrações do Cloud Assembly. A integração com o Ansible não validará a sintaxe YAML de `hostVariable` no modelo de nuvem, mas a máquina de controle do Ansible lançará um erro quando você executar um playbook no caso de uma sintaxe ou um formato incorreto.

O seguinte snippet YAML de modelo de nuvem mostra um exemplo de uso da propriedade `hostVariables`.

```
Cloud_Ansible_1:
  type: Cloud.Ansible
  properties:
    host: '${resource.AnsibleLinuxVM.*}'
    osType: linux
    account: ansible-CAVA
    username: ${input.username}
    password: ${input.password}
    maxConnectionRetries: 20
    groups:
      - linux_vms
    playbooks:
      provision:
        - /root/ansible-playbooks/install_web_server.yml
    hostVariables: |
      message: Hello ${env.requestedBy}
      project: ${env.projectName}
```

Integrações Ansible esperam que as credenciais de autenticação estejam presentes em um modelo de nuvem de uma das seguintes maneiras:

- Nome de usuário e senha no recurso do Ansible.
- Nome de usuário e `privateKeyFile` no recurso do Ansible.
- Nome de usuário no recurso do Ansible e chave privada no recurso de processamento, especificando `remoteAccess` para `generatedPublicPrivateKey`.

Ao criar uma integração com o Ansible Open Source, você deve fornecer informações de login para o usuário de integração se conectar à máquina de controle Ansible usando SSH. Para executar manuais com uma integração, você pode especificar um usuário diferente no código YAML da integração. A propriedade `username` é obrigatória e necessária para a conexão com a máquina virtual na qual o Ansible fará alterações. A propriedade `playbookRunUsername` é opcional e pode ser fornecida para executar o playbook no nó do Ansible. O valor padrão de `playbookRunUsername` é o nome de usuário da integração de endpoint do Ansible.

Se você especificar um usuário diferente, esse usuário deverá ter acesso de gravação ao arquivo de hosts Ansible e deverá ter permissão para criar arquivos de chave privada.

Quando você adiciona um bloco Ansible Open Source a um modelo de nuvem, o vRealize Automation cria a entrada de host para a máquina virtual conectada. Por padrão, o vRealize Automation usará o nome do recurso da máquina virtual para criar a entrada do host, mas pode especificar qualquer nome usando a propriedade `hostName` no YAML do blueprint. Para se comunicar com a máquina, o vRealize Automation criará a variável de host `ansible_host: IP Address` para a entrada do host. Você pode substituir o comportamento padrão para configurar a comunicação usando FQDN, especificando a palavra-chave `ansible_host` sob `hostVariables` e fornecendo o FQDN como seu valor. O seguinte snippet de código YAML mostra um exemplo de como o nome do host e a comunicação FQDN podem ser configurados:

```
Cloud_Ansible:
  type: Cloud Ansible
  properties:
    osType: linux
    username: ubuntu
  groups:
    - sample
  hostName: resource name
  host: name of host
  account: name of account
  hostVariables:
    ansible_host:Host FQDN
```

Neste exemplo, você substitui o valor `ansible_host` padrão fornecendo o FQDN. Isso pode ser útil para usuários que desejam que o Ansible Open Source se conecte à máquina host usando o FQDN.

O valor padrão de `hostVariables` no YAML será `ansible_host:IP_address`, e o endereço IP é usado para comunicação com o servidor.

Se a propriedade “count” YAML for maior que 1 para o Ansible Open Source, o nome do host poderá ser mapeado para qualquer uma das propriedades da respectiva máquina virtual. O exemplo a seguir mostra o mapeamento de um recurso de máquina virtual chamado Ubuntu-VM quando queremos que sua propriedade “address” seja mapeada para o nome do host.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Em modelos de nuvem, certifique-se de que o caminho para o playbook Ansible esteja acessível ao usuário especificado na conta de integração. Você pode usar um caminho absoluto para especificar a localização do manual, mas isso não é necessário. Um caminho absoluto para a pasta pessoal do usuário é recomendado para que o caminho permaneça válido mesmo se as credenciais de integração do Ansible mudarem com o tempo.

Configurar a integração com o Ansible Tower no Cloud Assembly

Você pode integrar o Ansible Tower com o Cloud Assembly para oferecer suporte ao gerenciamento da configuração de recursos implantados. Depois de configurar a integração, será possível adicionar componentes virtuais do Ansible Tower a implantações novas ou existentes a partir do editor de modelo de nuvem.

Pré-requisitos

- Conceda aos usuários não administradores as permissões apropriadas para acessar o Ansible Tower. Há duas opções que funcionam para a maioria das configurações. Escolha uma que seja a mais apropriada para a sua configuração.
 - Conceda aos usuários as funções Administrador de Inventário e Administrador de Modelos de Trabalho no nível da organização.
 - Conceda aos usuários permissão de Administrador para um inventário específico e a função Executar para todos os modelos de trabalho usados para provisionamento.
- Você deve configurar as credenciais e os modelos apropriados no Ansible Tower para uso com as suas implantações. Modelos podem ser modelos de trabalho ou modelos de fluxo de trabalho. Modelos de trabalho definem o inventário e o playbook para uso com uma implantação. Há um mapeamento de 1:1 entre um modelo de trabalho e um playbook. Playbooks usam uma sintaxe semelhante à do YAML para definir tarefas que estão associadas ao modelo. Para a maioria das implantações típicas, use credenciais de máquina para autenticação.

Modelos de fluxo de trabalho permitem que os usuários criem sequências que consistem em qualquer combinação de modelos de trabalho, sincronizações de projeto e sincronizações de inventário vinculadas, para que você possa executá-las como uma única unidade. O Ansible Tower Workflow Visualizer ajuda os usuários a criar modelos de fluxo de trabalho. Para a maioria das implantações típicas, você pode usar credenciais de máquina para autenticação.

- a Faça login no Ansible Tower e navegue até a seção Modelos.
- b Selecione a opção para adicionar um novo modelo de trabalho.
 - Selecione as credenciais que você já criou. Estas são as credenciais da máquina a ser gerenciada pelo Ansible Tower. Para cada modelo de trabalho, pode haver um objeto de credencial.

- Para a seleção do limite, selecione a opção para avisar ao iniciar. Isso garante que o modelo de trabalho seja executado em relação ao nó que está sendo provisionado ou desprovisionado no Cloud Assembly. Se essa opção não for selecionada, um erro de limite não definido será exibido quando o blueprint que contém o modelo de trabalho for implantado.
- c Selecione Adicionando um novo modelo de fluxo de trabalho.
 - Selecione as credenciais que você já criou e defina o inventário. Usando o Workflow Visualizer, projete o modelo de fluxo de trabalho.

Para a caixa Limite de modelos de fluxo de trabalho ou trabalho, geralmente você pode selecionar Avisar ao Iniciar. Essa seleção garante que o modelo de trabalho ou fluxo de trabalho seja executado no nó que está sendo provisionado ou desprovisionado do Cloud Assembly.

- Você pode visualizar a execução dos modelos de trabalho ou fluxo de trabalho chamados do Cloud Assembly na guia Trabalhos do Ansible Tower.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Clique em Ansible Tower.
A página de configuração do Ansible é exibida.
- 3 Insira o **Nome do Host**, que pode ser um endereço IP, e outras informações necessárias para a instância do Ansible Tower.
- 4 Insira o **Nome de Usuário** e a **Senha** de autenticação com base em interface do usuário para a instância aplicável do Ansible Tower.
- 5 Clique em **Validar** para verificar a integração.
- 6 Digite um **Nome** e uma **Descrição** apropriados para a integração.
- 7 Clique em **Adicionar**.

Resultados

O Ansible Tower está disponível para uso em modelos de nuvem.

Próximo passo

Adicione componentes do Ansible Tower aos modelos de nuvem desejados. Você deve especificar o modelo de trabalho aplicável com permissão de execução para o usuário especificado na conta de integração.

- 1 Na página da tela do modelo de nuvem, selecione Ansible sob o título Gerenciamento de Configuração no menu de opções do blueprint e arraste o componente Ansible Tower até a tela.
- 2 Use o painel à direita para configurar as propriedades apropriadas do Ansible Tower, como modelos de trabalho.

Quando você adiciona um bloco Ansible Tower a um modelo de nuvem, o vRealize Automation cria a entrada de host para a máquina virtual conectada no Ansible Tower. Por padrão, o vRealize Automation usará o nome do recurso da máquina virtual para criar a entrada do host, mas pode especificar qualquer nome usando a propriedade `hostName` no YAML do blueprint. Para se comunicar com a máquina, o vRealize Automation criará a variável de host `ansible_host: IP Address` para a entrada do host. Você pode substituir o comportamento padrão para configurar a comunicação usando FQDN, especificando a palavra-chave `ansible_host` sob `hostVariables` e fornecendo o FQDN como seu valor. O seguinte snippet de código YAML mostra um exemplo de como o nome do host e a comunicação FQDN podem ser configurados:

```
Cloud_Ansible_Tower_1:
  type: Cloud Ansible Tower
  properties:
    host: name of host
    account: name of account
    hostName: resource name
    hostVariables:
      ansible_host: Host FQDN
```

Neste exemplo, você substitui o valor `ansible_host` padrão fornecendo o FQDN. Isso pode ser útil para usuários que desejam que o Ansible Tower se conecte à máquina host usando o FQDN.

O valor padrão de `hostVariables` no YAML será `ansible_host:IP_address`, e o endereço IP é usado para comunicação com o servidor.

Se a propriedade “count” YAML for maior que 1 para o Ansible Tower, o nome do host poderá ser mapeado para qualquer uma das propriedades da respectiva máquina virtual. O exemplo a seguir mostra o mapeamento de um recurso de máquina virtual chamado Ubuntu-VM quando queremos que sua propriedade “address” seja mapeada para o nome do host.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Ao adicionar um componente Ansible Tower a um modelo de nuvem, você pode especificar o modelo de trabalho para chamar no YAML do modelo de nuvem. Você também pode especificar modelos de fluxo de trabalho ou uma combinação de modelos de trabalho e modelos de fluxo de trabalho. Se o tipo de modelo não for especificado, por padrão, o vRealize Automation assumirá que você está chamando um modelo de trabalho.

O seguinte snippet YAML mostra um exemplo de como uma combinação de modelos de trabalho e fluxo de trabalho pode ser chamada em um modelo de nuvem do Ansible Tower.

```
Cloud_Ansible_1:
  type: Cloud.Ansible.Tower
  properties:
    host: '${resource.CentOS_Machine.*}'
    account:
    maxConnectionRetries: 2
    maxJobRetries: 2
    templates:
```

```
provision:
  - name: My workflow
    type: workflow
  - name: My job template
```

Adicionamos o `maxConnectionsRetries` e o `maxJobRetries` para lidar com falhas relacionadas ao Ansible. Os modelos de nuvem aceitam o valor personalizado e, caso nenhum valor seja fornecido, o valor padrão será usado. Para o `maxConnectionRetries`, o valor padrão é 10 e, para o `maxJobRetries`, o valor padrão é 3.

Observação Versões anteriores do vRealize Automation ofereciam suporte à execução de modelos de trabalho apenas usando o esquema `jobTemplate` no modelo de nuvem. Agora, `jobTemplate` está obsoleto e talvez seja removido em releases futuros. Por enquanto, o uso da propriedade `jobTemplate` continuará funcionando conforme esperado. Para executar modelos de fluxo de trabalho e usar recursos adicionais, é recomendável usar o esquema de modelos.

Modelos de nuvem do Cloud Assembly para integrações com o Ansible Tower incluem a propriedade `useDefaultLimit` com um valor `true` ou `false` para definir onde os modelos do Ansible são executados. Os modelos do Ansible podem ser modelos de trabalho ou modelos de fluxo de trabalho. Se esse valor for definido como `true`, os modelos especificados serão executados na máquina especificada na caixa Limite da página Modelos Ansible. Se o valor for definido como `false`, os modelos serão executados na máquina provisionada, mas os usuários deverão marcar a caixa de seleção Avisar ao Iniciar na página Modelos do Ansible Tower. Por padrão, o valor dessa propriedade é `false`. O exemplo YAML a seguir mostra como a propriedade `useDefaultLimit` aparece em modelos de nuvem.

```
templates:
  provision:
    - name: ping aws_credentials
      type: job
      useDefaultLimit: false
      extraVars: '{"rubiconSurveyJob" : "checkSurvey"}'
```

Além disso, como mostra o exemplo anterior, você pode usar a propriedade `extraVars` para especificar variáveis extras ou variáveis de pesquisa. Esse recurso pode ser útil para executar modelos que requerem entrada. Se um usuário manteve a variável de pesquisa, você deve transmitir essa variável na seção `extraVars` do modelo de nuvem para evitar erros.

Criar uma integração com o SaltStack Config no vRealize Automation

É possível criar uma integração com o SaltStack Config para acessar o serviço do SaltStack Config e usar objetos e ações do SaltStack Config no vRealize Automation.

Com o vRealize Automation SaltStack Config, você pode provisionar, configurar e implantar software para suas máquinas virtuais em qualquer escala usando a automação controlada por eventos. Você também pode usar o SaltStack Config para definir e aplicar estados de software ideais e compatíveis por todo o seu ambiente.

Instalação

Antes de integrar o SaltStack Config ao vRealize Automation, você deve instalá-lo no seu ambiente. Consulte [Instalando e configurando o SaltStack Config](#) para obter mais informações.

Considerações

O vRealize Automation SaltStack Config integrado está disponível para vRealize Automation com as seguintes condições:

- A integração do SaltStack Config está associada a um host específico durante a instalação.
- No momento, o vRealize Automation não oferece suporte à multilocação para o SaltStack Config.
- O tenant do vRealize Automation pode suportar uma integração do SaltStack Config e um mestre Salt. O mestre do Salt pode suportar vários subordinados.
- Antes de poder excluir uma integração do SaltStack Config no vRealize Automation, você deve excluir todas as implantações existentes que usam a integração do SaltStack Config.

Pré-requisitos

- Verifique se você tem credenciais de administrador do vRealize Automation e credenciais de administrador do SaltStack Config (acesso no nível raiz).

Você precisa de credenciais de administrador do vRealize Automation e credenciais de administrador do SaltStack Config (acesso no nível raiz) para criar uma integração do SaltStack Config.

Você também precisa de credenciais de administrador do SaltStack Config para abrir e trabalhar no serviço do SaltStack Config em si.

Você usa credenciais do vRealize Automation para acessar credenciais do vRealize Automation e SaltStack Config para acessar credenciais do SaltStack Config.

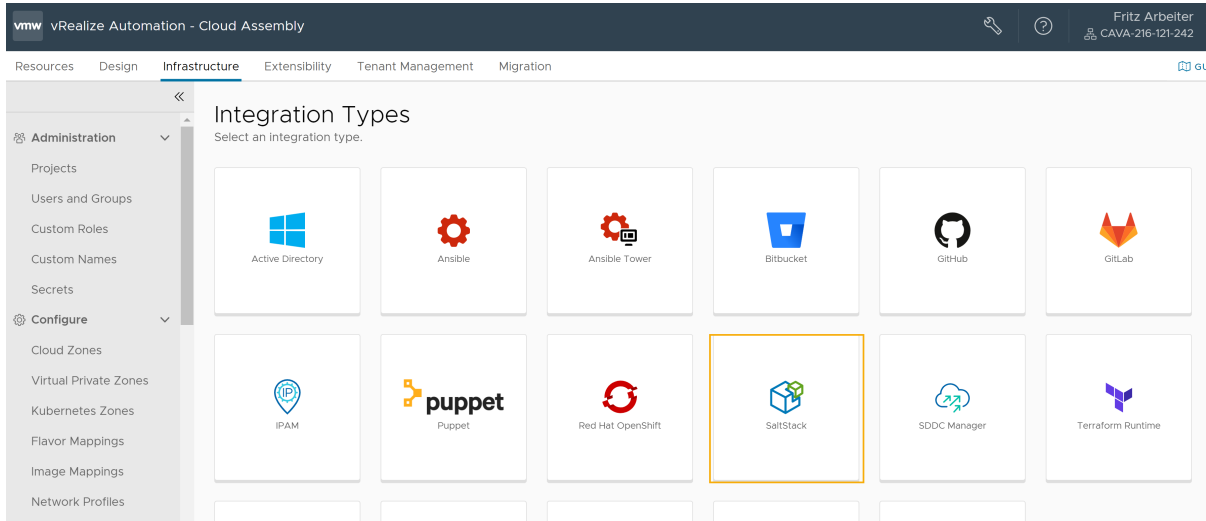
Para obter informações sobre credenciais de administrador do SaltStack Config, consulte o guia [Instalando e configurando o SaltStack Config](#).

- Verifique se o serviço do SaltStack Config foi instalado.
- Verifique se o mestre Salt a ser usado na integração do SaltStack Config contém o Plug-in Mestre.
- Verifique se você tem a função de administrador do serviço do SaltStack Config em vRealize Automation. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem a função de administrador do serviço do Cloud Assembly no vRealize Automation. Consulte [Funções de usuário de serviço e organização no vRealize Automation](#).

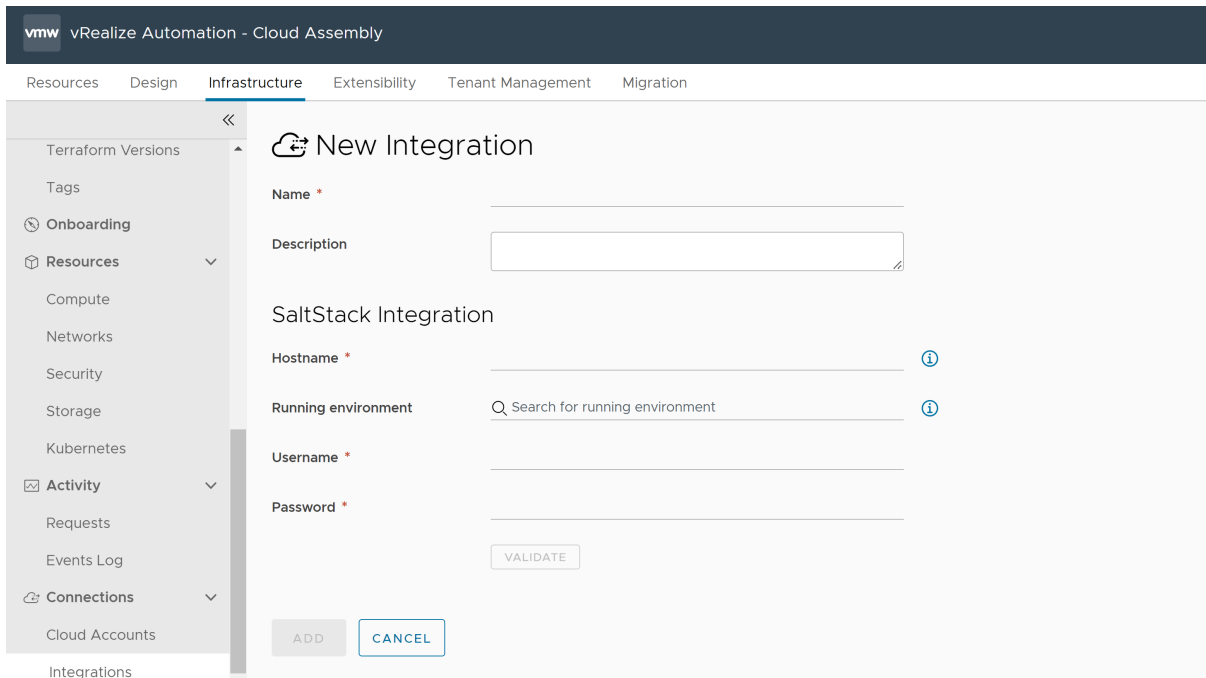
Configurar uma integração do SaltStack Config no vRealize Automation

Depois de instalar o SaltStack Config para vRealize Automation, você poderá configurar a integração no Cloud Assembly.

- 1 No Cloud Assembly, selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione o tipo de integração SaltStack Config.



- 3 Preencha o formulário.



- a Insira um nome para a integração.
- b (Opcional) Forneça uma descrição para a integração.

- c Insira o nome do host para o servidor do SaltStack Config.
- d Especifique o ambiente de execução para a integração do SaltStack Config.

Se você estiver usando a propriedade `saltConfiguration` para implantar subordinados e aplicar arquivos de estado em suas máquinas virtuais, não precisará configurar um ambiente de execução. No entanto, é recomendável que você atualize seus modelos de nuvem para usar o recurso SaltStack Config. A propriedade `saltConfiguration` se tornará obsoleta em um lançamento futuro.

Se você estiver usando o recurso SaltStack Config para implantar subordinados e aplicar arquivos de estado às suas máquinas virtuais, selecione o ambiente de execução **embedded-ABX-onprem**.

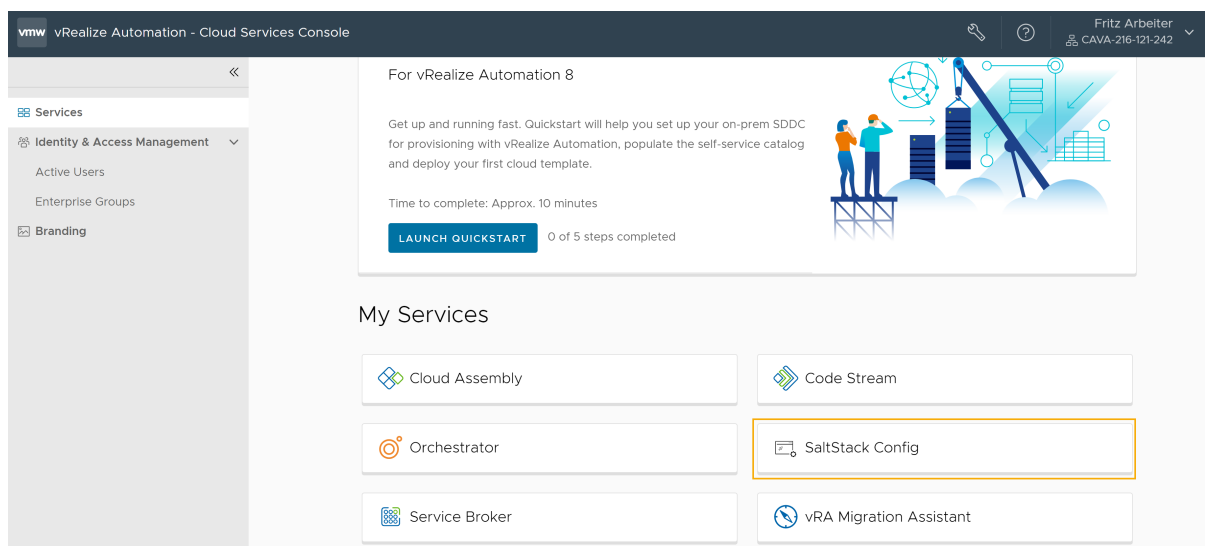
- e Insira o nome e a senha do usuário administrador do SaltStack Config usados para acessar o host especificado.
- f Clique em **Validar** para confirmar o acesso do administrador ao host de integração do SaltStack Config.

Se a validação falhar, certifique-se de inserir o nome do host, o nome de usuário e a senha corretos.
- g Clique em **Salvar**.

Acessar sua integração do SaltStack Config

Depois de salvar o ponto de integração do SaltStack Config, você pode abrir o serviço de integração do SaltStack Config.

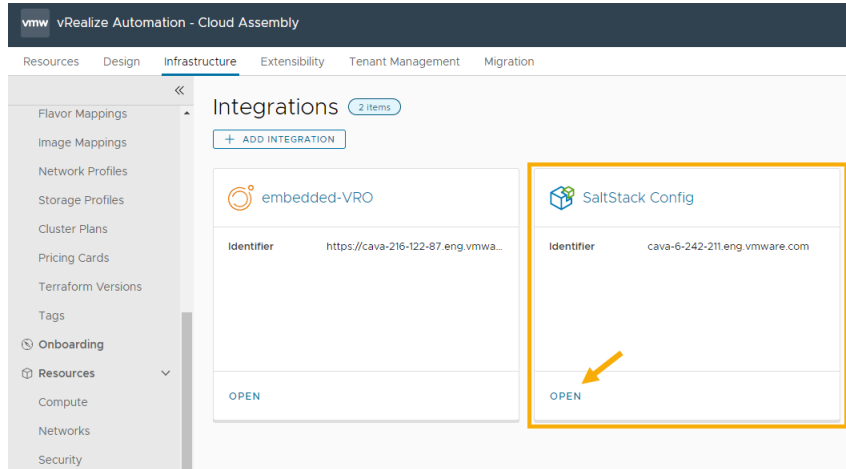
- 1 Se você tiver implantado o SaltStack Config por meio do vRealize Suite Lifecycle Manager, poderá clicar no bloco de serviço no Console de Serviço do vRealize Automation para abrir a integração e acessar o host.



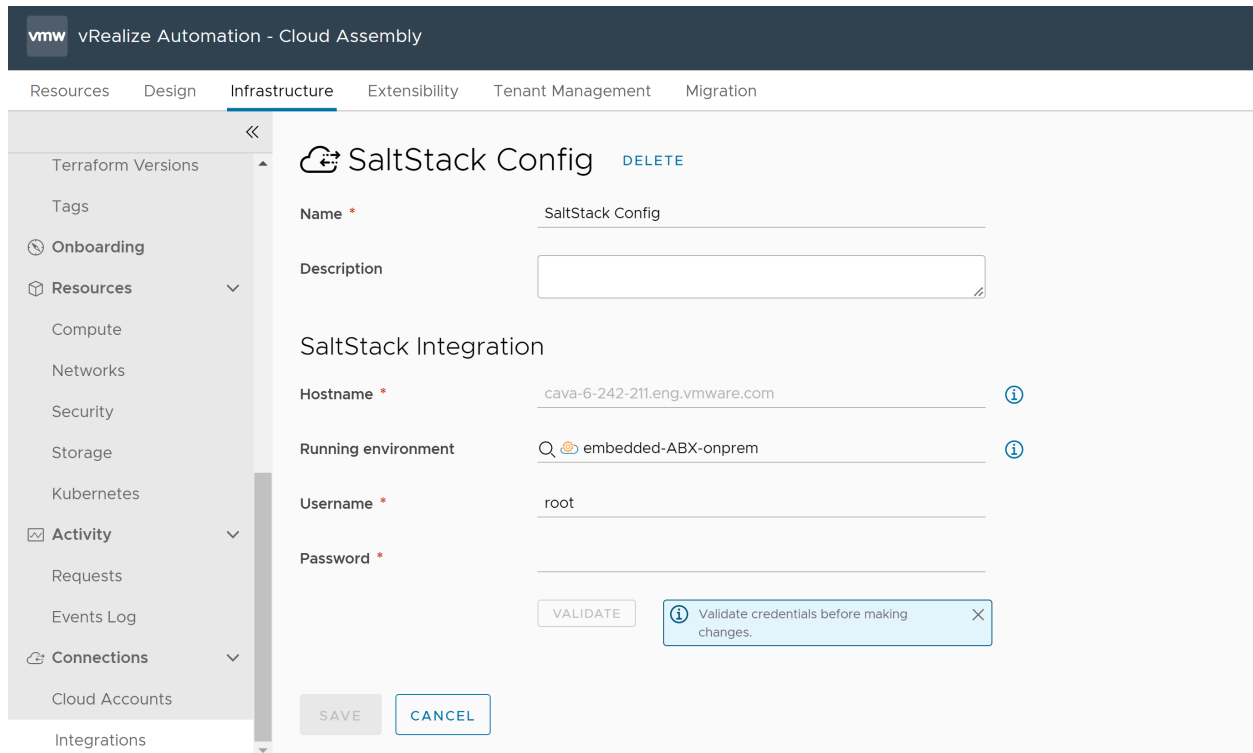
Se você fez uma instalação autônoma do SaltStack Config, poderá acessar o serviço usando o nome do host do SaltStack Config.

- Quando solicitado a fazer login no SaltStack Config, insira seu nome e senha de usuário administrador do SaltStack Config.

Se precisar fazer alterações na integração, selecione **Infraestrutura > Conexões > Integrações**, selecione o bloco de integração com o SaltStack Config disponível e clique em **Abrir**.



O nome do host não pode ser alterado após a configuração da integração. Você pode editar apenas o nome, a descrição, o ambiente de execução e as credenciais da integração.



Saiba como usar o SaltStack Config

SaltStack Config é um produto autônomo que você pode integrar e usar no vRealize Automation.

- Saiba como adicionar o [recurso SaltStack Config](#) para instalar subordinados em máquinas virtuais nas suas implantações do Cloud Assembly.
- Saiba como [implantar subordinados usando a API \(RaaS\)](#) em um ambiente Linux ou Windows.

Como criar uma integração do Active Directory no Cloud Assembly

O Cloud Assembly oferece suporte para a integração com servidores Active Directory, para permitir a criação imediata de contas de computador em uma unidade organizacional (OU) especificada em um servidor Active Directory antes do provisionamento de uma máquina virtual. O Active Directory oferece suporte a uma conexão LDAP com o servidor Active Directory.

Uma política do Active Directory associada a um projeto é aplicada a todas as máquinas virtuais provisionadas dentro do escopo desse projeto. Os usuários podem especificar uma ou mais tags para aplicar seletivamente a política às máquinas virtuais provisionadas para as zonas de nuvem com as tags de capacidade correspondentes.

Para implantações locais, a integração do Active Directory permite configurar um recurso de verificação de integridade que mostra o status da integração e a integração do ABX subjacente da qual ela depende, incluindo o proxy de nuvem de extensibilidade necessário. Antes de aplicar uma política do Active Directory, o Cloud Assembly verifica o status das integrações subjacentes. Se a integração estiver íntegra, o Cloud Assembly criará os objetos de computador implantados no Active Directory especificado. Se a integração não estiver íntegra, a operação de implantação ignorará a fase do Active Directory durante o provisionamento.

Pré-requisitos

- A integração do Active Directory requer uma conexão LDAP com o servidor Active Directory.
- Se você estiver configurando uma integração do Active Directory com o vCenter no local, deverá configurar uma integração ABX com um proxy de nuvem de extensibilidade. Selecione **Extensibilidade > Atividade > Integrações** e escolha **Ações de Extensibilidade no Local**.
- Se você estiver configurando uma integração com o Active Directory na nuvem, deverá ter uma conta do Microsoft Azure ou do Amazon Web Services.
- Você deve ter um projeto configurado com zonas de nuvem apropriadas e mapeamentos de imagem e tipos para usar com a integração do Active Directory.
- A OU desejada no seu Active Directory deve ser pré-criada antes de você associar a integração do Active Directory a um projeto.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e depois **Nova Integração**.
- 2 Clique em **Active Directory**.

- 3 Na guia **Resumo**, insira o host LDAP apropriado e os nomes de ambientes.

O host LDAP especificado é usado para validar a integração do Active Directory e também será usado para implantações subsequentes se nenhum host alternativo for especificado e chamado devido a erros ou indisponibilidade.

- 4 Insira o nome e a senha do servidor LDAP.
- 5 Insira o DN Base apropriado que especifica a raiz dos recursos do Active Directory desejados.

Observação É possível especificar apenas um DN por integração do Active Directory.

- 6 Clique em **Validar** para garantir que a integração seja funcional.
- 7 Insira um nome e uma descrição dessa integração.
- 8 Clique em **Salvar**.
- 9 Clique na guia **Projeto** para adicionar um projeto à integração do Active Directory.
Na caixa de diálogo **Adicionar Projetos**, você deve selecionar um nome de projeto e um DN relativo, que é um DN existente no DN base especificado na guia Resumo.
- 10 Na seleção Opções Estendidas, forneça uma lista separada por vírgulas de **Hosts Alternativos** que serão usados se o servidor selecionado inicialmente estiver indisponível durante a implantação. O servidor primário é sempre usado para validação inicial da integração.

Observação Se o formato do host principal for LDAP, o LDAPS não terá suporte para hosts alternativos.

- 11 Insira o tempo em segundos para aguardar até que o servidor inicial responda antes de tentar um servidor alternativo na caixa **Tempo Limite da Conexão**.
- 12 Clique em **Salvar**.

Resultados

Agora, é possível associar o projeto com a integração do Active Directory a um modelo de nuvem. Quando uma máquina é provisionada usando esse modelo de nuvem, ela é previamente preparada no Active Directory e na unidade organizacional especificados.

Inicialmente, as integrações do Active Directory são implantadas em uma UO padrão com poucas restrições de usuário. A UO é definida por padrão quando você mapeia uma integração do Active Directory para um projeto. Você pode adicionar uma propriedade chamada `FinalRelativeDN` a blueprints para alterar a UO de implantações do Active Directory. Essa propriedade permite que você especifique a UO a ser usada com uma implantação do Active Directory.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: CenOS8
```

```
flavor: tiny
activeDirectory:
  finalRelativeDN: ou=test
  securityGroup: TestSecurityGroup
```

Conforme mostrado no exemplo de YAML anterior, os usuários podem adicionar uma propriedade a uma implantação de integração do Active Directory que adiciona uma conta de computador ao grupo de segurança, para que sejam atribuídas as permissões apropriadas para acessar o recurso compartilhado em uma rede. A máquina virtual do Active Directory é inicialmente implantada em uma UO fixa. Porém, quando a máquina estiver pronta para ser liberada, ela será movida para uma UO diferente com a política apropriada, conforme aplicável aos usuários.

Se uma conta de computador for movida para uma UO diferente após a implantação, o Cloud Assembly tentará excluir as contas na UO inicial. A exclusão de contas de computador apenas será bem-sucedida no caso de máquinas virtuais movidas para uma UO diferente no mesmo domínio.

Você também pode implementar uma verificação de integridade com base em tags para integrações do Active Directory locais, da seguinte maneira.

- 1 Crie uma integração do Active Directory conforme descrito nas etapas anteriores.
- 2 Clique na guia **Projeto** para adicionar um projeto à integração do Active Directory.
- 3 Selecione um nome de projeto e um DN relativo na caixa de diálogo Adicionar Projetos. O DN relativo deve existir no DN base especificado.

Há dois comutadores nesta caixa de diálogo que permitem que você controle a configuração do Active Directory dos modelos de nuvem. Ambos os comutadores estão desligados por padrão.

- **Substituir** – Esse comutador permite que você substitua as propriedades do Active Directory, especificamente o DN relativo nos modelos de nuvem. Quando ligado, você pode alterar a UO especificada na propriedade `relativeDN` no modelo de nuvem. Quando provisionada, a máquina será adicionada à UO especificada na propriedade `relativeDN` no modelo de nuvem. O exemplo a seguir mostra a hierarquia de modelo de nuvem na qual essa propriedade aparece.

```
activeDirectory:
  relativeDN: OU=ad_integration_machine_override
```

- **Ignorar** - Esse comutador permite ignorar a configuração do Active Directory para o projeto. Quando ligado, adiciona uma propriedade ao modelo de nuvem chamada `ignoreActiveDirectory` à máquina virtual associada. Quando essa propriedade é definida como verdadeira, significa que a máquina não é adicionada ao Active Directory quando implantada.
- 4 Adicione as tags apropriadas. Essas tags são aplicáveis à zona de nuvem à qual a política do Active Directory pode ser aplicada.
 - 5 Clique em Salvar.

O status da integração do Active Directory é exibido para cada integração na página **Infraestrutura > Conexões > Integrações** no Cloud Assembly.

É possível associar o projeto à integração do Active Directory com um modelo de nuvem. Quando uma máquina for provisionada usando esse modelo, ela será pré-configurada no Active Directory e UO especificados.

Configurar uma integração do VMware SDDC Manager

Você pode adicionar uma integração do VMware SDDC Manager com o vRealize Automation para facilitar o uso de domínios de carga de trabalho como parte de contas de nuvem do VMware Cloud Foundation (VCF) no vRealize Automation.

Pré-requisitos

- O vRealize Automation oferece suporte para integração apenas com o VMware SDDC Manager 4.1 e versões mais recentes.

Procedimentos

- 1 Selecione **Infraestrutura > Conexões > Integrações** e clique em **Adicionar Integração**.
- 2 Selecione SDDC Manager.
A página de configuração da integração com o SDDC Manager é exibida.
- 3 Na seção Resumo, insira um **Nome** e uma **Descrição** para a integração.
- 4 Na seção Credenciais do SDDC Manager, insira o **Endereço IP/FQDN do SDDC Mgr** para a máquina do servidor SDDC Manager.
- 5 Insira o Nome de Usuário e a Senha da conta de administrador a ser usada para a conexão inicial com o SDDC Manager. Como prática recomendada, evite usar a conta de administrador para se conectar. Use uma conta diferente que tenha privilégios de administrador no SDDC Manager para criar funções de serviço.

Essas credenciais são usadas para configurar inicialmente a conexão com o SDDC Manager e, em seguida, são criadas credenciais de serviço para uso na conexão a partir de uma conta de nuvem do VCF.
- 6 Clique em **Validar** para verificar a conexão com o SDDC Manager.
- 7 Clique em **Adicionar**.

Resultados

Após a criação da integração, você poderá visualizar as cargas de trabalho associadas ao SDDC na guia Domínio de carga de trabalho que aparece na página de integração concluída. Além disso, você pode visualizar e selecionar cargas de trabalho associadas à integração e, em seguida, clicar no botão **Adicionar Conta de Nuvem** para abrir uma página para a criação de uma conta de nuvem do VCF que usará a carga de trabalho selecionada.

Próximo passo

Depois de configurar a conta de nuvem do VCF, um botão **Configuração de Nuvem** aparecerá no topo da página. Clique nesse botão para iniciar o assistente de instalação de nuvem do VCF.

Integrando com o vRealize Operations Manager

O vRealize Automation pode trabalhar com vRealize Operations Manager para realizar o posicionamento avançado de cargas de trabalho, fornecer métricas de integridade de implantação e máquinas virtuais e exibir preços.

Número e tipo de integrações

A integração entre os dois produtos deve ser de local para local, não é uma combinação entre local e nuvem.

Você pode integrar uma instância do vRealize Automation com várias instâncias do vRealize Operations Manager, mas uma instância do vRealize Operations Manager só pode ser conectada a uma instância do vRealize Automation.

Não é possível conectar um cluster agregado do vRealize Operations Manager ao vRealize Automation.

Requisitos básicos para a integração

Para fazer a integração com o vRealize Operations Manager, acesse **Infraestrutura > Conexões > Integrações**. Para adicionar a integração, você precisa da URL do vRealize Operations Manager e das credenciais para a conta de login descrita na próxima seção. Além disso, o vRealize Automation e o vRealize Operations Manager precisam gerenciar o mesmo endpoint do vSphere.

Conta de login para integração

Além do vRealize Operations Manager, você precisa de uma conta de login local ou não local do vRealize Operations Manager para a integração usar. Essa conta requer privilégios somente leitura à instância de adaptador do vCenter para o endpoint do vSphere. Observe que uma conta não local talvez precise ser importada no vRealize Operations Manager e ter sua função somente leitura atribuída. Para a integração, o formato de nome de usuário para o login de conta não local é *nomeusuário@domínio@origem-autenticada*, como *jdoe@company.com@workspaceone*. As fontes autenticadas são definidas durante a configuração inicial do servidor do vRealize Operations Manager.

Consulte as seções a seguir para obter detalhes. Para obter informações sobre preços, consulte [Como usar cartões de preços no vRealize Automation](#).

Posicionamento avançado de cargas de trabalho usando o vRealize Operations Manager

O vRealize Automation e o vRealize Operations Manager podem trabalhar em conjunto para o posicionamento ideal de cargas de trabalho de implantação.

Você habilita o posicionamento de cargas de trabalho no nível da zona de nuvem com base no vSphere. Somente os clusters habilitados para o Distributed Resource Scheduler (DRS) de uma zona de nuvem estão qualificados para posicionamento avançado usando o vRealize Operations Manager.

- **vRealize Automation posicionamento** – O mecanismo de posicionamento do vRealize Automation é baseado na intenção do aplicativo. Ele considera restrições baseadas em tags, associação a projeto e as zonas de nuvem associadas, bem como os filtros de afinidade relacionados à rede, ao armazenamento e ao processamento. O posicionamento de recursos depende de todos esses fatores e também da presença de outros recursos de destino relacionados na mesma implantação.
- **vRealize Operations Manager posicionamento** – O vRealize Operations Manager considera a intenção operacional para o posicionamento ideal. A intenção operacional pode levar em consideração as cargas de trabalho passadas e as previsões futuras e hipotéticas.

Ao usar o posicionamento da carga de trabalho avançado, você deve aplicar a marcação vRealize Automation para implementar decisões de intenção de negócios, em vez de usar as opções de intenção de negócios do vRealize Operations Manager.

Ao integrar-se com o vRealize Operations Manager, o vRealize Automation continuará a seguir seu modelo de intenção de aplicativo e suas restrições relacionadas para filtrar em busca do posicionamento de destino. Em seguida, nesses resultados, ele usa a recomendação do vRealize Operations Manager para refinar o posicionamento.

Na ausência de uma recomendação

Se você habilitar o posicionamento avançado de cargas de trabalho e a análise do vRealize Operations Manager não retornar recomendações, será possível configurar o vRealize Automation para fazer fallback para o posicionamento de intenção de aplicativo padrão.

Limitações sobre o posicionamento de cargas de trabalho

Determinadas limitações são aplicáveis ao usar o vRealize Operations Manager para posicionar cargas de trabalho.

- O vRealize Operations Manager não oferece suporte ao posicionamento de cargas de trabalho em pools de recursos no vCenter Server.
- Se o vRealize Operations Manager estiver inativo, o tempo limite usado para o posicionamento de cargas de trabalho para chamar o vRealize Operations Manager poderá expirar.
- O posicionamento não atravessa várias zonas de nuvem. O vRealize Automation envia uma zona de nuvem ao vRealize Operations Manager recomendações de posicionamento nessa única zona de nuvem.

Como habilitar o posicionamento de cargas de trabalho

Para habilitar o posicionamento da carga de trabalho, há etapas a serem tomadas para o vSphere, o vRealize Operations Manager e o vRealize Automation.

- 1 No Cloud Assembly, conecte-se à sua conta de nuvem do vCenter Server.

As opções estão em **Infraestrutura > Conexões > Contas de Nuvem**.

- 2 No vCenter Server, verifique se existem clusters habilitados para DRS e se eles estão definidos como totalmente automatizados.
- 3 No vRealize Operations Manager, verifique se o mesmo vCenter Server está sendo gerenciado.

Você precisa do vRealize Operations Manager 8 ou posterior.

- 4 No Cloud Assembly, adicione a integração com o vRealize Operations Manager.

As opções estão em **Infraestrutura > Conexões > Integrações**.

Para adicionar a integração, você precisará da URL do nó primário do vRealize Operations Manager abaixo, mais o nome de usuário e a senha de login.

`https://operations-manager-IP-address-or-FQDN/suite-api`

Depois de inserir os valores, clique em VALIDAR.

- 5 Sincronize a integração com o vCenter Server clicando em Sincronizar.
Também sincronize sempre que o Cloud Assembly e o vRealize Operations Manager começarem a gerenciar um novo vCenter Server.

- 6 No Cloud Assembly, crie uma zona de nuvem para a conta do vCenter Server.

As opções estão em **Infraestrutura > Configurar > Zona da Nuvem**.

- 7 Na guia Resumo da zona de nuvem, defina a Política de Colocação como AVANÇADA.
- 8 Na Política de Colocação, selecione se deseja que o vRealize Automation faça fallback para o posicionamento padrão caso o vRealize Operations Manager não retorne recomendações.

Solucionando problemas de posicionamento de cargas de trabalho

Se o vRealize Operations Manager não estiver recomendando os posicionamentos de cargas de trabalho da maneira esperada, revise os detalhes da solicitação de implantação no Cloud Assembly ou vRealize Automation Service Broker.

- 1 Acesse **Infraestrutura > Atividade > Solicitações** e clique na solicitação.
- 2 Em Detalhes da Solicitação, examine as fases de alocação.
Procure os destinos que foram identificados com ou sem sucesso.
- 3 Em Detalhes da Solicitação, no canto superior direito, habilite Modo Dev.
- 4 Siga o caminho da solicitação para localizar blocos de filtros.

5 Clique em um bloco de filtro e revise a seção a seguir.

```
filterName: ComputePlacementPolicyAffinityHostFilter
  v computeLinksBefore
  v computeLinksAfter
  v filteredOutHostsReasons
```

| Entrada | Descrição |
|-------------------------|---|
| computeLinksBefore | Lista de possíveis hosts de posicionamento com base em algoritmos do vRealize Automation. |
| computeLinksAfter | Host de posicionamento selecionado. |
| filteredOutHostsReasons | Mensagens que descrevem por que um host foi selecionado ou rejeitado. Quando o vRealize Operations Manager selecionar o host, a seguinte mensagem será exibida. advance policy filter: Filtered hosts based on recommendation from vROPS. |

Saiba mais sobre o posicionamento da carga de trabalho

Para encontrar a melhor infraestrutura na qual fazer uma implantação, o vRealize Automation toma várias decisões de filtragem. A integração do vRealize Automation com o vRealize Operations Manager pode refinar ainda mais a decisão de posicionamento.

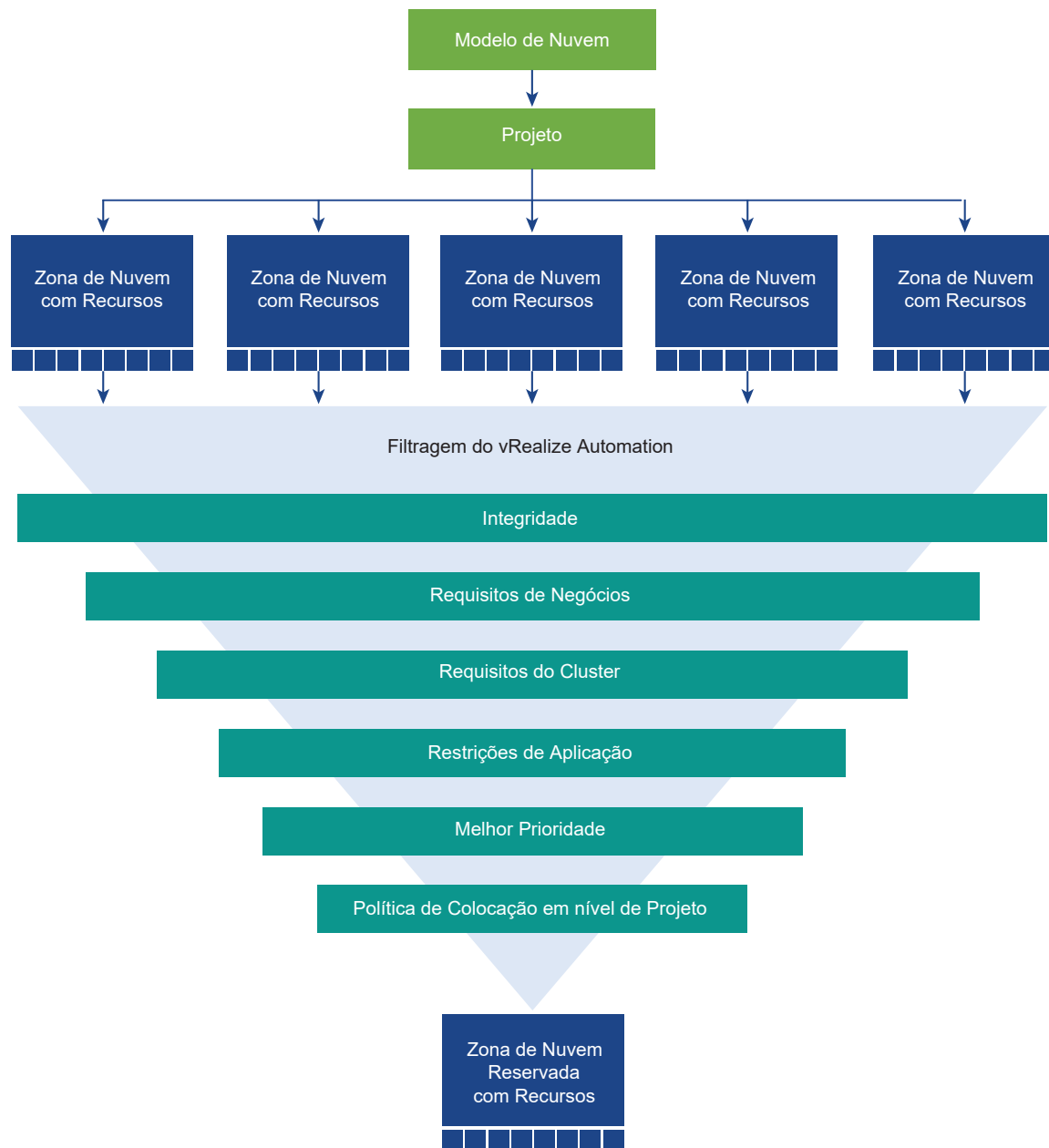
O vRealize Operations Manager pode ajudar a posicionar as cargas de trabalho da maneira ideal, desde que você tenha ativado a opção de política de colocação Avançada em suas zonas de nuvem baseadas no vSphere.

Além disso, as contas de nuvem do vSphere das zonas de nuvem devem ser monitoradas pelo vRealize Operations Manager.

Fase 1: Reserva

Observação Embora o nome seja o mesmo, a reserva não está relacionada ao recurso de reserva do vRealize Automation 7.

A fase de reserva do vRealize Automation é a mesma, sem considerar se você ativou ou não a colocação Avançada no vRealize Operations Manager.



- 1 A reserva começa com um modelo de nuvem vinculado a um projeto. Esse projeto, por sua vez, está vinculado a zonas de nuvem.
- 2 As zonas de nuvem consistem em hosts de recursos de processamento, pools, clusters e armazenamento anexado.
Inicialmente, qualquer zona de nuvem no projeto pode ser um alvo de posicionamento potencial.
- 3 O vRealize Automation faz uma filtragem para remover as zonas de nuvem que não têm recursos íntegros suficientes para a implantação.

Por exemplo, se houver muitos recursos desligados ou em manutenção, essa zona de nuvem será removida.

- 4 O vRealize Automation faz uma filtragem para remover as zonas de nuvem que não atendem aos requisitos de negócios.

Por exemplo, a implantação pode exceder um limite de preço ou orçamento para a zona.

- 5 O vRealize Automation faz uma filtragem para remover as zonas de nuvem que não atendem aos requisitos de cluster.

Por exemplo, os recursos da zona de nuvem podem ter limites de uso de CPU ou memória que são muito baixos para a implantação.

- 6 O vRealize Automation faz uma filtragem para remover as zonas de nuvem que não têm afinidade com as restrições do aplicativo.

A afinidade requer que as tags de restrição no nível do projeto ou do modelo de nuvem correspondam às tags de capacidade encontradas em algum lugar nos recursos da zona de nuvem.

Por exemplo, se o modelo de nuvem ou o projeto incluir uma restrição para usar o armazenamento com a tag `pci`, uma zona de nuvem que não tenha recursos de armazenamento com essa tag de capacidade será removida.

- 7 O vRealize Automation seleciona as zonas de nuvem com a melhor prioridade de provisionamento.

- 8 Se a política de colocação no nível do projeto for diferente de Padrão, o vRealize Automation selecionará uma zona de nuvem que ofereça suporte à política de colocação não padrão.

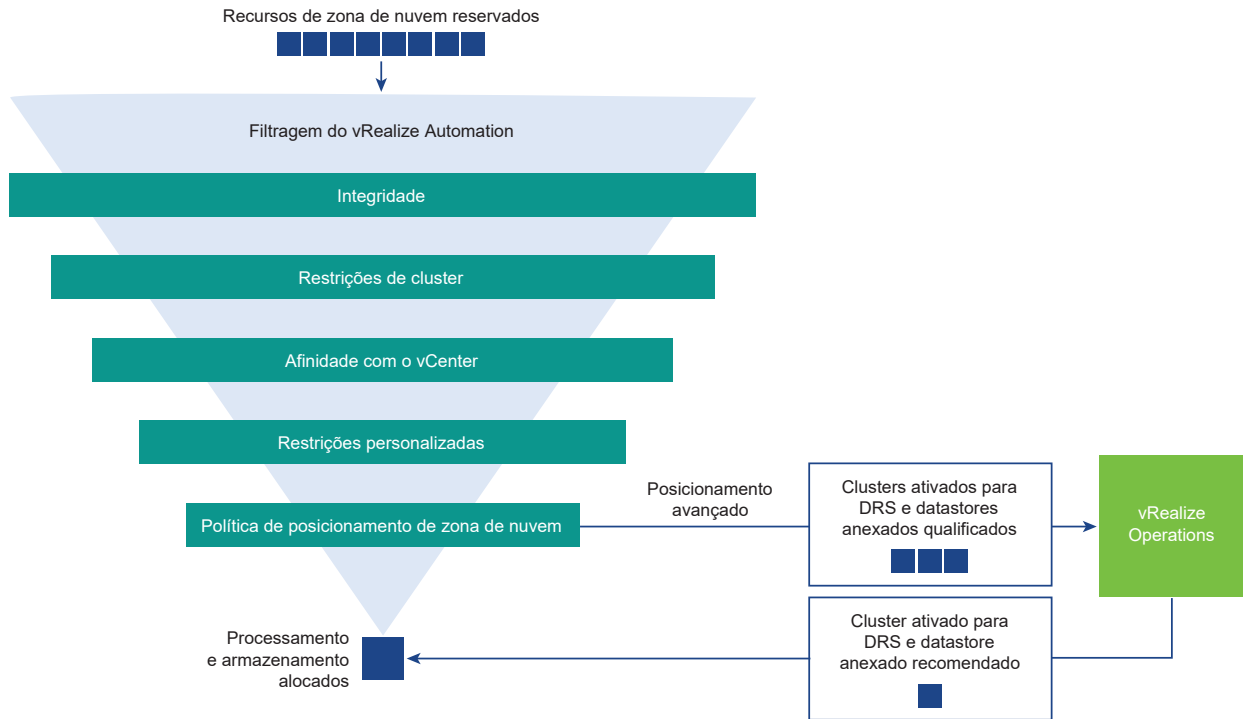
Nesta versão, a Dispersão é a única que não é padrão. A propagação distribui a carga selecionando a zona de nuvem com a proporção mais baixa de máquinas virtuais para hosts. O padrão simplesmente implanta na primeira zona disponível.

A política de posicionamento do projeto é apenas um fator durante a fase de reserva da zona de nuvem. Ela não tem efeito nem relação com a política de colocação da zona de nuvem na fase de alocação.

Quando concluída, a fase de reserva seleciona uma zona de nuvem e seus recursos. O vRealize Automation reserva a primeira zona disponível que ainda está qualificada depois de passar pelos filtros anteriores.

Fase 2: Alocação

O vRealize Automation inspeciona os recursos de processamento reservados da zona de nuvem e o armazenamento vinculado.



- 1 Na zona de nuvem, o vRealize Automation faz uma filtragem para remover os recursos que estão em estado desligado ou de manutenção.

Observe que ainda há recursos íntegros suficientes para a implantação. Caso contrário, toda a zona de nuvem teria sido filtrada durante a fase de reserva.

- 2 O vRealize Automation faz uma filtragem para remover os recursos que não correspondem às restrições no nível do cluster encontradas no modelo de nuvem ou no projeto.

Por exemplo, um recurso na zona de nuvem pode ser marcado como `test` em **Infraestrutura > Recursos > Processamento**.

Se o modelo de nuvem ou o projeto incluir uma tag de restrição para usar um recurso `dev`, o recurso `test` será removido.

Além disso, os perfis de armazenamento ou de rede na zona de nuvem podem ser marcados de maneiras que não correspondem às restrições de rede ou de armazenamento no nível do cluster do modelo de nuvem ou do projeto.

- 3 O vRealize Automation faz uma filtragem para remover os recursos com base nas configurações de afinidade definidas no vCenter.

Por exemplo, pode haver uma regra no vCenter em que a presença de uma máquina virtual em um cluster pode impedir que outro cluster seja usado.

- 4 O vRealize Automation faz uma filtragem para remover os recursos que não correspondem à nenhuma restrição personalizada restante encontrada no modelo de nuvem ou no projeto.

Por exemplo, se o modelo de nuvem incluir uma restrição para usar uma imagem marcada com `ubuntu`, uma zona de nuvem na qual nenhum dos mapeamentos de imagem estiver marcado com `ubuntu` será removida.

- 5 O vRealize Automation procura os melhores processamento e armazenamento possíveis de acordo com a política de colocação da zona de nuvem.

O vRealize Automation envolve o vRealize Operations Manager somente quando as duas condições abaixo são verdadeiras:

- A política de colocação da zona de nuvem está definida como Avançada.
- Após a filtragem da etapa 4, pelo menos um cluster ativado para DRS e o armazenamento vinculado a ele permanecem qualificados.

Caso contrário, o vRealize Automation continuará com seu próprio algoritmo de posicionamento sem entrada do vRealize Operations Manager.

Recomendação de posicionamento do vRealize Operations Manager

Se qualificado para entrada do vRealize Operations Manager, o vRealize Automation contata o vRealize Operations Manager para receber uma recomendação dos melhores processamento e armazenamento possíveis para a implantação. O vRealize Automation envia os seguintes dados para o vRealize Operations Manager:

- Os clusters ativados para DRS de destino qualificados e seus repositórios de dados ou cluster de repositório de dados anexados
- A contagem de recursos ou o tamanho do cluster da implantação
- Requisitos de CPU e memória para as máquinas virtuais na implantação
- Requisitos de disco para as máquinas virtuais na implantação

Nos destinos qualificados, se o vRealize Operations Manager puder retornar um posicionamento ideal para cada uma das máquinas virtuais, o vRealize Automation alocará o processamento e o armazenamento de acordo com a recomendação do vRealize Operations Manager.

Para obter mais informações sobre como o vRealize Operations Manager lida com cargas de trabalho, consulte a [documentação do vRealize Operations](#).

Se o vRealize Operations Manager não conseguiu encontrar uma recomendação ou se o vRealize Automation não conseguiu encontrar nenhum cluster e armazenamento ativado para DRS, o vRealize Automation verifica a configuração de fallback da zona de nuvem:

- Com fallback
 - O vRealize Automation aloca o processamento e o armazenamento que permanecem qualificados mesmo sem uma recomendação do vRealize Operations Manager.
- Sem fallback
 - O vRealize Automation cancela a solicitação e não continua o provisionamento.

Fase 3: Provisionamento

O vRealize Automation implanta as máquinas virtuais, o armazenamento e a rede solicitados por meio do adaptador referente ao destino de posicionamento selecionado no fim da fase de alocação.

O destino de posicionamento consiste em hosts de processamento, clusters ou pools de recursos e no repositório de dados de armazenamento ou no cluster de repositório de dados anexado.

Otimização contínua usando o vRealize Operations Manager

Quando você adiciona o adaptador do vRealize Automation no vRealize Operations Manager, o vRealize Operations Manager cria automaticamente um novo centro de dados personalizado (CDC) para cargas de trabalho com base no vRealize Automation.

Com a otimização contínua, você aproveita o rebalanceamento e a realocação de cargas de trabalho e usa o vRealize Automation com o vRealize Operations Manager além do posicionamento inicial das cargas de trabalho. À medida que os recursos de virtualização se movem ou recebem mais ou menos carga, as cargas de trabalho provisionadas do vRealize Automation podem se mover conforme necessário.

- A otimização contínua cria automaticamente um novo CDC no vRealize Operations Manager. Há um novo CDC para cada zona de nuvem do vRealize AutomationvSphere.
- O CDC recém-criado contém todos os clusters gerenciados do vRealize Automation associados à zona de nuvem.

Observação Não crie manualmente um CDC misto de clusters do vRealize Automation e não do vRealize Automation.

- Você usa o vRealize Operations Manager para executar a otimização contínua do CDC com base no vRealize Automation recém-criado.
- Cargas de trabalho só podem ser rebalanceadas ou realocadas na mesma zona de nuvem ou CDC.
- A otimização nunca cria uma nova violação de posicionamento do vRealize Automation ou do vRealize Operations Manager.
 - Se você tiver violações de posicionamento existentes, a otimização poderá corrigir problemas de intenção operacional do vRealize Operations Manager.
 - Se você tiver violações de posicionamento existentes, a otimização não poderá corrigir problemas de intenção de negócios do vRealize Operations Manager.

Por exemplo, se você tiver usado o vRealize Operations Manager para mover manualmente uma máquina virtual até um cluster que não oferece suporte às suas restrições, o vRealize Operations Manager não detectará uma violação nem tentará resolvê-la.
- Essa versão obedece à intenção operacional no nível do CDC. Todos os clusters do vRealize Automation dos membros são otimizados para as mesmas configurações.

Para definir uma intenção operacional diferente para os clusters, você deve configurá-los em CDCs do vRealize Automation separados, associados a zonas de nuvem do vSphere separadas. Ter diferentes clusters de teste e produção pode ser uma situação de exemplo.

- A intenção de aplicativo do vRealize Automation e as restrições definidas no vRealize Automation são seguidas durante qualquer operação de rebalanceamento ou realocação de otimização.
- Tags de posicionamento do vRealize Operations Manager não podem ser aplicadas a cargas de trabalho provisionadas do vRealize Automation.

Além disso, há suporte para otimização programada envolvendo várias máquinas. Otimizações programadas regularmente não são processos do tipo tudo ou nada. Se condições interromperem a movimentação das máquinas, as máquinas realocadas com sucesso permanecerão realocadas, e o próximo ciclo do vRealize Operations Manager tentará realocar o restante como é habitual para o vRealize Operations Manager. Essa otimização parcialmente concluída não causa nenhum efeito negativo no vRealize Automation.

Como habilitar a otimização contínua

Quando você adiciona o adaptador do vRealize Automation no vRealize Operations Manager, o vRealize Operations Manager cria automaticamente um centro de dados dedicado para cargas de trabalho com base no vRealize Automation.

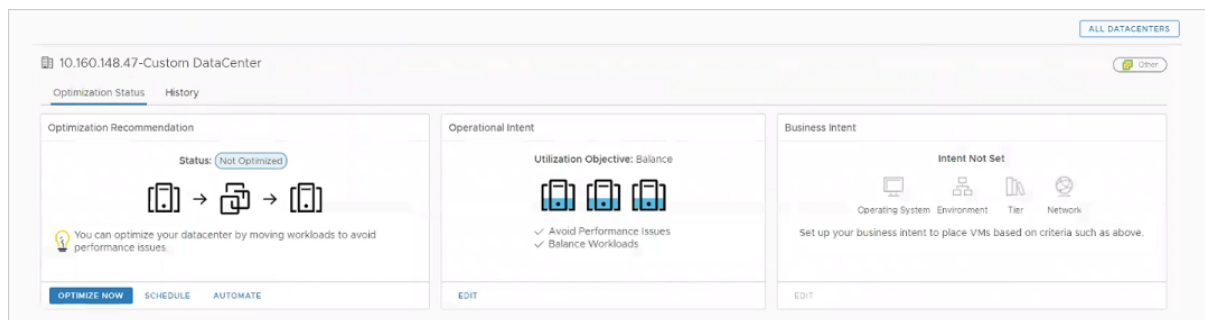
Além de adicionar a integração dentro do Cloud Assembly, não há etapas de instalação separadas para otimização contínua. Você pode começar configurando e usando o vRealize Operations Manager para realocação da carga de trabalho no novo centro de dados. Consulte o [Exemplo de otimização contínua](#).

Exemplo de otimização contínua

O exemplo a seguir mostra um fluxo de trabalho de rebalanceamento para otimização contínua do vRealize Automation com o vRealize Operations Manager.

- 1 Na página inicial do vRealize Operations Manager, clique em **Otimização da Carga de Trabalho**.
- 2 Selecione o centro de dados do vRealize Automation criado automaticamente.
- 3 Em **Intenção Operacional**, clique em **Editar** e selecione **Balancear**.

Não é possível selecionar ou editar a Intenção de Negócios, que fica desabilitada quando o centro de dados é para a otimização do vRealize Automation.



- 4 Em **Recomendação de Otimização**, clique em **Otimizar Agora**.

O vRealize Operations Manager exibe um diagrama antes e depois da operação proposta.

- 5 Clique em **Seguinte**.
- 6 Clique em **Iniciar Ação**.
- 7 No vRealize Automation, monitore a operação em andamento clicando em **Recursos > Implantações** e observando o status do evento.

| Events Request inputs | | | |
|---|------------|-------------|------------|
| #7 - Relocate RRD-WLP-003 In Progress Requested by: System User Requested for: Fritz Arbeiter Requested on: August 13, 2018 11:43 AM | | | |
| Tasks | Component | Status | Depends On |
| Submitted | Deployment | Successful | |
| Pre-approval | Deployment | Approved | |
| Relocate | Deployment | In Progress | |
| Post-approval | Deployment | | |
| Completed | Deployment | | |

Quando o rebalanceamento terminar, o vRealize Automation será atualizado. A página Recursos de processamento mostra que máquinas foram movidas.

No vRealize Operations Manager, a próxima coleta de dados atualiza a exibição para mostrar que a otimização foi concluída.

10.160.148.47-Custom DataCenter

ALL DATACENTERS

Other

Optimization Status History

Optimization Recommendation

Status: Optimized

Your workloads are optimized according to your settings.

OPTIMIZE NOW

SCHEDULE

AUTOMATE

Operational Intent

Utilization Objective: Balance

✓ Avoid Performance Issues

✓ Balance Workloads

EDIT

Business Intent

Intent Not Set

Operating System Environment Tier Network

Set up your business intent to place VMs based on criteria such as above.

EDIT

No vRealize Operations Manager, você pode revisar a operação clicando em **Administração > Histórico > Tarefas Recentes**.

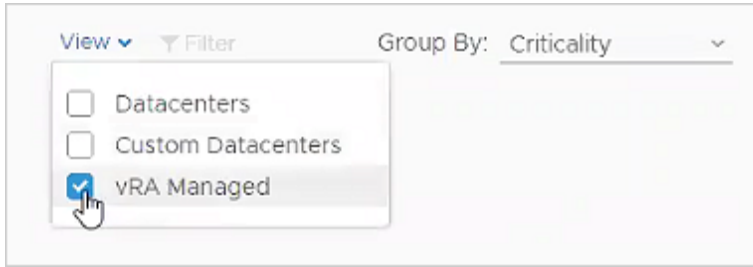
Localizar centros de dados do vRealize Automation gerenciados

Você pode usar o vRealize Operations Manager para exibir apenas os centros de dados do vRealize Automation gerenciados.

Procedimentos

- 1 Na página inicial do vRealize Operations Manager, clique em **Otimização da Carga de Trabalho**.

- 2 Próximo ao canto superior direito, clique no menu suspenso **Exibir**.
- 3 Selecione apenas os centros de dados do vRealize Automation gerenciados.



Monitoramento da implantação com base no vRealize Operations Manager

O vRealize Automation agora pode mostrar dados do vRealize Operations Manager sobre as suas implantações.

Revisar o conjunto filtrado de métricas diretamente no vRealize Automation dispensa a tarefa de acessar ou pesquisar o vRealize Operations Manager. Embora não seja possível iniciar no contexto para o vRealize Operations Manager, obviamente você tem a liberdade de fazer login e usar o vRealize Operations Manager para dados adicionais, conforme necessário.

Habilitar dados do vRealize Operations Manager

Para que o vRealize Automation mostre dados do vRealize Operations Manager, integrações específicas devem estar presentes. As integrações exigem que você forneça o endereço e as credenciais de login para o vRealize Automation, o vRealize Operations Manager e o vCenter.

Procedimentos

- 1 No vRealize Operations Manager, acesse **Fontes de Dados > Integrações** e verifique ou adicione a integração com a sua conta do vCenter.
- 2 No Cloud Assembly, acesse **Infraestrutura > Conexões > Contas de Nuvem** e verifique ou adicione sua conta do vCenter.

O vRealize Operations Manager e o vRealize Automation devem estar conectados ao mesmo vCenter.

- 3 No vRealize Operations Manager, acesse **Fontes de Dados > Integrações** e adicione a integração com a sua conta de adaptador do vRealize Automation 8.x.
- 4 No Cloud Assembly, acesse **Infraestrutura > Conexões > Integrações** e adicione a integração com o vRealize Operations Manager.

Digite o endereço do vRealize Operations Manager no seguinte formato:

`https://operations-manager-IP-address-or-FQDN/suite-api`

Para obter informações adicionais, consulte [Integrando com o vRealize Operations Manager](#).

Próximo passo

No Cloud Assembly, clique em **Recursos > Implantações**, selecione uma implantação no vCenter e verifique se a guia Monitor é exibida.

Integridade e alertas fornecidos pelo vRealize Operations Manager

Quando o monitoramento está ativado, o vRealize Automation recupera alertas de Integridade do vRealize Operations Manager e associados sobre as suas implantações.

Para acessar o monitoramento, clique em uma implantação e selecione a guia **Monitorar**. Se a guia estiver ausente, consulte [Habilitar dados do vRealize Operations Manager](#).

Para ver os alertas, realce o nome da implantação na parte superior da árvore do componente no painel esquerdo.

- É possível revisar a gravidade e o texto dos alertas.
- Para concentrar-se em áreas de interesse, filtre e classifique os dados nas colunas.
- Somente crachás de Integridade e alertas de Integridade são exibidos. Outros tipos de alerta, como Eficiência ou Risco, não têm suporte.

Métricas fornecidas pelo vRealize Operations Manager

Quando o monitoramento está habilitado, o vRealize Automation recupera métricas do vRealize Operations Manager sobre suas implantações.

Para acessar o monitoramento, clique em uma implantação e selecione a guia **Monitorar**. Se a guia estiver ausente, consulte [Habilitar dados do vRealize Operations Manager](#).

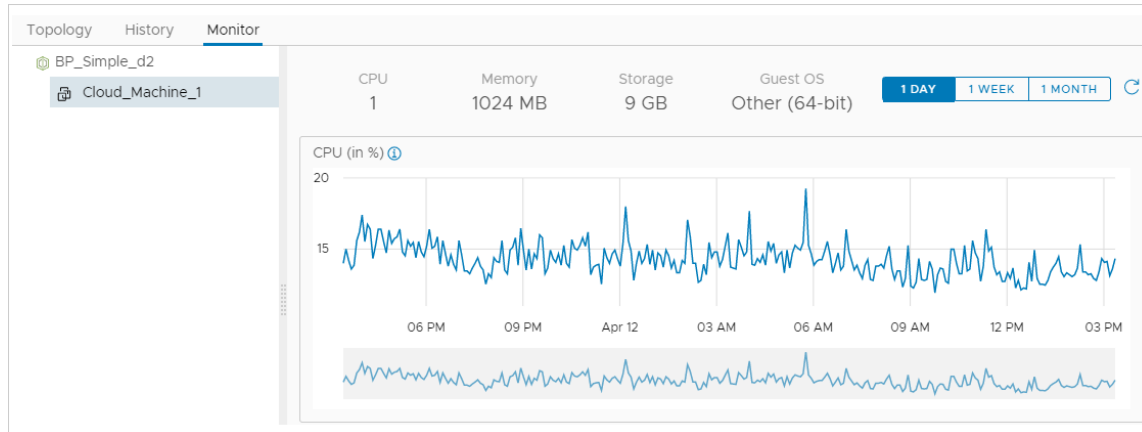
Para ver as métricas, expanda a árvore de componentes à esquerda e realce uma máquina virtual.

- Métricas não são armazenadas em cache. Eles são diretamente provenientes do vRealize Operations Manager e podem demorar alguns minutos para serem carregadas.
- Apenas as métricas de máquinas virtuais são exibidas. Não há suporte para métricas de outros componentes, como o vCloud Director, Softwares ou XaaS.
- Apenas as métricas de máquinas virtuais do vSphere são exibidas. Outros provedores de nuvem, como a AWS ou o Azure, não são compatíveis.

As métricas aparecem como gráficos de linha do tempo que mostram altos e baixos para as seguintes medidas.

- CPU
- Memória
- IOPS de armazenamento
- MBPS de rede

Para revelar o nome da métrica específica, clique no ícone azul de informações no canto superior esquerdo da linha do tempo.

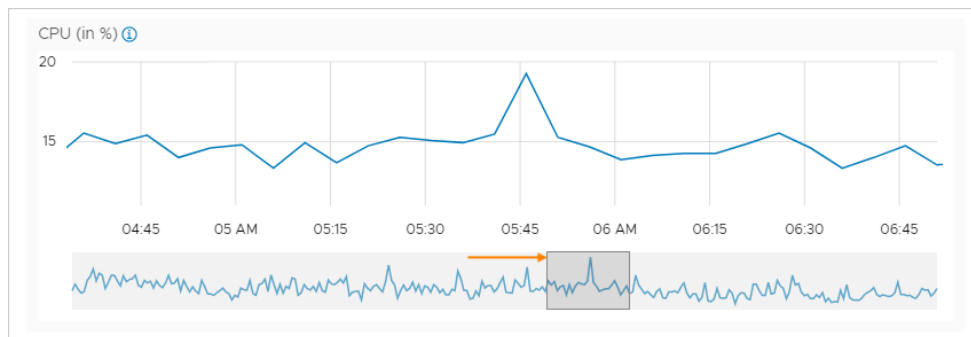


Agindo com base nos dados fornecidos pelo vRealize Operations Manager

Quando as métricas fornecidas pelo vRealize Operations Manager expõem um problema, você pode identificar as áreas de problemas diretamente no vRealize Automation.

Para ver as métricas fornecidas pelo vRealize Operations Manager, clique em uma implantação e selecione a guia **Monitorar**. Se a guia estiver ausente, consulte [Habilitar dados do vRealize Operations Manager](#).

Estão disponíveis métricas para o dia, a semana ou o mês anterior. Para ampliar o zoom em uma área de interesse, selecione uma pequena área na parte inferior e sombreada sob a linha do tempo de qualquer métrica:



Gerenciamento de recursos e otimização de implantação usando métricas do vRealize Operations Manager no vRealize Automation

Em um ambiente integrado do vRealize Automation e do vRealize Operations Manager, você pode acessar insights e alertas para objetos do vRealize Automation que são monitorados pelo vRealize Operations Manager.

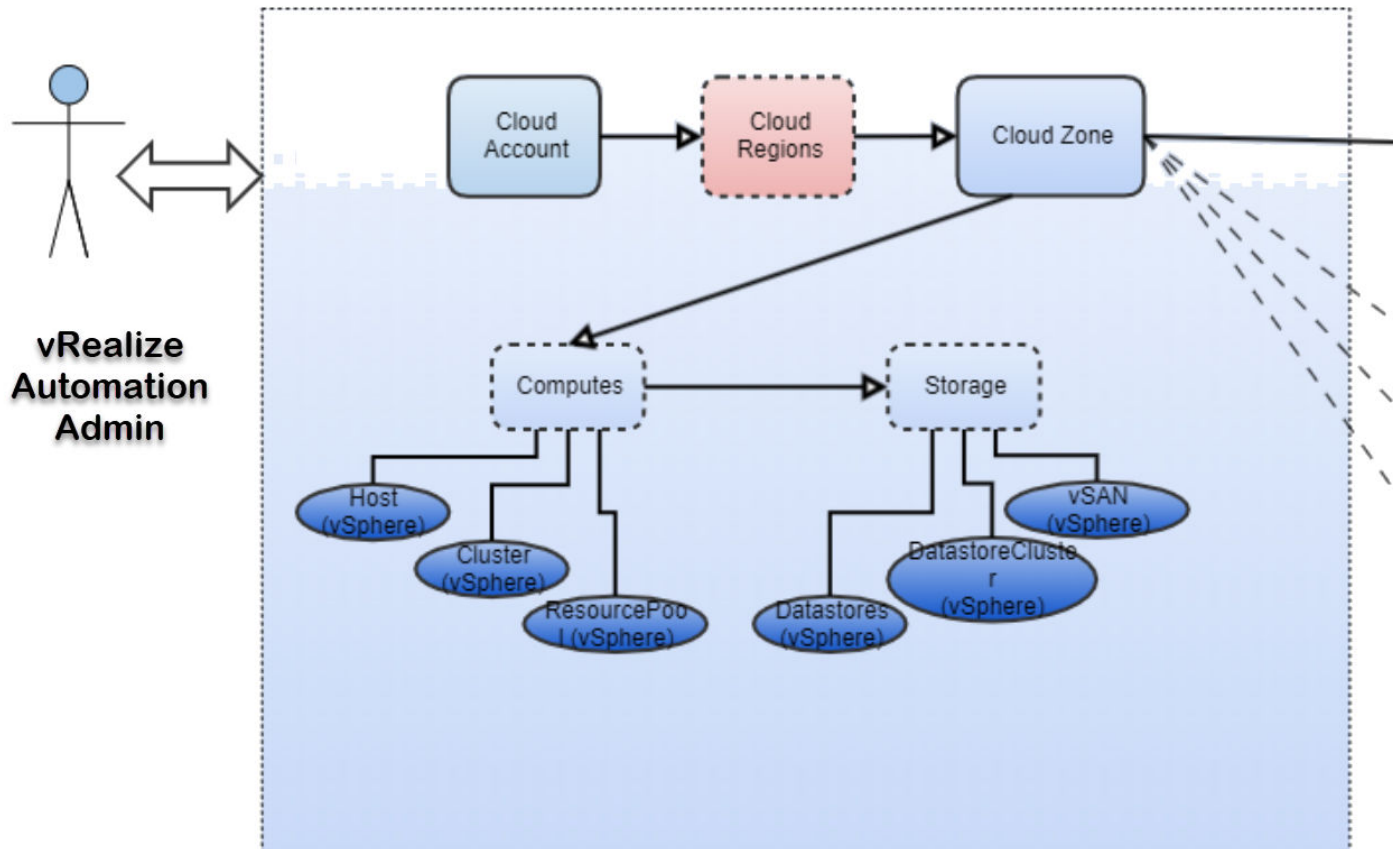
O painel **Insights** e as páginas de guia **Alertas** fornecem a capacidade em tempo real e informações de conscientização relacionadas de que você precisa para tomar decisões de gerenciamento no vRealize Automation sem precisar abrir o vRealize Operations Manager. As informações são fornecidas pelo aplicativo vRealize Operations Manager associado.

Como trabalhar com o painel Insights e com alertas de recursos

O painel **Insights** transmite informações sobre o consumo da capacidade em todos os processamentos na zona de nuvem e agrupadas por projetos. Ele também pode mostrar implantações de projeto que requerem otimização.

As páginas **Alertas** exibem potenciais preocupações de capacidade e desempenho para objetos como zonas de nuvem, projetos, implantações e máquinas virtuais. Elas também contêm informações para os proprietários do projeto sobre quais de suas implantações podem ser otimizadas. Cada link de implantação abre a guia **Otimizar** na implantação, onde orientações específicas são fornecidas.

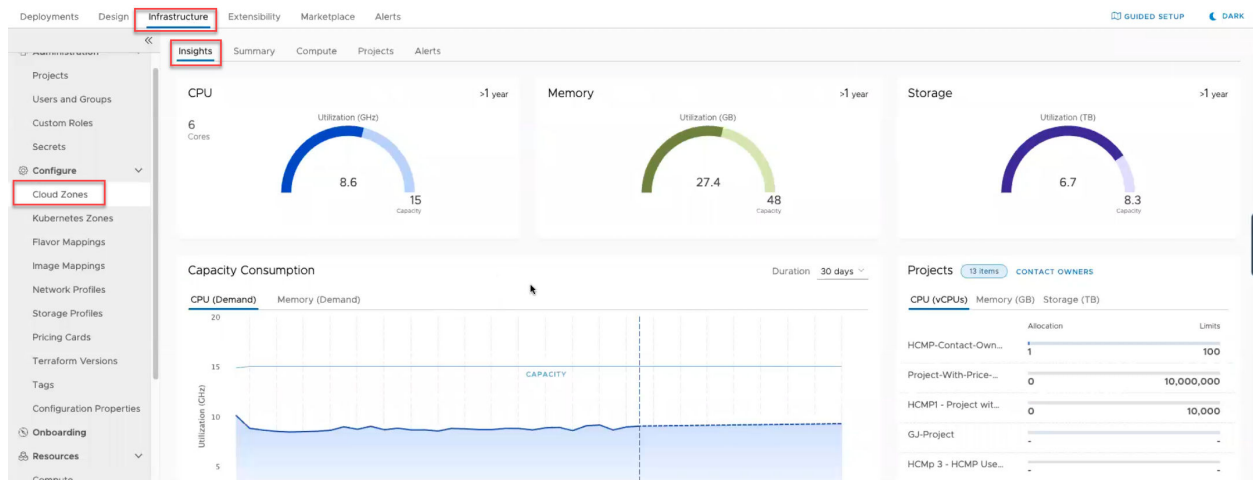
O diagrama a seguir ilustra a relação entre seus recursos do vRealize Automation e as implantações e os dados que o aplicativo vRealize Operations Manager associado fornece para você no vRealize Automation.



Como trabalhar com o painel Insights

O painel **Insights**, disponível em cada página de zona de nuvem, contém as seguintes métricas do vRealize Operations Manager:

- Uso de CPU, memória e armazenamento como uma porcentagem da capacidade
- Resumo do consumo de capacidade
- Histórico de uso e demanda de CPU e memória
- Consumo entre projetos
- Capacidade de recurso recuperável, com economia de custos, para implantações e projetos em uma zona de nuvem



Ele também fornece uma opção para alertar os proprietários do projeto sobre implantações que podem ser otimizadas.

O dashboard **Insights** está disponível para zonas de nuvem do vSphere e do VMware Cloud on AWS, desde que as contas de nuvem estejam configuradas tanto no vRealize Automation quanto no vRealize Operations Manager e estejam sendo monitoradas no vRealize Operations Manager.

Para obter detalhes, consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#).

Trabalhando com alertas

As páginas **Alertas** fornecem as seguintes categorias de filtragem. Categorias de filtragem são fornecidas pelo aplicativo vRealize Operations Manager associado.

- Gravidade
- Status
- Impacto
- Tipo
- Subtipo

■ Recurso

Cada filtro pode ser ainda mais refinado usando filtros rápidos. Por exemplo, o filtro de recursos pode ser ainda mais refinado por seus tipos de filtro rápido de zona de nuvem, máquina virtual, implantação e recurso de projeto.

Use combinações de filtros e filtros rápidos para controlar quais alertas estão disponíveis para exibição.

Deployments Design Infrastructure Extensibility Marketplace Alerts

Resource Type Quick filters

Today

- ☒ Cloud Zone
- ☒ Virtual Machine
- ☐ Deployment
- ☒ Project

Yesterday

Virtual machine is powered off for more than 5 days 4:40 PM
Virtual Machine » Cloud_vSphere_Machine_1-mcm222450-155465769232
Virtual machine is powered off for more than 5 days

Virtual machine is powered off for more than 5 days 4:40 PM
Virtual Machine » Cloud_vSphere_Machine_2-mcm222451-155465774235
Virtual machine is powered off for more than 5 days

AlertDefinition_20571bc0-a68c-477c-bb93-118da83... 1:26 PM
Cloud Zone » sqa-vc65 / Datacenter

AlertDefinition_6b5667f5-eb02-4b2e-bcf9-40cbb2... 1:26 PM
Cloud Zone » sqa-vc67.sqa.local / Datacenter

AlertDefinition_bf5e68e4-28f1-4992-af8d-94ea214ff... 1:26 PM
Cloud Zone » sqa-vc67.sqa.local / Datacenter

1 / 7

Virtual machine is powered off for more than 5 days
Created: Dec 13, 2020, 4:40:46 PM | Updated: Dec 14, 2020, 7:04:47 PM
Virtual Machine » Cloud_vSphere_Machine_1-mcm222450-155465769232

Virtual machine is powered off for more than 5 days

Severity: Warning Status: Active Impact: Health Type: Infrastructure

Suggestions 2 REVIEW DEPLOYMENT

- Delete powered off machines
- Manually power on the virtual machine.

Notes

Leave a note...

ADD NOTE

Alguns **Alertas** fornecem informações e um link para implantações que podem ser otimizadas. Um alerta individual pode fornecer a opção de entrar em contato com o proprietário do projeto, examinar um dashboard do Insights ou realizar as ações possíveis.

The screenshot displays the vRealize Automation Cloud Assembly interface. The top navigation bar includes tabs for Deployments, Design, Infrastructure, Extensibility, Marketplace, and Alerts (which is currently selected). Below the navigation bar, there are filters for Severity (set to Critical) and Status (set to Active). The main content area is divided into two sections: 'Today' and 'Yesterday'. The 'Today' section shows an alert titled 'The project has some deployments that contain optimizable resources' with a severity of Critical and a status of Active. The alert details show it was created on Dec 14, 2020, at 6:17:44 PM and updated at the same time. The project is 'vc65 project'. The alert message states: 'The project has some deployments that contain optimizable resources.' Below the alert details, there are suggestions for action, including 'REVIEW PROJECT'. A red box highlights the 'Deployments to review' section, which contains a table with one entry: 'contact-owner-test-dep-2'. A red arrow points from the alert title in the sidebar to the details view. Another red arrow points from the 'Deployments to review' table to the 'Notes' section, which contains the text 'Investigating'.

Alertas estão disponíveis para objetos de recursos do vSphere e do VMware Cloud on AWS.

Para obter detalhes sobre como configurar e usar alertas integrados, consulte [Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation](#) e [Como usar Alertas para otimizar implantações no vRealize Automation](#).

O que são planos de integração no Cloud Assembly

Um plano de integração de carga de trabalho é usado para identificar máquinas que foram coletadas por dados de um tipo de conta de nuvem em uma região de destino ou centro de dados, mas que ainda não são gerenciadas por um projeto do Cloud Assembly.

Quando você adiciona uma conta de nuvem que contém máquinas implantadas fora do Cloud Assembly, as máquinas não são gerenciadas pelo Cloud Assembly até que sejam integradas. Use um plano de integração para colocar máquinas não gerenciadas no gerenciamento do Cloud Assembly. Crie um plano, preencha-o com máquinas e, em seguida, execute o plano para importar as máquinas. Usando o plano de integração, é possível criar um modelo de nuvem e também é possível criar uma ou várias implantações.

Você pode integrar uma ou várias máquinas não gerenciadas em um único plano selecionando as máquinas manualmente.

- Você pode integrar até 3.500 máquinas não gerenciadas de um único plano de integração por hora.
- Você pode integrar até 17.000 máquinas não gerenciadas ao mesmo tempo de vários planos de integração por hora.

As máquinas disponíveis para integração de carga de trabalho estão listadas em **Recursos > Recursos > Máquinas Virtuais** com o rótulo *Discovered* na coluna Origem. Somente as máquinas coletadas através de dados são listadas. Após a integração das máquinas, elas aparecem na coluna Origem como *Deployed*. Você pode filtrar por máquinas descobertas ou implantadas

clicando no ícone de filtro



A interface do vRealize Automation Cloud Assembly exibe a seção de Máquinas Virtuais. No topo, há uma barra de navegação com as opções: Resources, Design, Infrastructure e Extensibility. Abaixo, há uma barra lateral com o menu "Resources" expandido, mostrando opções como Deployments, Resources, All Resources, Virtual Machines, Volumes e Networking & Security. No centro, há uma seção de filtros com o botão "CLEAR ALL" e uma lista de opções de origem de recursos: Projects, Cloud Types, Cloud Accounts, Resource Tags e Resource Origin. A opção "Resource Origin" está expandida, mostrando "Deployed" (25) e "Discovered" (1442), com a opção "Discovered" selecionada. À direita, há uma seção intitulada "Virtual Machines" com um botão "+ NEW VM" e uma tabela de máquinas virtuais.

| | Name | Depl |
|----|------------------------------|------|
| >> | ⋮ popove-vSphere Server... | |
| >> | ⋮ aws-vm-mcm602-1866... | |
| >> | ⋮ dboikliev-vRealizeOrch... | |

A pessoa que executa o plano de integração de carga de trabalho é automaticamente atribuída como o proprietário da máquina.

A integração também oferece suporte à integração de propriedades personalizadas, discos anexados, alteração de proprietários de implantação e redes vSphere.

- Propriedades personalizadas - você pode definir propriedades personalizadas no plano e nos níveis de máquina individuais. Uma propriedade personalizada definida no nível da máquina substitui a mesma propriedade no nível do plano.
- Discos anexados - se uma máquina tiver discos não inicializáveis, eles serão automaticamente integrados à máquina pai. Para visualizar os discos não inicializáveis, clique no nome da máquina no plano e navegue até a guia **Armazenamento**.

- Propriedade de implantação - A integração permite que você altere o proprietário de implantação padrão. Para alterar o proprietário, selecione uma implantação na guia **Implantação**, clique em **Ações > Alterar Proprietário** e selecione o usuário desejado associado ao projeto.

Exemplos de integração

Para obter exemplos de técnicas de integração, consulte [Exemplo: máquinas selecionadas integradas como uma implantação única no Cloud Assembly](#).

Assinaturas de eventos de integração

Um evento `Deployment Onboarded` é criado ao executar o plano. Usando opções da guia extensibilidade, é possível assinar e executar ações nesses eventos de implantação.

Após a integração, você pode atualizar um projeto como uma ação de dia 2 para implantações integradas. Para usar a ação de alterar projeto, o projeto de destino deve usar os mesmos recursos da zona de nuvem que a implantação. Você não pode executar a ação de alterar projeto em implantações integradas nas quais tenha feito alterações após a integração.

Exemplo: máquinas selecionadas integradas como uma implantação única no Cloud Assembly

Neste exemplo, são integradas duas máquinas não gerenciadas como uma única implantação do Cloud Assembly e cria-se um único modelo de nuvem para todas as máquinas no plano.

Quando você cria uma conta de nuvem, os dados de todas as máquinas que estão associadas a ela são coletados e, em seguida, exibidos na página **Recursos > Recursos > Máquinas**. Se a conta de nuvem tiver máquinas que foram implantadas fora do Cloud Assembly, será possível usar um plano de integração para permitir que o Cloud Assembly gerencie as implantações de máquina.

Observação Você só pode renomear implantações antes que elas sejam integradas. Após a integração, a opção **Renomear** fica desativada.

Pré-requisitos

- Verifique se você tem a função de usuário necessária. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Revise [O que são planos de integração no Cloud Assembly](#).
- Crie e prepare um projeto do Cloud Assembly.

Esse procedimento envolve algumas das etapas do caso de uso básico do Wordpress. Consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).

- Crie um projeto, adicione usuários e atribua funções de usuário no projeto. Consulte [Parte 2: Criar o projeto do Cloud Assembly de exemplo](#).
- Crie uma conta de nuvem do Amazon Web Services para o projeto. Consulte a seção da conta de nuvem do [Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo](#).

A conta de nuvem do Amazon Web Services neste procedimento contém máquinas que foram implantadas antes que a conta de nuvem fosse adicionada ao Cloud Assembly e por um aplicativo diferente do Cloud Assembly.

- Verifique se a página **Recursos > Recursos > Máquinas Virtuais** contém máquinas para integrar. Consulte [Gerenciando recursos no Cloud Assembly](#) para obter mais informações.

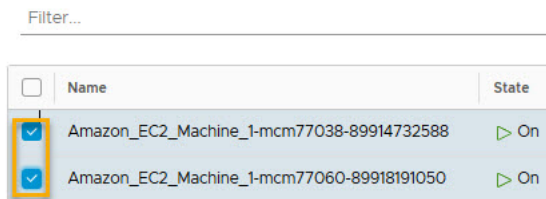
Procedimentos

- 1 Vá para **Infraestrutura > Integração**.
- 2 Clique em **Novo Plano de Integração** e digite os valores de amostra.

| Configuração | Valor de amostra |
|----------------|--|
| Nome do plano | VC-sqa-deployments |
| Descrição | Amostra de plano de integração para a máquina do AWS para a conta de nuvem OurCo-AWS |
| Conta de nuvem | OurCo-AWS |
| Projeto padrão | WordPress |

- 3 Clique em **Criar**.
- 4 Na guia **Implantações** do plano, clique em **Selecionar Máquinas**, escolha uma ou mais máquinas e clique em **OK**.

Select Machines



- 5 Selecione **Criar uma implantação que contenha todas as máquinas** e clique em **Criar**.
- 6 Clique na caixa de seleção ao lado do novo nome da implantação e clique em **Modelo de nuvem....**
- 7 Clique em **Criar Modelo de Nuvem no formato do Cloud Assembly** e insira um nome de modelo de nuvem, ou clique em **Atribuir um Modelo de Nuvem existente** e selecione o modelo de nuvem desejado a ser atribuído.

Observação O mapeamento de Modelos de Nuvem para implantações integradas é apenas para paridade visual para os consumidores finais. Implantações integradas não são compatíveis com Modelos de Nuvem.

8 Clique em **Salvar**.

Cloud Template Configuration

Mapping of Cloud Templates to onboarded deployments is only for visual parity for end consumers. Onboarded deployments are not compatible with Cloud Templates.

Deployment: Demo

☐ None (use runtime snapshot)
☐ Create Cloud Template in Cloud Assembly format
☒ Assign an existing Cloud Template

| Name | Project | Last Updated |
|---------------------------------------|------------|--------------------------|
| <input checked="" type="radio"/> Demo | onboarding | Oct 21, 2021, 1:36:15 PM |
| <input type="radio"/> 171 | onboarding | Jun 10, 2021, 8:21:55 AM |
| <input type="radio"/> asdf | onboarding | May 25, 2021, 9:24:07 AM |
| <input type="radio"/> asdf | onboarding | Dec 7, 2020, 3:03:53 PM |

CANCEL SAVE

Observação Quando seu plano de integração usa uma máquina do vSphere, você deve editar o modelo de nuvem após a conclusão do processo de integração. O processo de integração não pode vincular a máquina do vSphere de origem e seu modelo de máquina, e o modelo de nuvem resultante conterá a entrada `imageRef: "no image available"` no código do modelo de nuvem. O modelo de nuvem não poderá ser implantado até que você especifique o nome do modelo correto no campo `imageRef:`. Para facilitar a localização e atualização do modelo de nuvem após a conclusão do processo de integração, use a opção **Nome do modelo de nuvem** na página **Configuração de modelo de nuvem** da implantação. Registre o nome do modelo de nuvem gerado automaticamente ou insira e registre um nome de modelo de nuvem de sua escolha. Quando a integração estiver concluída, localize e abra o modelo de nuvem e substitua a entrada `"no image available"` no campo `imageRef:` pelo nome do modelo correto.

9 Clique na caixa de seleção de nome da implantação, clique em **Executar** e, em seguida, clique novamente em **Executar** na página **Executar Plano**.

As máquinas selecionadas são integradas como uma implantação única, com um modelo de nuvem acompanhante.

- 10 Abra e examine o modelo de nuvem clicando na página **Projetar > Modelos de nuvem** e, depois, no nome do modelo de nuvem.
- 11 Abra e examine a implantação clicando na página **Recursos > Implantações** e, depois, no nome da implantação.

Configuração avançada para o ambiente do Cloud Assembly

É possível configurar o ambiente do Cloud Assembly para oferecer suporte a configurações, integração e implantação de projetos.

Para obter informações relacionadas e adicionais sobre métodos de administração, como trabalhar com usuários e logs e ingressar ou sair do Programa de Experiência do Cliente, consulte a ajuda de [Administrando o vRealize Automation](#).

Como configurar um servidor proxy de Internet para o vRealize Automation

Para instalações do vRealize Automation em redes isoladas sem acesso direto à Internet, você pode usar um servidor proxy de Internet para permitir a funcionalidade Internet por proxy. O servidor proxy de Internet é compatível com HTTP e HTTPS.

Para configurar e usar provedores de nuvem pública, como a Amazon Web Services (AWS), o Microsoft Azure e a Google Cloud Platform (GCP), bem como os pontos de integração externos, como IPAM, Ansible e Puppet, com o vRealize Automation, você deve configurar um servidor proxy de Internet para acessar o servidor proxy de Internet interno do vRealize Automation.

O vRealize Automation contém um servidor proxy interno que se comunica com o seu servidor proxy de Internet. Esse servidor se comunicará com o servidor proxy se tiver sido configurado com o comando `vracli proxy set` Se você não tiver configurado um servidor proxy de Internet para a sua organização, o servidor proxy interno do vRealize Automation tentará se conectar diretamente à Internet.

É possível configurar o vRealize Automation para usar um servidor proxy de Internet usando o utilitário de linha de comando `vracli` fornecido. Informações sobre como usar a API do `vracli` estão disponíveis usando o argumento `--help` na linha de comando `vracli`, por exemplo `vracli proxy --help`.

O acesso ao servidor proxy de Internet requer o uso de controles incorporados no local de extensibilidade com base em ações (ABX) que estão integrados ao vRealize Automation.

Observação O acesso ao Workspace ONE Access (anteriormente chamado de VMware Identity Manager) não tem suporte por meio do proxy de Internet. Não é possível usar o comando `vracli set vidm` para acessar o Workspace ONE Access por meio do servidor proxy de Internet.

O servidor proxy interno requer IPv4 como formato de IP padrão. Ele não exige restrições de protocolo de Internet, autenticação ou ações de "Man-in-the-middle" no tráfego de certificado TLS (HTTPS).

Pré-requisitos

- Verifique se você tem um servidor HTTP ou HTTPS, que possa ser usado como o servidor proxy de Internet, na rede do vRealize Automation e que seja capaz de transmitir o tráfego de saída para sites externos. A conexão deve ser configurada para IPv4.
- Certifique-se de que o servidor proxy de Internet de destino esteja configurado para oferecer suporte ao IPv4 como seu formato IP padrão e não ao IPv6.
- Se o servidor proxy de Internet usar TLS e exigir uma conexão HTTPS com seus clientes, você deverá importar o certificado de servidor usando um dos seguintes comandos antes de definir a configuração de proxy.

- `vracli certificate proxy --set path_to_proxy_certificate.pem`
- `vracli certificate proxy --set stdin`

Use o parâmetro `stdin` para entrada interativa.

Procedimentos

- 1 Crie uma configuração de proxy para os pods ou contêineres que são usados pelo Kubernetes. Neste exemplo, o servidor proxy é acessado usando o esquema HTTP.

```
vracli proxy set --host http://proxy.vmware.com:3128
```

- 2 Mostre a configuração de proxy.

```
vracli proxy show
```

O resultado será semelhante a:

```
{
  "enabled": true,
  "host": "10.244.4.51",
  "java-proxy-exclude": "*.local|*.localdomain|localhost|10.244.*|
192.168.*|172.16.*|kubernetes|sc2-rdops-vm06-dhcp-198-120.eng.vmware.com|10.192.204.9|
*.eng.vmware.com|sc2-rdops-vm06-dhcp-204-9.eng.vmware.com|10.192.213.146|sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com|10.192.213.151|sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "java-user": null,
  "password": null,
  "port": 3128,
  "proxy-
exclude": ".local,.localdomain,localhost,10.244.,192.168.,172.16.,kubernetes,sc2-
rdops-vm06-dhcp-198-120.eng.vmware.com,10.192.204.9,.eng.vmware.com,sc2-
rdops-vm06-dhcp-204-9.eng.vmware.com,10.192.213.146,sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com,10.192.213.151,sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "scheme": "http",
  "upstream_proxy_host": null,
  "upstream_proxy_password_encoded": "",
  "upstream_proxy_port": null,
  "upstream_proxy_user_encoded": "",
  "user": null,
  "internal.proxy.config": "dns_v4_first on \nhttp_port
0.0.0.0:3128\nlogformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs
%<st %rm %ru %<un %Sh/%<a %mt\naccess_log stdio:/tmp/logger squid\ncoredump_dir /\ncache
```

```
deny all \nappend_domain .prelude.svc.cluster.local\nacl mylan src 10.0.0.0/8\nacl mylan
src 127.0.0.0/8\nacl mylan src 192.168.3.0/24\nacl proxy-exclude dstdomain .local\nacl
proxy-exclude dstdomain .localdomain\nacl proxy-exclude dstdomain localhost\nacl
proxy-exclude dstdomain 10.244.\n acl proxy-exclude dstdomain 192.168.\n acl proxy-exclude
dstdomain 172.16.\n acl proxy-exclude dstdomain kubernetes\nacl proxy-exclude dstdomain
10.192.204.9\nacl proxy-exclude dstdomain .eng.vmware.com\nacl proxy-exclude dstdomain
10.192.213.146\nacl proxy-exclude dstdomain 10.192.213.151\nalways_direct allow proxy-
exclude\nhttp_access allow mylan\nhttp_access deny all\n# End autogen configuration\n",
    "internal.proxy.config.type": "default"
}
```

Observação Se você tiver configurado um servidor proxy de Internet para a sua organização, "internal.proxy.config.type": "non-default" aparecerá no exemplo acima em vez de 'default'. Por segurança, a senha não é exibida.

Observação Se você usar o parâmetro `-proxy-exclude`, deverá editar os valores padrão. Por exemplo, se quiser adicionar `acme.com` como um domínio que não pode ser acessado usando o servidor proxy de Internet, use as seguintes etapas:

- a Insira `vracli proxy default-no-proxy` para obter as configurações padrão de exclusão de proxy. Esta é uma lista de domínios e redes gerados automaticamente.
- b Edite o valor para adicionar `.acme.com`.
- c Insira `vracli proxy set --proxy-exclude ...` para atualizar as definições de configuração.
- d Execute o comando `/opt/scripts/deploy.sh` para reimplantar o ambiente.

- 3 (Opcional) Exclua domínios DNS, FQDNs e endereços IP para impedir que eles sejam acessados pelo servidor proxy de Internet.

Sempre modifique os valores padrão da variável `proxy-exclude` usando `parameter --proxy-exclude`. Para adicionar o domínio `exclude.vmware.com`, primeiro use o comando `vracli proxy show` e depois copie a variável `proxy-exclude` e adicione o valor de domínio usando o comando `vracli proxy set ...`, conforme abaixo:

```
vracli proxy set --host http://
proxy.vmware.com:3128 --proxy-exclude "exclude.vmware.com,docker-
registry.prelude.svc.cluster.local,localhost,.local,.cluster.local,10.244.,192.,172.16.,sc-
rdops-vm11-dhcp-75-38.eng.vmware.com,10.161.75.38,.eng.vmware.com"
```

Observação Adicione elementos a `proxy-exclude` em vez de substituir os valores. Se você excluir os valores padrão do `proxy-exclude`, o vRealize Automation não funcionará corretamente. Se isso acontecer, exclua a configuração de proxy e comece novamente.

- 4 Depois de definir o servidor proxy de Internet com o comando `vracli proxy set ...`, você poderá usar o comando `vracli proxy apply` para atualizar a configuração do servidor proxy de Internet e tornar as configurações de proxy mais recentes ativas.

- 5 Se ainda não tiver feito isso, ative as alterações de script executando o seguinte comando:

```
/opt/scripts/deploy.sh
```

- 6 (Opcional) Se necessário, configure o servidor proxy para oferecer suporte ao acesso externo na porta 22.

Para oferecer suporte a integrações como o Puppet e o Ansible, o servidor proxy deve permitir que a porta 22 acesse os hosts relevantes.

Exemplo: Amostra de configuração do Squid

Em relação à etapa 1, se você estiver configurando um proxy Squid, poderá ajustar sua configuração em `/etc/squid/squid.conf` adaptando-a à seguinte amostra:

```
acl localnet src 192.168.11.0/24

acl SSL_ports port 443

acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

http_access allow !Safe_ports
http_access allow CONNECT !SSL_ports
http_access allow localnet

http_port 0.0.0.0:3128

maximum_object_size 5 GB
cache_dir ufs /var/spool/squid 20000 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320

client_persistent_connections on
server_persistent_connections on
```

O que posso fazer com o mapeamento do NSX-T para vários vCenters no vRealize Automation

Você pode associar uma conta de nuvem do NSX-T a uma ou mais contas de nuvem do vCenter para oferecer suporte a vários objetivos de implantação.

Você pode associar a mesma rede de NSX-T existente a perfis de rede de diferentes vCenters e provisionar uma implantação no vCenter com base em restrições. Alguns exemplos estão listados abaixo:

- Modelos de nuvem que contêm uma única máquina com várias NICs que usam o mesmo perfil de rede, no qual esse perfil de rede contém uma rede do NSX-T que se estende por vários vCenters.
- Modelos de nuvem que contêm uma máquina em uma rede *privada* que usa o perfil de rede com isolamento baseado em sub-rede e que usa uma rede do NSX-T *existente* que abrange vários vCenters.
- Modelos de nuvem que contêm uma única máquina em uma rede *privada* que usa um perfil de rede com isolamento baseado em grupo de segurança e que usa uma rede do NSX-T que se expande por vCenters.
- Modelos de nuvem que contêm uma única máquina em uma rede *roteada* que usa um perfil de rede com uma rede do NSX-T que se estende por vários vCenters.
- Modelos de nuvem que contêm um balanceador de carga sob demanda definido em um perfil de rede no qual o balanceador de carga é aplicado a todos os vCenters na rede.
- Modelos de nuvem que contêm uma rede sob demanda definida em um perfil de rede no qual a rede sob demanda é usada por todos os vCenters que usam o perfil de rede.
- Modelos de nuvem que contêm um grupo de segurança sob demanda que, opcionalmente, contém regras de firewall e no qual o grupo de segurança esteja associado a todos os vCenters na rede.

Você pode configurar o IPAM interno ou externo vRealize Automation na rede NSX-T e compartilhar o mesmo endereço IP para máquinas provisionadas em diferentes vCenters.

Se nenhum perfil de rede for definido em seu sistema, você poderá provisionar um modelo em nuvem que contém várias máquinas em diferentes vCenters que compartilham uma única rede NSX-T *existente*.

O que acontecerá se eu remover uma associação de conta de nuvem do NSX no vRealize Automation

Se você remover uma associação entre uma conta de nuvem do NSX e uma conta de nuvem do vCenter, você também precisará atualizar os perfis de rede relacionados para remover os objetos NSX associados.

Se você remover uma associação entre uma conta de nuvem do NSX e uma conta de nuvem do vCenter, os elementos de infraestrutura não serão atualizados automaticamente pelo vRealize Automation. Você precisa atualizar os perfis de rede existentes para remover os objetos NSX associados.

A interface do usuário fornece informações para ajudar a destacar os elementos de perfil de rede afetados da seguinte forma:

- Se o perfil de rede tiver um rede NSX existente selecionada:
 - O objeto está marcado como *inválido* e a mensagem *Alguns objetos de rede estão ausentes ou são inválidos* é exibida.
 - Os objetos são removidos quando você salva o perfil de rede.
- Se o perfil de rede tiver o isolamento de aplicativo configurado, você deverá atualizar as configurações da política de isolamento antes que o perfil de rede possa ser salvo.
- Se o perfil de rede tiver grupos de segurança ou balanceadores de carga selecionados, os objetos serão removidos quando você salvar o perfil de rede.

As implantações existentes continuam a funcionar conforme projetadas para os componentes existentes, mas falharão ao criar novos componentes, por exemplo, em uma operação de dimensionamento horizontal.

Se você restabelecer a associação, o perfil de rede será preenchido novamente e as implantações existentes funcionarão como projetadas.

Se você remover a conta de nuvem do NSX, o comportamento acima será o mesmo, mas os objetos de rede serão marcados como *ausentes* em vez de *inválidos*.

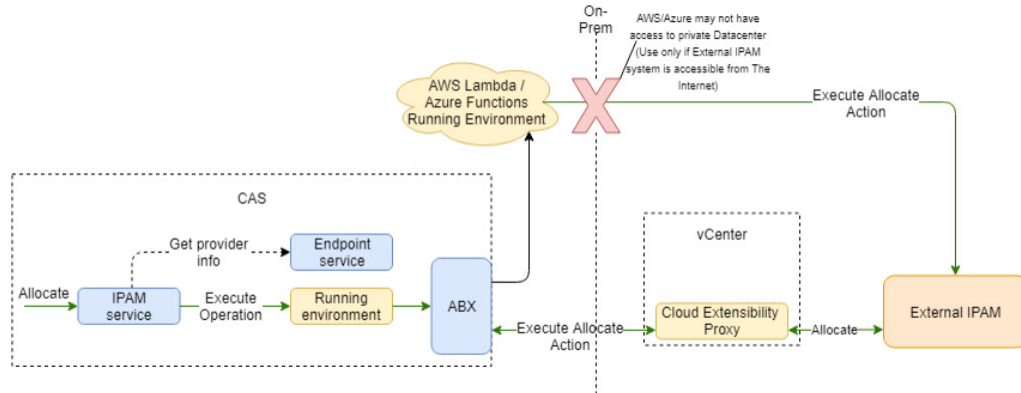
Como usar o SDK de IPAM para criar um pacote de integração de IPAM externo específico do provedor para o vRealize Automation

Fornecedores e parceiros de IPAM externos podem baixar e usar o SDK de IPAM para criar um pacote de integração de IPAM que permite ao vRealize Automation oferecer suporte à sua solução de IPAM específica do provedor.

O processo para criar e implantar um pacote de integração de IPAM personalizado para o vRealize Automation usando o SDK de IPAM fornecido está descrito no documento [Criando e implantando um pacote de integração de IPAM específico do provedor para o VMware Cloud Assembly](#).

Conforme descrito no documento, você pode baixar o *VMware vRealize Automation Third-Party IPAM SDK* mais recente disponível no site [VMware code](#). Os seguintes pacotes IPAM SDK estão disponíveis:

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



Antes de criar um pacote de integração de IPAM específico de fornecedor usando o SDK de IPAM, verifique se já existe um para o vRealize Automation. Você pode verificar se há um pacote de integração de IPAM específico do provedor no site do provedor de IPAM ou no [VMware Marketplace](#).

Embora o exemplo do [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#) seja específico do fornecedor, ele também contém informações de referência úteis.

Usando o vRealize Automation com a Azure VMware Solution

Este procedimento descreve como configurar o vRealize Automation para trabalhar com um ambiente de nuvem híbrida de autoatendimento da Microsoft Azure VMware Solution, para que seja possível usar cargas de trabalho do vRealize Automation nesse ambiente.

O vRealize Automation oferece suporte a conexões com a Azure VMware Solution (AVS) para movimentar e executar cargas de trabalho da VMware em um ambiente de nuvem do Azure. A AVS foi criada pela Microsoft para oferecer suporte à interface com ambientes VMware.

O uso da AVS é bem documentado pela Microsoft. Você pode encontrar a documentação aqui:

- Azure VMware Solution - <https://docs.microsoft.com/en-us/azure/azure-vmware/>

Para usar a AVS no vRealize Automation, você deve configurar as contas de nuvem do vCenter e do NSX-T. Consulte a seguinte documentação para configurar essas contas na nuvem:

- Configurar a conta de nuvem do vCenter - [Criar uma conta de nuvem do vCenter no vRealize Automation](#)
- Criar uma conta de nuvem do NSX-T - [Criar uma conta de nuvem do NSX-T no vRealize Automation](#)

O procedimento a seguir descreve as etapas genéricas para configurar seu ambiente para que você possa implantar cargas de trabalho do vRealize Automation na AVS.

- 1 Instale e configure a Azure VMware Solution com base nas instruções do fornecedor, conforme apropriado para o seu ambiente.
- 2 Crie contas de nuvem do vCenter e do NSX-T na sua implantação do vRealize Automation.

Usando o vRealize Automation com o Google Cloud VMware Engine

Este procedimento descreve como configurar o vRealize Automation para trabalhar com um ambiente de nuvem híbrida de autoatendimento do Google Cloud VMware Engine, para que você possa usar cargas de trabalho do vRealize Automation nesse ambiente.

O vRealize Automation oferece suporte a conexões com o Google Cloud VMware Engine (GCVE) para movimentar e executar cargas de trabalho da VMware na Google Cloud. O GCVE foi criado pelo Google para oferecer suporte à interface com ambientes VMware.

O uso do GCVE é bem documentado pelo Google. Você pode encontrar a documentação aqui:

- Google Cloud VMware Engine - <https://cloud.google.com/vmware-engine/docs>

Para usar o GCVE com o vRealize Automation, você deve configurar contas de nuvem do vCenter e do NSX-T no vRealize Automation. Consulte a seguinte documentação para configurar essas contas na nuvem:

- Configurar a conta de nuvem do vCenter - [Criar uma conta de nuvem do vCenter no vRealize Automation](#)
- Criar uma conta de nuvem do NSX-T - [Criar uma conta de nuvem do NSX-T no vRealize Automation](#)

O procedimento a seguir descreve as etapas generalizadas para configurar seu ambiente para que você possa implantar cargas de trabalho do vRealize Automation no GCVE.

- 1 Instale e configure o Google Cloud VMware Engine com base nas instruções do fornecedor, conforme apropriado para o seu ambiente.
- 2 Crie contas de nuvem do vCenter e do NSX-T na sua implantação do vRealize Automation.

Usando o vRealize Automation com a Oracle Cloud VMware Solution

Este procedimento descreve como configurar o vRealize Automation para trabalhar com um ambiente de nuvem híbrida de autoatendimento da Oracle Cloud VMware Solution, para que você possa usar cargas de trabalho do vRealize Automation nesse ambiente.

O vRealize Automation oferece suporte a conexões com a Oracle Cloud VMware Solution (OCVS) para movimentar e executar cargas de trabalho da VMware na Oracle Cloud. A OCVS foi criada pela Oracle para oferecer suporte à interface com ambientes VMware.

O uso da OCVS é bem documentado pela Oracle. Você pode encontrar a documentação aqui:

- Oracle Cloud VMware Solution - <https://docs.oracle.com/en-us/iaas/Content/VMware/Concepts/ocvsoverview.htm>

Para usar a OCVS, você deve configurar as contas de nuvem do vCenter e do NSX-T. Consulte a seguinte documentação para configurar essas contas na nuvem:

- Configurar a conta de nuvem do vCenter - [Criar uma conta de nuvem do vCenter no vRealize Automation](#)

- Criar uma conta de nuvem do NSX-T - [Criar uma conta de nuvem do NSX-T no vRealize Automation](#)

O procedimento a seguir descreve as etapas generalizadas para configurar seu ambiente para que você possa implantar cargas de trabalho do vRealize Automation na OCVS.

- 1 Instale e configure a Oracle Cloud VMware Solution com base nas instruções do fornecedor, conforme apropriado para o seu ambiente.
- 2 Crie contas de nuvem do vCenter e do NSX-T na sua implantação do vRealize Automation.

Usando o vRealize Automation com o VMware Cloud on Dell EMC

Este procedimento descreve como configurar o vRealize Automation para trabalhar com um ambiente de nuvem híbrida de autoatendimento do VMware Cloud on Dell EMC, para que você possa usar cargas de trabalho do vRealize Automation nesse ambiente.

O vRealize Automation oferece suporte a conexões com o VMware Cloud on Dell EMC para movimentar e executar cargas de trabalho da VMware.

Consulte a documentação do VMware Cloud on Dell EMC em <https://docs.vmware.com/br/VMware-Cloud-on-Dell-EMC/index.html> para obter mais informações.

Para usar o vRealize Automation com o VMware Cloud on Dell EMC, você deve configurar uma conta de nuvem do vCenter. Consulte a seguinte documentação para configurar essa conta de nuvem:

- Configurar a conta de nuvem do vCenter - [Criar uma conta de nuvem do vCenter no vRealize Automation](#)

O procedimento a seguir descreve as etapas generalizadas para configurar seu ambiente para que você possa implantar cargas de trabalho do vRealize Automation no VMware Cloud on Dell EMC.

- 1 Instale e configure o VMware Cloud on Dell EMC com base nas instruções do fornecedor, conforme apropriado para o seu ambiente.
- 2 Crie uma conta de nuvem do vCenter na sua implantação do vRealize Automation.

Como compilar a infraestrutura de recursos do Cloud Assembly

4

A infraestrutura de recursos do Cloud Assembly é onde são definidas as regiões de conta de nuvem como zonas nas quais os modelos de nuvem e suas cargas de trabalho podem ser implantados.

Além disso, a infraestrutura de recursos envolve a criação de mapeamentos comuns de imagens e tamanhos de máquinas e perfis que definem os recursos de rede e armazenamento em regiões de conta de nuvem ou centros de dados.

Este capítulo inclui os seguintes tópicos:

- Como adicionar zonas de nuvem que definem regiões de posicionamento de destino ou centros de dados do Cloud Assembly
- Como adicionar mapeamentos de tipos no vRealize Automation para especificar dimensionamentos de máquinas comuns
- Como adicionar mapeamentos de imagem no vRealize Automation para acessar sistemas operacionais comuns
- Como adicionar perfis de rede no vRealize Automation
- Como adicionar perfis de armazenamento do Cloud Assembly que se referem a diferentes requisitos
- Como usar cartões de preços no vRealize Automation
- Como usar tags para gerenciar recursos e implantações do Cloud Assembly
- Como trabalhar com recursos no vRealize Automation
- Configurando recursos de tenant de vários provedores com o vRealize Automation

Como adicionar zonas de nuvem que definem regiões de posicionamento de destino ou centros de dados do Cloud Assembly

Uma zona de nuvem do Cloud Assembly é um conjunto de recursos dentro de um tipo de conta de nuvem, como AWS ou vSphere.

As zonas de nuvem em uma região específica da conta, são onde os modelos de nuvem implantam cargas de trabalho. Cada zona de nuvem está associada a um projeto do Cloud Assembly.

Selecione **Infraestrutura > Configurar > Zonas de Nuvem** e clique em **Adicionar Nova Zona**.

Saiba mais sobre as zonas de nuvem do Cloud Assembly

Zonas de nuvem do Cloud Assembly são seções de recursos de processamento que são específicos para o seu tipo de conta de nuvem, como AWS ou vSphere.

Zonas de nuvem são específicas de uma região, você deve atribuí-las a um projeto. Há uma relação de muitos para muitos entre zonas de nuvem e projetos. O Cloud Assembly tem suporte para implantação nas nuvens públicas mais conhecidas, incluindo Azure, AWS, GCP e vSphere. Consulte [Como adicionar contas de nuvem ao Cloud Assembly](#).

Os controles de colocação adicionais incluem opções de política de colocação, tags de recurso e tags de processamento.

■ Política de colocação

A política de posicionamento orienta a seleção de hosts para implantações na zona de nuvem especificada.

- padrão - Distribui recursos de processamento entre clusters e máquinas de hosts com base na disponibilidade. Por exemplo, todas as máquinas em uma implantação específica são provisionadas no primeiro host aplicável.
- binpack - Coloca recursos de processamento no host mais carregado que possui recursos disponíveis suficientes para executar o processamento fornecido.
- propagação - Provisiona recursos de processamento, em um nível de implantação, para o cluster ou host com o menor número de máquinas virtuais. Para o vSphere, o Distributed Resource Scheduler (DRS) distribui as máquinas virtuais pelos hosts. Por exemplo, todas as máquinas solicitadas em uma implantação são colocadas no mesmo cluster, mas a próxima implementação pode escolher outro cluster vSphere dependendo da carga atual.

Por exemplo, vamos supor que você tenha a seguinte configuração:

- Cluster DRS 1 com 5 máquinas virtuais
- Cluster DRS 2 com 9 máquinas virtuais
- Cluster DRS 3 com 6 máquinas virtuais

Se você solicitar um cluster de 3 máquinas virtuais e selecionar uma política de propagação, elas deverão ser colocadas no cluster 1. As cargas atualizadas se tornam 8 máquinas virtuais para o cluster 1, enquanto as cargas dos clusters 2 e 3 permanecem as mesmas: 9 e 6.

Em seguida, se você solicitar duas máquinas virtuais adicionais, elas serão colocadas no cluster DRS 3, que agora terá 8 máquinas virtuais. A carga dos clusters 1 e 3 permanece a mesma: 8 e 9.

Se duas zonas de nuvem corresponderem a todos os critérios necessários para o provisionamento, a lógica de posicionamento selecionará aquela com maior prioridade.

- **Tags de capacidade**

Os blueprints contêm tags de restrição para ajudar a determinar o posicionamento da implantação. Durante a implantação, tags de restrição de blueprint são mapeadas para tags de capacidade correspondentes em zonas de nuvem e recursos de computação para determinar quais zonas de nuvem estão disponíveis para o posicionamento de recursos de máquina virtual.

- **Cálculo**

É possível visualizar e gerenciar os recursos de processamento que estão disponíveis para provisionar cargas de trabalho, como zonas de disponibilidade da AWS e clusters vCenter, para essa zona de nuvem.

Observação A partir da versão 8.3 do vRealize Automation, as zonas de nuvem não podem mais compartilhar recursos de processamento. Ainda há suporte para as zonas de nuvem herdadas que usam recursos de processamento compartilhados, mas os usuários são solicitados a atualizá-las para conformidade com os padrões atuais.

As zonas de nuvem que são geradas automaticamente durante a criação da conta de nuvem são associadas aos recursos de processamento subjacentes após a coleta de dados.

Se um cluster de processamento vCenter estiver habilitado para DRS, a zona de nuvem só exibirá esse cluster na lista de cálculos e não exibirá os hosts herdeiros. Se um cluster de processamento do vCenter estiver habilitado para DRS, a zona de nuvem apenas exibirá os hosts ESXi independentes, se presentes.

Adicione recursos de processamento conforme apropriado para a zona de nuvem. A guia Processamento contém um mecanismo de filtro que permite que você controle como os recursos de processamento são incluídos com zonas de nuvem. Inicialmente, a seleção do filtro é Incluir todos os processamentos, e a lista abaixo mostra os recursos de processamento disponíveis. Todos eles estão disponíveis para uso em implantações. Você tem duas opções adicionais para adicionar recursos de processamento a uma zona de nuvem.

- **Selecionar o processamento manualmente** – Selecione esta opção se você quiser selecionar manualmente os recursos de processamento na lista abaixo. Depois de selecioná-los, clique em Adicionar processamento para adicionar os recursos à zona. Os recursos selecionados estão disponíveis para uso em implantações.
- **Incluir dinamicamente processamento por tag** - Selecione essa opção se quiser incluir ou excluir recursos de processamento para a zona com base em tags. Todos os recursos de processamento serão mostrados até que você adicione tags apropriadas que correspondam a tags existentes em recursos de processamento. Depois que você adicionar uma ou mais tags, os recursos de processamento com tags que correspondam ao filtro serão incluídos na zona e estarão disponíveis para uso em implantações. Por outro lado, as tags sem correspondência serão excluídas.

Para qualquer uma das opções de processamento, você pode remover um ou mais dos recursos de processamento mostrados na página marcando a caixa à direita e clicando em Remover.

As tags de cálculo ajudam a controlar ainda mais o posicionamento. É possível usar tags para filtrar recursos de processamento disponíveis apenas para aqueles que correspondem a uma ou mais tags, conforme mostrado nos exemplos a seguir.

- Os cálculos não contêm tags e nenhuma filtragem é usada.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags ⓘ

⌵ TAGS

| <input type="checkbox"/> | Name | Account / region | Type | Tags |
|--------------------------|------------|--------------------|-------------------|------|
| <input type="checkbox"/> | us-east-1a | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1b | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1c | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1d | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1e | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1f | Amazon / us-east-1 | Availability Zone | |

6 computes

- Dois cálculos contêm a mesma tag, mas nenhum filtro é usado.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

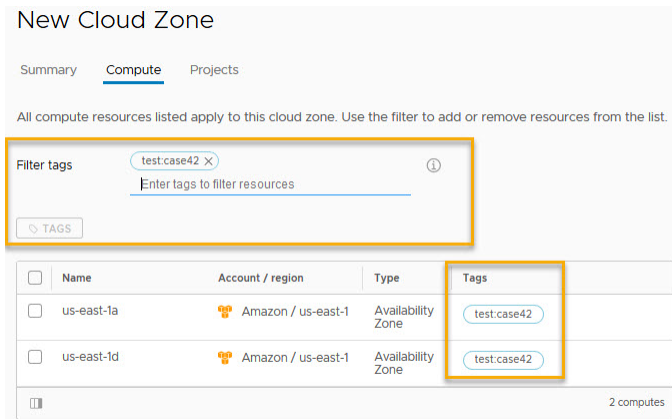
Filter tags ⓘ

⌵ TAGS

| <input type="checkbox"/> | Name | Account / region | Type | Tags |
|--------------------------|------------|--------------------|-------------------|-------------|
| <input type="checkbox"/> | us-east-1a | Amazon / us-east-1 | Availability Zone | test:case42 |
| <input type="checkbox"/> | us-east-1b | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1c | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1d | Amazon / us-east-1 | Availability Zone | test:case42 |
| <input type="checkbox"/> | us-east-1e | Amazon / us-east-1 | Availability Zone | |
| <input type="checkbox"/> | us-east-1f | Amazon / us-east-1 | Availability Zone | |

6 computes

- Dois cálculos contêm a mesma tag e o filtro de tag corresponde à tag usada nos dois cálculos.



■ Projetos

É possível ver quais projetos foram configurados para oferecer suporte ao provisionamento de carga de trabalho para essa zona de nuvem.

Depois de criar uma zona de nuvem, pode-se validar sua configuração.

Painel Insights

Se você tiver um aplicativo do vRealize Operations Manager associado que tenha sido configurado para trabalhar com o vRealize Automation, será possível acessar um painel **Insights** na zona de nuvem. Esse painel exibe informações relacionadas a capacidade sobre recursos e implantações para a zona de nuvem do vSphere ou VMware Cloud on AWS, desde que as contas de nuvem estejam configuradas tanto no vRealize Automation quanto no vRealize Operations Manager e estejam sendo monitoradas no vRealize Operations Manager. Para saber mais sobre o painel **Insights**, consulte [Gerenciamento de recursos e otimização de implantação usando métricas do vRealize Operations Manager no vRealize Automation](#).

Como adicionar mapeamentos de tipos no vRealize Automation para especificar dimensionamentos de máquinas comuns

Um mapa de tipo do vRealize Automation é onde se usa o idioma natural para definir tamanhos de implantação de destino para uma conta/região de nuvem específica.

Os mapas de tipo expressam os tamanhos de implantação que fazem sentido para o ambiente. Um exemplo pode ser *small* para 1 CPU e 2 GB de memória e *large* para 2 CPUs e 8 GB de memória para uma conta do vCenter em um centro de dados nomeado e t2.nano para uma conta do Amazon Web Services em uma região nomeada.

Selecione **Gerenciamento de Tenants > Mapeamentos de Tipos** ou **Infraestrutura > Mapeamentos de Tipos** e clique em **Novo Mapeamento de Tipos**.

Saiba mais sobre mapeamentos de tipo no vRealize Automation

Um mapeamento de tipo agrupa um conjunto de dimensionamentos de implantação de destino para uma conta/região de nuvem específica no vRealize Automation usando nomenclatura do idioma natural.

O mapeamento de tipo permite criar um mapeamento nomeado que contenha dimensionamentos de tipo semelhantes nas suas regiões de conta. Por exemplo, um mapa de tipo nomeado `standard_small` pode conter um tamanho de tipo semelhante (como 1 CPU, 2 GB de RAM) para algumas ou todas as regiões/contas disponíveis no seu projeto. Quando você compila um modelo de nuvem, você escolhe um tipo disponível que atenda às suas necessidades.

Organize os mapeamentos de tipo para seu projeto por objetivo de implantação.

Para simplificar a criação do modelo de nuvem, você poderá selecionar uma opção de pré-configuração quando adicionar uma nova conta de nuvem. Quando você seleciona a opção de pré-configuração, serão selecionados o mapeamento de tipo e o mapeamento de imagem mais populares da organização para a região especificada.

Com relação ao mapeamento de imagem em modelos de nuvem que contenham recursos do vSphere, se não houver mapeamentos de tipo definidos para uma zona de nuvem do vSphere, você poderá configurar a memória e a CPU ilimitadas usando as configurações específicas do vSphere no modelo de nuvem. Se houver mapeamentos de tipo definidos para uma zona de nuvem vSphere, o mapeamento de tipos servirá como um limite para configurações do vSphere específicas no modelo de nuvem.

Como adicionar mapeamentos de imagem no vRealize Automation para acessar sistemas operacionais comuns

Um mapa de imagem do vRealize Automation é onde se usa o idioma natural para definir sistemas operacionais de implantação de destino para uma conta/região de nuvem específica.

Selecione **Gerenciamento de Tenants > Mapeamentos de Imagens** e clique em **Novo Mapeamento de Imagens**.

Create Image Mapping

Account / region *

Image name *

Image *

Constraints

Tenant *

Cloud configuration

| | |
|---|--|
| 1 | |
|---|--|

Saiba mais sobre mapeamentos de imagem no vRealize Automation

Um mapeamento de imagem agrupa um conjunto de especificações predefinidas do sistema operacional de destino para uma conta/região de nuvem específica no vRealize Automation usando a nomenclatura do linguagem natural.

As contas de fornecedores de nuvem, como o Microsoft Azure e o Amazon Web Services usam imagens para agrupar um conjunto de condições de implantação de destino, incluindo o SO e as definições de configuração relacionadas. Os ambientes baseados em vCenter e NSX, incluindo o VMware Cloud on AWS, usam um mecanismo de agrupamento semelhante para definir um conjunto de condições de implantação do sistema operacional. Quando você compila e finalmente implanta e itera um modelo de nuvem, escolha uma imagem disponível que melhor atenda às suas necessidades.

Organize os mapeamentos de imagem para um projeto por configurações semelhantes do sistema operacional, estratégia de marcação e objetivo funcional da implantação.

Para simplificar a criação do modelo de nuvem, você poderá selecionar uma opção de pré-configuração quando adicionar uma nova conta de nuvem. Quando você seleciona a opção de pré-configuração, serão selecionados o mapeamento de tipo e o mapeamento de imagem mais populares da organização para a região especificada.

Ao adicionar informações de imagem a um modelo de nuvem, você usa a entrada `image` ou `imageRef` na seção `properties` de um componente de máquina. Por exemplo, se deseja clonar de um snapshot, use a propriedade `imageRef`.

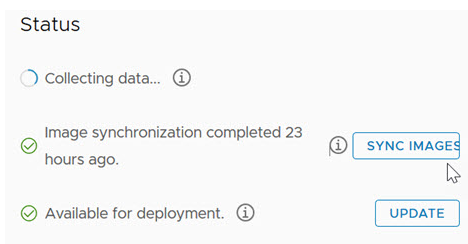
Para exemplos de entradas `image` e `imageRef` no código do modelo de nuvem, consulte [Capítulo 6 Como projetar suas implantações do Cloud Assembly](#).

Para atribuir uma permissão em uma biblioteca de conteúdo, um administrador deve conceder a permissão ao usuário como uma permissão global. Para obter informações relacionadas, consulte [Herança hierárquica de permissões para bibliotecas de conteúdo](#), em *Administração de máquinas virtuais vSphere*, na [Documentação do VMware vSphere](#).

Sincronizando imagens para a conta/região de nuvem

Você pode executar a sincronização de imagens para garantir que as imagens que está adicionando ou removendo para uma determinada conta/região de nuvem na página **Infraestrutura > Configurar > Mapeamento de Imagens** sejam atuais.

- 1 Abra a **Conta/Região de Nuvem** associada selecionando **Infraestrutura > Conexões > Contas de nuvem**. Selecione a conta/região de nuvem existente.
- 2 Clique no botão **Sincronizar Imagens** e deixe a ação ser concluída.



- 3 Quando a ação estiver concluída, clique em **Infraestrutura > Configurar > Mapeamento de Imagens**. Defina um novo mapeamento de imagem ou edite um existente e selecione a conta/região de nuvem da etapa 1.
- 4 Clique no ícone de sincronização de imagem na página **Mapeamento de Imagens**.



- 5 Defina as configurações de mapeamento de imagens para a conta/região de nuvem especificada na página **Mapeamento de Imagens**.

Como exibir detalhes do OVF

É possível incluir especificações do OVF em objetos de modelo de nuvem do Cloud Assembly, como componentes de máquina e mapas de imagem do vCenter. Se a imagem contiver um arquivo OVF, será possível descobrir seu conteúdo sem abrir o arquivo. Passe o cursor sobre o OVF para exibir os detalhes do OVF, incluindo nome e local. Para obter mais informações sobre o formato de arquivo OVF, consulte [vcenter ovf: property](#). "Para exibir os detalhes do OVF, o mapeamento de imagem deve residir no servidor Web."



Para obter informações relacionadas sobre como visualizar detalhes do OVF usando um link do OVF no campo de mapeamento, consulte o artigo [Modelo de nuvem de um OVA](#).

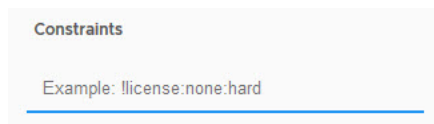
Usando imagens compartilhadas e mais recentes de uma galeria de imagens do Microsoft Azure

Ao criar mapeamentos de imagens para o Microsoft Azure, você pode selecionar imagens de uma galeria de imagens compartilhada do Azure na assinatura. As imagens no menu suspenso são coletadas por dados e disponibilizadas com base na região selecionada.

Embora as galerias de imagens compartilhadas possam ser usadas em várias assinaturas, elas não podem ser listadas no menu suspenso de mapeamento de imagens entre assinaturas. Apenas as imagens de uma assinatura específica são coletadas por dados e apresentadas na lista de mapeamentos de imagens. Para usar uma imagem de uma galeria de imagens em uma assinatura diferente, forneça o ID da imagem no mapeamento de imagens e use esse mapeamento de imagens no modelo de nuvem.

Como usar restrições e tags para refinar a seleção da imagem

Para refinar ainda mais a seleção de imagem em um modelo de nuvem, é possível adicionar uma ou mais restrições para especificar restrições com base em tag no tipo de imagem que pode ser implantada. O exemplo de **Restrições** fornecido que é exibido quando você está criando ou editando uma configuração de mapeamento de imagem é `!license:none:hard`. Esse exemplo ilustra uma restrição baseada em tag onde a imagem só poderá ser usada se a tag `license:none` não estiver presente no modelo de nuvem. Ao adicionar tags como `license:88` e `license:92`, a imagem especificada poderá ser usada somente se as tags `license:88` e `license:92` *estiverem* presentes no modelo de nuvem.



Como usar um script de configuração de nuvem para controlar a implantação

É possível usar um script de configuração de nuvem em um mapa de imagem, modelo de nuvem ou ambos para definir características de sistema operacional personalizadas a serem usadas em uma implantação do Cloud Assembly. Por exemplo, baseado na escolha de implantação de um modelo de nuvem em uma nuvem pública ou privada, é possível aplicar permissões de usuário específicas, permissões de SO ou outras condições à imagem. Um script de configuração de nuvem adere a um formato `cloud-init` para imagens baseadas no Linux ou a um formato `cloudbase-init` para imagens baseadas no Windows. O Cloud Assembly oferece suporte à ferramenta [cloud-init](#) para sistemas Linux e à ferramenta [cloudbase-init](#) para Windows.

Para máquinas Windows, é possível usar qualquer formato de script de configuração de nuvem compatível com `cloudbase-init`.

O recurso de máquina no seguinte código de modelo de nuvem de amostra usa uma imagem que contém um script de configuração da nuvem, cujo o conteúdo é visto na entrada `image`.

```
resources:
  demo-machine:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      image: MyUbuntu16
      https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ami-ubuntu-16.04-1.10.3-00-15269239.ova
      cloudConfig: |
        ssh_pwauth: yes
        chpasswd:
          list: |
            ${input.username}:${input.password}
          expire: false
        users:
          - default
          - name: ${input.username}
            lock_passwd: false
            sudo: ['ALL=(ALL) NOPASSWD:ALL']
            groups: [wheel, sudo, admin]
            shell: '/bin/bash'
      runcmd:
        - echo "Defaults:${input.username} !requiretty" >> /etc/sudoers.d/${input.username}
```

A avaliação de propriedades dinâmicas funciona ao usar o `cloudConfig` diretamente em um modelo de nuvem, mas não tem suporte com o `cloudConfig` em um mapa de imagem.

No código do modelo de nuvem, você usa a configuração `image` para fazer referência a uma imagem que é definida como um mapeamento de imagem. Use a configuração `imageRef` para identificar um modelo que contém um snapshot (para clones vinculados), um modelo de imagem ou um modelo de biblioteca de conteúdo OVF.

O que acontece quando um mapeamento de imagem e um modelo de nuvem contêm um script de configuração de nuvem

Quando um modelo de nuvem que contém um script de configuração de nuvem usa um mapeamento de imagem que contém um script de configuração de nuvem, ambos os scripts são combinados. A ação de mesclagem processa o conteúdo do script de mapeamento de imagem primeiro e o conteúdo do script de modelo de nuvem em seguida, considerando se os scripts estão no formato `#cloud-config` ou não.

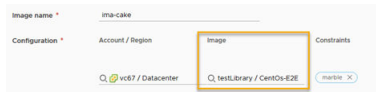
- Para scripts que estão no formato `#cloud-config`, a mesclagem combina o conteúdo de cada módulo (por exemplo `runcmd`, `users` e `write_files`) do seguinte modo:
 - Para módulos em que o conteúdo é uma lista, as listas de comandos do mapeamento de imagem e do modelo de nuvem são mescladas, excluindo comandos que são idênticos em ambas as listas.

- Para módulos em que o conteúdo é um dicionário, os comandos são mesclados, e o resultado é uma combinação dos dois dicionários. Se a mesma chave existir em ambos os dicionários, a chave do dicionário do script de mapeamento de imagem será preservada, e a chave do dicionário do script de modelo de nuvem será ignorada.
- Para módulos em que o conteúdo é uma cadeia de caracteres, os valores de conteúdo do script de mapeamento de imagem são mantidos, e os valores de conteúdo do script de modelo de nuvem são ignorados.
- Para scripts que estão em um formato diferente de `#cloud-config` ou quando um script está no formato `#cloud-config` e o outro não, ambos os scripts são combinados de forma que o script de mapeamento de imagem seja executado primeiro e o script de modelo de nuvem seja executado quando o script de mapeamento de imagem for concluído.

Para obter informações relacionadas, consulte [Mesclando seções de dados de usuários](#).

Adicionar uma imagem de uma biblioteca de conteúdo do vCenter

Quando uma biblioteca de conteúdo local ou de editor reside em um vCenter gerenciado pela sua organização do vRealize Automation, as imagens do modelo da biblioteca de conteúdo aparecem no menu suspenso de imagens. As imagens listadas incluem imagens de modelo OVF e VM no local ou bibliotecas de conteúdo do vCenter de editores. Imagens em bibliotecas de conteúdo de assinantes não aparecem no menu suspenso. O modelo do qual uma VM foi clonada é mostrado na seção de detalhes da máquina da interface do usuário de implantações da máquina.



Observação Se a biblioteca de conteúdo do vCenter for gerenciada pelo vRealize Automation, as informações do editor serão exibidas na grade de seleção de mapeamento de imagem no seguinte formato: *publisher_content_library_name / content_item_name*

Para atribuir uma permissão em uma biblioteca de conteúdo, um administrador deve conceder a permissão ao usuário como uma permissão global. Para obter informações relacionadas, consulte [Herança hierárquica de permissões para bibliotecas de conteúdo](#), em *Administração de máquinas virtuais vSphere*, na [Documentação do VMware vSphere](#).

Se a biblioteca de conteúdo de editor do vCenter não for gerenciada pelo vRealize Automation, as informações do assinante serão exibidas na grade de seleção de mapeamento de imagens no seguinte formato: *subscriber_content_library_name / content_item_name*

Por exemplo, no cenário a seguir, apenas os itens da biblioteca de conteúdo do assinante estão visíveis na lista de mapeamentos de imagens do vRealize Automation:

- Para um vCenter denominado VC-1, há uma biblioteca de conteúdo do assinante no VC, e é criada uma conta de nuvem no vRealize Automation que é associada a VC-1.
- Para um vCenter denominado VC-2, há uma biblioteca de conteúdo do editor no VC do qual a biblioteca de conteúdo do assinante de VC-1 é assinada. No entanto, não há conta de nuvem no vRealize Automation associada a VC-2.

Como VC-1 está associado a uma conta de nuvem do vRealize Automation, a biblioteca de conteúdo do assinante está disponível no vRealize Automation. Seu conteúdo é coletado e exibido na lista de mapeamentos de imagens do vRealize Automation. No entanto, como VC-2 não está associado a uma conta de nuvem, o vRealize Automation não tem conhecimento de sua biblioteca de conteúdo do editor. Para exibir os itens da biblioteca de conteúdo do editor na lista de mapeamento de imagens, você deve associar uma conta de nuvem ao vCenter VC-2.

Quando você implanta um modelo de nuvem que contém um mapeamento de imagem de modelo de VM, o vRealize Automation tenta acessar a imagem mapeada na biblioteca de conteúdo que está mais próxima do armazenamento de dados e, em seguida, mais próxima do host da máquina a ser provisionada. Isso pode incluir uma biblioteca de conteúdo local, bem como uma biblioteca de conteúdo de editor ou assinante.

Quando você implanta um modelo de nuvem que contém um mapeamento de imagem de modelo OVF, as imagens OVF serão acessadas conforme especificado na linha de mapeamento de imagem se a imagem estiver em uma biblioteca de conteúdo local ou um assinante local de uma biblioteca de conteúdo de editor remoto especificada.

Para obter informações relacionadas sobre a criação e o uso de bibliotecas de conteúdo do vCenter, consulte (em inglês) [Using Content Libraries](#) na [Documentação do produto vSphere](#) e a postagem no blog [How to Use Content Libraries in vRealize Automation 8 and vRealize Automation Cloud](#).

Mais informações sobre como configurar e usar scripts de configuração de nuvem

Para obter mais informações sobre como trabalhar com scripts de configuração de nuvem em modelos de nuvem, consulte [Inicialização de máquinas no Cloud Assembly](#).

Consulte também os artigos do blog da VMware (em inglês): [vSphere Customization with Cloud-init While Using vRealize Automation 8 or Cloud](#) e [Customizing Cloud Assembly Deployments with Cloud-Init](#).

Como adicionar perfis de rede no vRealize Automation

Um perfil de rede do vRealize Automation descreve o comportamento da rede a ser implantada.

Por exemplo, uma rede pode precisar ser voltada para a Internet, em vez de ser somente interna.

Redes e perfis de rede são específicos da nuvem.

Selecione **Infraestrutura > Configurar > Perfis de Rede** e clique em **Novo Perfil de Rede**.

Saiba mais sobre perfis de rede no vRealize Automation

Um perfil de rede define um grupo de redes e configurações de rede que estão disponíveis para uma conta de nuvem em uma determinada região ou centro de dados no vRealize Automation.

Geralmente, são definidos perfis de rede para oferecer suporte a um ambiente de implantação de destino, por exemplo, um ambiente de teste pequeno no qual uma rede existente tem apenas acesso de saída ou um ambiente de produção balanceado por carga que precisa de um conjunto de políticas de segurança. Imagine um perfil de rede como uma coleção de características de rede específicas da carga de trabalho.

O que há em um perfil de rede

Um perfil de rede contém informações específicas para um tipo de conta de nuvem nomeada e uma região no vRealize Automation, incluindo as seguintes configurações:

- Conta/região de nuvem nomeada e tags de capacidade opcionais para o perfil de rede.
- Redes existentes nomeadas e suas configurações.
- Políticas de rede que definem o aspecto sob demanda e outros aspectos do perfil de rede.
- Inclusão opcional de balanceadores de carga existentes.
- Inclusão opcional de grupos de segurança existentes.

Você determina a funcionalidade do gerenciamento de IPs da rede com base no perfil da rede.

Tags de capacidade do perfil de rede são combinadas com tags de restrição em modelos de nuvem para ajudar a controlar a seleção da rede. Além disso, todas as tags atribuídas às redes coletadas pelo perfil de rede também são correspondidas com tags no modelo de nuvem para ajudar a controlar a seleção da rede quando o modelo de nuvem é implantado.

As tags de capacidade são opcionais. Tags de capacidade são aplicadas a todas as redes no perfil de rede, mas somente quando as redes são usadas como parte desse perfil de rede. Para perfis de rede que não contêm tags de capacidade, a correspondência de tag ocorre apenas nas tags de rede. As configurações de rede e segurança definidas no perfil de rede correspondente são aplicadas quando o modelo de nuvem é implantado.

Ao usar um IP estático, o intervalo de endereços é gerenciado pelo vRealize Automation. Para o DHCP, os endereços IP iniciais e finais são gerenciados pelo servidor DHCP independente, e não pelo vRealize Automation. Ao usar o DHCP ou a alocação de endereços de rede mistos, o valor de utilização da rede é definido como zero. Um intervalo alocado de rede sob demanda é baseado no CIDR e no tamanho da sub-rede especificados no perfil da rede. Para oferecer suporte à atribuição estática e dinâmica na implantação, o intervalo alocado é dividido em dois intervalos: um para alocação estática e outro para alocação dinâmica.

Redes

As redes, também conhecidas como sub-redes, são subdivisões lógicas de uma rede IP. Uma rede agrupa uma conta de nuvem, um endereço IP ou um intervalo e tags de rede para controlar como e onde provisionar uma implantação de modelo de nuvem. Os parâmetros de rede no perfil definem como as máquinas na implantação podem se comunicar umas com as outras pela camada de IP 3. As redes podem ter tags.

Você pode adicionar redes ao perfil de rede, editar aspectos de redes que são usados pelo perfil de rede e remover redes do perfil de rede.

Ao adicionar uma rede ao perfil de rede, você pode selecionar as redes disponíveis em uma lista filtrada de redes do vSphere e do NSX. Se o tipo de rede for compatível com o tipo de conta de nuvem, você poderá adicioná-lo ao perfil de rede.

Em uma implantação baseada em VCF, os segmentos de rede do NSX são criados localmente na rede do NSX-T, eles não são criados como redes globais.

■ Domínio de rede ou Zona de transporte

Um domínio de rede ou zona de transporte é o comutador virtual distribuído (dvSwitch) para o vSphere vNetwork Distributed PortGroups (dvPortGroup). Uma *zona de transporte* é um conceito existente do NSX que é semelhante a termos como *dvSwitch* ou *dvPortGroup*.

Ao usar uma conta de nuvem do NSX, o nome do elemento na página é **Zona de transporte**. Caso contrário, é **Domínio de rede**.

Para comutadores padrão, o domínio de rede ou zona de transporte é idêntico ao próprio comutador. O domínio de rede ou a zona de transporte define os limites das sub-redes dentro do vCenter.

Uma zona de transporte controla quais hosts um comutador lógico do NSX pode acessar. Ele pode abranger um ou mais clusters vSphere. Zonas de transporte controlam quais clusters e quais máquinas virtuais podem participar do uso de uma rede específica. Sub-redes que pertencerem à mesma zona de transporte do NSX podem ser usadas para os mesmos hosts de máquina.

- **Domínio**

Representa o nome de domínio da máquina. O nome de domínio é transmitido para a especificação de personalização da máquina vSphere.

- **CIDR IPv4 e gateway padrão IPv4**

Os componentes de máquina do vSphere no modelo de nuvem oferecem suporte para IPv4, IPv6 e atribuição de IP de pilha dupla para interfaces de rede. Por exemplo: 192.168.100.14/24 representa o endereço IPv4 192.168.100.14 e seu prefixo de roteamento associado 192.168.100.0, ou de forma equivalente, sua máscara de sub-rede 255.255.255.0 que tem 1 bit de entrelinhamento 24. O bloco IPv4 192.168.100.0/22 representa os 1024 endereços IP do 192.168.100.0 para o 192.168.103.255.

- **CIDR IPv6 e gateway padrão IPv6**

Os componentes de máquina do vSphere no modelo de nuvem oferecem suporte para IPv4, IPv6 e atribuição de IP de pilha dupla para interfaces de rede. Por exemplo, 2001:db8::/48 representa o bloco de endereços IPv6 de 2001:db8:0:0:0:0:0:0 a 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

O formato IPv6 não tem suporte com redes sob demanda.

- **Servidores DNS e Domínios de pesquisa de DNS**

- **Suportar IP público**

Selecione essa opção para sinalizar a rede como pública. Os componentes de rede em um modelo de nuvem que têm uma propriedade `network type: public` correspondem às redes que estão sinalizadas como públicas. Outras correspondências ocorrem durante a implantação do modelo de nuvem para determinar a seleção da rede.

- **Padrão para zona**

Selecione essa opção para sinalizar a rede como padrão para a zona da nuvem. Durante a implantação de modelo de nuvem, as redes padrão são preferidas sobre outras redes.

- **Origem**

Identifica a fonte da rede.

- **Tags**

Especifica uma ou mais tags atribuídas à rede. As tags são opcionais. A correspondência de tags afeta quais redes estão disponíveis para suas implantações de modelo de nuvem.

As tags de rede existem no próprio item de rede, independentemente do perfil de rede. As tags de rede se aplicam a todas as ocorrências da rede que foram adicionadas a todos os perfis de rede que contenham essa rede. As redes podem ser modeladas em qualquer número de perfis de rede. Independentemente da residência do perfil de rede, uma tag de rede será associada a essa rede onde quer que a rede seja usada.

Ao implantar um modelo de nuvem, tags de restrição nos componentes de rede de um modelo de nuvem são correspondidas a tags de rede, incluindo tags de capacidade de perfil de rede. Para perfis de rede que contêm tags de capacidade, estas são aplicadas a todas as redes que estão disponíveis para esse perfil de rede. As configurações de rede e segurança definidas no perfil de rede correspondente são aplicadas quando o modelo de nuvem é implantado.

Políticas de rede

Usando perfis de rede, você pode definir sub-redes para domínios de rede existentes que contêm configurações de endereço IP estático, DHCP ou uma mistura de configurações de endereço IP estático e DHCP. Você pode definir sub-redes e especificar configurações de endereço IP usando a guia **Políticas de Rede**.

Ao usar o NSX-V, o NSX-T ou o VMware Cloud on AWS, as configurações de política de rede são usadas quando um modelo de nuvem requer `networkType: outbound` OU `networkType: private` ou quando uma rede NSX requer `networkType: routed`.

Dependendo da conta de nuvem associada, você pode usar políticas de rede para definir configurações para os tipos de rede `outbound`, `private` e `routed` e para grupos de segurança sob demanda. Você também pode usar políticas de rede para controlar redes `existing` quando há um balanceador de carga associado a essa rede.

As redes de saída permitem um acesso unidirecional a redes de upstream. As redes privadas não permitem qualquer acesso externo. As redes roteadas permitem tráfego leste/oeste entre as redes roteadas. As redes existentes e públicas nesse perfil são usadas como as redes subjacentes ou upstream.

As opções para as seguintes seleções sob demanda estão descritas na ajuda na tela sobre **Perfis de rede** e são resumidas abaixo.

- **Não criar rede sob demanda ou grupo de segurança sob demanda**

É possível usar essa opção ao especificar um tipo de rede `existing` ou `public`. Modelos de nuvem que exigem uma rede `outbound`, `private` ou `routed` não são correspondidos a esse perfil.

- **Criar uma rede sob demanda**

É possível usar essa opção ao especificar um tipo de rede `outbound`, `private` ou `routed`.

A Amazon Web Services, o Microsoft Azure, o NSX, o vSphere e o VMware Cloud on AWS oferecem suporte para essa opção.

- **Criar um grupo de segurança sob demanda**

É possível usar essa opção ao especificar um tipo de rede `outbound` ou `private`.

Um novo grupo de segurança será criado para modelos de nuvem correspondentes se o tipo de rede for `outbound` ou `private`.

A Amazon Web Services, o Microsoft Azure, o NSX e o VMware Cloud on AWS oferecem suporte para essa opção.

As configurações de políticas de rede podem ser específicas para o tipo de conta na nuvem. Essas configurações são descritas na ajuda de sinalização na tela e resumidas abaixo:

- **Domínio de rede ou Zona de transporte**

Um domínio de rede ou zona de transporte é o comutador virtual distribuído (dvSwitch) para o vSphere vNetwork Distributed PortGroups (dvPortGroup). Uma *zona de transporte* é um conceito existente do NSX que é semelhante a termos como *dvSwitch* ou *dvPortGroup*.

Ao usar uma conta de nuvem do NSX, o nome do elemento na página é **Zona de transporte**. Caso contrário, é **Domínio de rede**.

Para comutadores padrão, o domínio de rede ou zona de transporte é idêntico ao próprio comutador. O domínio de rede ou a zona de transporte define os limites das sub-redes dentro do vCenter.

Uma zona de transporte controla quais hosts um comutador lógico do NSX pode acessar. Ele pode abranger um ou mais clusters vSphere. Zonas de transporte controlam quais clusters e quais máquinas virtuais podem participar do uso de uma rede específica. Sub-redes que pertencerem à mesma zona de transporte do NSX podem ser usadas para os mesmos hosts de máquina.

- **Sub-rede externa**

Uma rede sob demanda com acesso de saída requer uma sub-rede externa que tenha acesso de saída. A sub-rede externa é usada para fornecer acesso de saída se solicitado no modelo de nuvem — ela não controla o posicionamento da rede. Por exemplo, a sub-rede externa não afeta o posicionamento de uma rede privada.

- **CIDR**

A notação CIDR é uma representação compacta de um endereço IP e do seu prefixo de roteamento associado. O valor de CIDR especifica o intervalo de endereços de rede a ser usado durante o provisionamento para criar sub-redes. Essa configuração de CIDR na guia **Políticas de Rede** aceita a notação IPv4 que termina em /nn e contém valores entre 0 e 32.

- **Tamanho da sub-rede**

Essa opção especifica o tamanho da rede sob demanda, usando notação IPv4, para cada rede isolada em uma implantação que usa esse perfil de rede. A configuração do tamanho da sub-rede está disponível para gerenciamento de endereço IP interno ou externo.

O formato IPv6 não tem suporte com redes sob demanda.

- **Roteador lógico distribuído**

Para uma rede roteada sob demanda, você deve especificar uma rede lógica distribuída ao usar uma conta de nuvem do NSX-V.

Um roteador lógico distribuído (DLR) é usado para rotear o tráfego leste/oeste entre redes roteadas sob demanda no NSX-V. Essa opção só estará visível se o valor de conta/região para o perfil de rede estiver associado a uma conta de nuvem do NSX-V.

■ **Atribuição de intervalo de IPs**

Essa opção está disponível para contas de nuvem que oferecem suporte ao NSX ou ao VMware Cloud on AWS, incluindo o vSphere.

A configuração de intervalo de IPs está disponível ao usar uma rede existente com um ponto de integração de IPAM externo.

Você pode selecionar uma das três opções a seguir para especificar um tipo de atribuição de intervalo de IPs para a rede de implantação:

■ **Estático e DHCP**

Padrão e recomendado. Essa opção mista usa as configurações alocadas de **CIDR** e **Intervalo de sub-redes** para configurar o pool de servidores DHCP para oferecer suporte à metade da alocação do espaço de endereços usando o método DHCP (dinâmico) e à metade da alocação do espaço de endereços IP usando o método Estático. Use essa opção quando algumas das máquinas que estão conectadas a uma rede sob demanda exigem endereços IP estáticos atribuídos e outras exigem endereços IP dinâmicos. Dois intervalos de IP são criados.

Essa opção é mais eficaz em implantações com máquinas que estão conectadas a uma rede sob demanda, em que algumas das máquinas são recebem IPs estáticos e outras máquinas têm IPs atribuídos dinamicamente por um servidor DHCP do NSX e implantações em que o VIP do balanceador de carga é estático.

■ **DHCP (dinâmico)**

Essa opção usa o CIDR alocado para configurar um pool de IPs em um servidor DHCP. Todos os endereços IP para essa rede são atribuídos dinamicamente. Um único intervalo de IPs é criado para cada CIDR alocado.

■ **Estático**

Essa opção usa o CIDR alocado para alocar endereços IP estaticamente. Use-a quando um servidor DHCP não precisa ser configurado para esta rede. Um único intervalo de IPs é criado para cada CIDR alocado.

■ **Blocos de IP**

A configuração de blocos de IPs está disponível ao usar uma rede sob demanda com um ponto de integração de IPAM externo.

Usando a configuração de blocos de IP, é possível adicionar um bloco de IPs nomeado, ou intervalo, ao perfil de rede do seu provedor de IPAM externo integrado. Você também pode remover um bloco de IP adicionado do perfil de rede. Para obter informações sobre como criar uma integração de IPAM externo, consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).

O IPAM externo está disponível para os seguintes tipos de conta/região de nuvem:

- vSphere
- vSphere com NSX-T
- vSphere com NSX-V

■ Recursos de Rede - Rede externa

Redes externas também são chamadas de redes existentes. Essas redes são coletadas por dados e disponibilizadas para seleção.

■ Recursos de Rede - Roteador lógico de camada 0

O NSX-T usa o roteador lógico de camada 0 como gateway para redes externas à implantação do NSX. O roteador lógico de camada 0 configura o acesso de saída para redes sob demanda.

■ Recursos de Rede - Edge Cluster

O cluster de borda especificado fornece serviços de roteamento. O cluster de borda é usado para configurar o acesso de saída para redes sob demanda e balanceadores de carga. Ele identifica o cluster de borda ou o pool de recursos no qual o dispositivo de borda deve ser implantado.

■ Recursos de Rede - Repositório de dados de borda

O repositório de dados de borda especificado é usado para provisionar o dispositivo de borda. Essa configuração aplica-se somente ao NSX-V.

Tags podem ser usadas para especificar quais redes estão disponíveis para o modelo de nuvem.

Balanceadores de carga

Você pode adicionar balanceadores de carga ao perfil de rede. Os balanceadores de carga listados estão disponíveis com base nas informações coletadas por dados da conta de nuvem de origem.

Se uma tag em qualquer um dos balanceadores de carga no perfil de rede corresponder a uma tag em um componente de balanceador de carga no modelo de nuvem, o balanceador de carga será levado em consideração durante a implantação. Os balanceadores de carga em um perfil de rede correspondido são usados quando um modelo de nuvem é implantado.

Para obter mais informações, consulte [Usando configurações de balanceador de carga em perfis de rede no vRealize Automation](#) e [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Grupos de segurança

Quando um modelo de nuvem é implantado, os grupos de segurança em seu perfil de rede são aplicados às NICs de máquina que são provisionadas. Para um perfil de rede específico do Amazon Web Services, os grupos de segurança no perfil de rede estão disponíveis no mesmo domínio de rede (VPC) que as redes listadas na guia Redes. Se o perfil de rede não tiver redes listadas na guia Redes, todos os grupos de segurança disponíveis serão exibidos.

Você pode usar um grupo de segurança para definir ainda mais as configurações de isolamento para uma rede `private` ou `outbound` sob demanda. Grupos de segurança também são aplicados a redes `existing`. Você também pode atribuir grupos de segurança globais.

Os grupos de segurança listados estão disponíveis com base nas informações coletadas por dados da conta de nuvem de origem ou adicionadas como um grupo de segurança sob demanda em um modelo de nuvem de projeto. Para obter mais informações, consulte [Recursos de segurança no vRealize Automation](#).

Os grupos de segurança são aplicados a todas as máquinas na implantação que estão conectadas à rede que corresponde ao perfil de rede. Como pode haver várias redes em um modelo de nuvem, cada uma correspondendo a um perfil de rede diferente, é possível usar diferentes grupos de segurança para diferentes redes.

Observação Além de especificar um grupo de segurança, você também pode selecionar redes (padrão) do NSX, redes do vSphere ou ambas. Quando você implanta um modelo de nuvem, o vRealize Automation adiciona o grupo de segurança alocado ou especificado aos NICs de máquina que estão conectados à rede alocada do NSX. Somente os NICs de máquina que estão conectados a uma rede do NSX podem ser adicionados a um grupo de segurança do NSX. Se o NIC da máquina estiver conectado a uma rede do vSphere, haverá falha na implantação do modelo.

Adicionar uma tag a um grupo de segurança existente permite que você use esse grupo de segurança em um componente `Cloud.SecurityGroup` de modelo de nuvem. Um grupo de segurança deve ter pelo menos uma tag ou não poderá ser usado em um modelo de nuvem. Para obter mais informações, consulte [Recursos de segurança no vRealize Automation](#) e [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Mais informações sobre perfis de rede, redes, modelos de nuvem e tags

Para obter mais informações sobre redes, consulte [Recursos de rede no vRealize Automation](#).

Para obter exemplos de amostras de código de componentes de rede em um modelo de nuvem, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Para obter exemplos de fluxos de trabalho de automação de rede, consulte [Network Automation com o Cloud Assembly](#) e o NSX.

Para obter mais informações sobre tags e estratégia de marcação, consulte [Como usar tags para gerenciar recursos e implantações do Cloud Assembly](#).

Para obter informações sobre como nomear NICs de máquina, consulte [Como posso configurar um nome de controlador de interface de rede usando ações de extensibilidade](#).

Como usar as configurações de rede em perfis de rede e modelos de nuvem no vRealize Automation

Você usa redes e perfis de rede no vRealize Automation para ajudar a definir o comportamento do provisionamento de rede para suas implantações.

No vRealize Automation, é possível definir perfis de rede específicos da nuvem. Consulte [Saiba mais sobre perfis de rede no vRealize Automation](#).

Usando as configurações de rede e de perfil de rede, é possível controlar como os endereços IP de rede são usados em modelos de nuvem e implantações do vRealize Automation.

Suporte para IPv4 e IPv6 em redes do vRealize Automation

As redes do vRealize Automation oferecem suporte para IPv4 de pilha única, IPv6 de pilha única ou IPv4 e IPv6 de pilha dupla.

O IPv6 não é compatível com redes do vSphere e do NSX existentes.

O IPv6 não é compatível com balanceadores de carga, redes sob demanda do NSX ou provedores de IPAM externos, como o Infoblox.

Suporte para provedores de IPAM externos

Além do suporte de IPAM interno fornecido, você pode usar um provedor de IPAM externo para alocar dinamicamente ou estaticamente o endereço IP para redes – como intervalos de IP para redes existentes em seus designs/implantações de modelo de nuvem e blocos de IP para redes sob demanda em seus designs/implantações de modelo de nuvem.

O suporte para provedores de IPAM externos, como o Infoblox, está disponível para pontos de integração de IPAM específicos do fornecedor que você cria usando a sequência de menu **Infraestrutura > Conexões > Adicionar Integração > IPAM**.

As opções para definir as informações de endereço do provedor de IPAM externo estão disponíveis por meio da opção **Adicionar intervalo de IP IPAM** na página **Políticas de rede > Adicionar intervalo de IP IPAM**.

Para obter informações sobre como criar um ponto de integração de IPAM externo, consulte [Como configurar uma integração externa de IPAM no vRealize Automation](#). Para obter um exemplo de como criar um ponto de integração de IPAM para um fornecedor de IPAM específico, consulte [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#).

Tipos de rede

Um componente de rede em um modelo de nuvem é definido como um dos tipos `networkType` a seguir.

| Tipo de rede | Definição |
|-----------------------|---|
| <code>existing</code> | <p>Seleciona uma rede existente que esteja configurada no provedor de nuvem subjacente, como vCenter, Amazon Web Services e Microsoft Azure. Uma rede existente é exigida pela rede do <code>outbound</code> sob demanda.</p> <p>É possível definir um intervalo de endereços IP estáticos em uma rede existente.</p> |
| <code>public</code> | <p>As máquinas em uma rede pública podem ser acessadas na Internet. Um administrador de TI define essas redes. A definição de uma rede do <code>public</code> é idêntica à de uma rede do <code>existing</code> para redes que permitem que o tráfego de rede ocorra em redes públicas.</p> |
| <code>private</code> | <p>Um tipo de rede sob demanda.</p> <p>Limita o tráfego de rede que ocorrerá somente entre os recursos na rede implantada. Ele impede o tráfego de entrada e saída. No NSX, ele pode ser equivalente a NAT sob demanda de um-para-muitos.</p> |
| <code>outbound</code> | <p>Um tipo de rede sob demanda.</p> <p>Limita o tráfego de rede entre os recursos de processamento e na implantação, mas também permite um tráfego de rede de saída unidirecional. No NSX, ele pode ser equivalente a NAT sob demanda de um-para-muitos com IP externo.</p> |
| <code>routed</code> | <p>Um tipo de rede sob demanda.</p> <p>Redes roteadas contêm um espaço de IPs roteável dividido em sub-redes disponíveis que estão vinculadas. As máquinas virtuais provisionadas com redes roteadas e que tenham o mesmo perfil de rede roteada poderão se comunicar umas com as outras e com a rede externa.</p> <p>As redes roteadas são um tipo de rede sob demanda que está disponível para redes NSX-V e NSX-T. O Microsoft Azure e o Amazon Web Services fornecem essa conectividade por padrão.</p> <p>Uma rede <code>routed</code> só está disponível para especificação do modelo de nuvem em um componente de rede <code>Cloud.NSX.Network</code>.</p> |

Para obter mais informações, consulte [Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation](#).

Para conhecer exemplos de modelos de nuvem preenchidos que contêm dados de componentes de rede, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Exemplos de cenários de rede

Pode-se esperar o seguinte comportamento quando você implanta um modelo de nuvem que usa a seguinte configuração de perfil de rede.

| Tipo ou cenário de rede | Nenhum perfil de rede disponível para a zona de nuvem | Perfis de rede disponíveis para a zona de nuvem |
|-------------------------|---|--|
| Nenhuma rede | <p>Se nenhuma rede for especificada no modelo de nuvem, uma rede aleatória será selecionada na mesma região de provisionamento que o processamento.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>Se não existir nenhuma rede em uma região de provisionamento disponível, o provisionamento falhará.</p> | <p>Uma rede é selecionada a partir de um perfil de rede correspondente.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>Se nenhum dos perfis de rede atender aos critérios, o provisionamento falhará.</p> |
| Rede existente | <p>Se o componente de rede no modelo de nuvem contiver tags de restrição, essas restrições serão usadas para filtrar a lista de redes disponíveis. As tags de restrição no componente de rede do modelo de nuvem correspondem às tags de rede e às tags de restrição de perfil de rede, se disponíveis.</p> <p>Na lista de redes filtradas, uma única rede é selecionada na mesma região de provisionamento que o processamento.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>Se após a filtragem com base em restrições não houver nenhuma rede na região de provisionamento, o provisionamento falhará.</p> | <p>Uma rede é selecionada a partir de um perfil de rede correspondente.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>Se nenhum dos perfis de rede atender aos critérios, o provisionamento falhará.</p> <p>As restrições de rede podem ser usadas para filtrar as redes existentes no perfil com base nas tags previamente atribuídas.</p> |
| Rede pública | <p>Se a rede tiver restrições, essas restrições serão usadas para filtrar a lista de redes disponíveis que tenham o conjunto de atributos <code>supports public IP</code>.</p> <p>Na lista de redes filtradas, uma rede aleatória é selecionada na mesma região de provisionamento que o processamento.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>Se após a filtragem com base em restrições não houver redes públicas na região de provisionamento, o provisionamento falhará.</p> | <p>Uma rede com o atributo <code>supports public IP</code> será selecionada a partir de um perfil de rede correspondente.</p> <p>A preferência é dada às redes que são rotuladas como padrão.</p> <p>As restrições de rede podem ser usadas para filtrar as redes públicas existentes no perfil com base nas tags pré-configuradas.</p> |

| Tipo ou cenário de rede | Nenhum perfil de rede disponível para a zona de nuvem | Perfis de rede disponíveis para a zona de nuvem |
|---|--|---|
| Rede privada | O provisionamento falha porque as redes privadas exigem informações de um perfil de rede. | <p>Uma nova rede ou novo grupo de segurança é criado com base nas configurações do perfil de rede correspondente.</p> <p>As tags de restrição de rede podem ser usadas para filtrar perfis de rede e redes.</p> |
| Rede de saída | O provisionamento falha porque as redes de saída exigem informações de um perfil de rede. | <p>Uma nova rede ou novo grupo de segurança é criado com base nas configurações do perfil de rede correspondente.</p> <p>As tags de restrição de rede podem ser usadas para filtrar perfis de rede e redes.</p> |
| Rede roteada sob demanda | O provisionamento falha porque as redes roteadas exigem informações de um perfil de rede. | <p>Para NSX-V, precisamos da seleção do DLR (roteador lógico distribuído).</p> <p>Para NSX-T e VMware Cloud on AWS, precisamos de configurações sob demanda semelhantes como private e outbound.</p> |
| Exemplo de caso de uso do WordPress com redes existentes ou públicas | O provisionamento ocorre conforme descrito para uma rede pública ou rede existente. | <p>Veja as descrições acima para o comportamento da rede pública e da rede existentes.</p> <p>Consulte Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly.</p> |
| Exemplo de uso do WordPress com redes existentes ou públicas e redes privadas ou externas | O provisionamento falha porque a rede requer informações de um perfil de rede. | <p>Veja as descrições acima para uma rede privada e uma rede de saída.</p> <p>Consulte Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly.</p> |
| Exemplo de caso de uso do WordPress com balanceador de carga | <p>O provisionamento falha porque um balanceador de carga requer informações de um perfil de rede.</p> <p>O provisionamento poderá ocorrer quando balanceadores de carga existentes estiverem presentes.</p> | <p>Um novo balanceador de carga é criado com base na configuração do perfil de rede.</p> <p>Você pode especificar um balanceador de carga existente que foi ativado no perfil de rede.</p> <p>O provisionamento falha se você solicitar um balanceador de carga existente, mas nenhum atender às restrições no perfil de rede.</p> <p>Consulte Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly.</p> |

Usando configurações de grupos de segurança em perfis de rede e designs de modelo de nuvem no vRealize Automation

Você pode definir e alterar configurações de grupos de segurança em perfis de rede e em designs de modelo de nuvem.

É possível usar recursos de grupos de segurança de várias maneiras:

- Grupo de segurança existente especificado em um perfil de rede

Você pode adicionar um grupo de segurança existente a um perfil de rede. Quando um design de modelo de nuvem usar esse perfil de rede, suas máquinas serão agrupadas como membros do grupo de segurança. Esse método não requer que você inclua um recurso de grupo de segurança em um design de modelo de nuvem. Você também pode usar um balanceador de carga nessa configuração. Para obter informações relacionadas, consulte [Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation](#).

- Componente de grupos de segurança associado ao recurso de máquina em um design de modelo de nuvem

Você pode arrastar e soltar um recurso de grupo de segurança em um design de modelo de nuvem e vincular esse recurso de grupo de segurança a uma NIC de máquina usando tags de restrição no recurso de grupo de segurança existente no design de modelo de nuvem e no grupo de segurança existente no recurso com coleta de dados. Também é possível fazer essa associação conectando os objetos com uma linha de conexão na tela do design de modelo de nuvem, semelhante a como você associa redes a máquinas na tela de design.

Ao arrastar e soltar um recurso de grupo de segurança na tela de design de modelo de nuvem, ele pode ser do tipo `existing` ou `new`. Se for um tipo de grupo de segurança `existing`, você deverá adicionar um valor de restrição de tag conforme solicitado. Se for um tipo de grupo de segurança `new`, você poderá configurar regras de firewall.

- Um grupo de segurança existente alocado com restrições de tag e associado a uma NIC de máquina no modelo de nuvem

Por exemplo, você pode associar um recurso de grupo de segurança a uma NIC de máquina (em um recurso de máquina) no design de modelo de nuvem, correspondendo tags entre os dois recursos.

Como um exemplo para o NSX-T quando tags são especificadas no endpoint de origem, você pode usar tags do NSX-T especificadas no seu aplicativo NSX-T. Em seguida, pode usar uma tag do NSX-T, especificada como uma restrição em um recurso de rede em um design de modelo de nuvem, em que o recurso de rede está conectado a uma NIC de máquina no design de modelo de nuvem. Tags do NSX-T permitem agrupar máquinas dinamicamente usando uma tag do NSX-T que é coletada por dados a partir do endpoint de origem do NSX-T. Use uma porta lógica ao criar a tag do NSX-T no NSX-T.

- Regras de firewall em um recurso de grupo de segurança sob demanda em um design de modelo de nuvem

Você pode adicionar regras de firewall a um grupo de segurança sob demanda no design de modelo de nuvem.

Para obter informações sobre as regras de firewall disponíveis, consulte [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#).

Saiba mais

Para obter informações sobre como definir grupos de segurança em perfis de rede, consulte [Saiba mais sobre perfis de rede no vRealize Automation](#).

Para obter informações sobre como visualizar e alterar as configurações de grupos de segurança nas páginas de recursos de infraestrutura, consulte [Recursos de segurança no vRealize Automation](#).

Para obter informações sobre como definir grupos de segurança em designs de modelos de nuvem, consulte [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#).

Para conhecer exemplos de recursos de grupo de segurança em designs de modelos de nuvem, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Usando configurações de balanceador de carga em perfis de rede no vRealize Automation

Você pode definir configurações de balanceador de carga na sua configuração de perfil de rede.

Você pode adicionar um balanceador de carga existente a um perfil de rede usando a guia **Balanceador de Carga**.

É possível adicionar um balanceador de carga a um design de modelo de nuvem associando-o a um perfil de rede que contenha um ou mais balanceadores de carga ou diretamente usando um recurso de balanceador de carga no código ou na tela de design de modelo de nuvem.

Exemplos para incluir um balanceador de carga de VIP com base no uso de grupos de segurança em um perfil de rede

Existem dois tipos de grupos de segurança que você pode usar em um perfil de rede: um grupo de segurança existente selecionado na guia **Grupos de Segurança** e um grupo de segurança sob demanda que você cria usando uma política de isolamento na guia **Políticas de Rede**.

Quando um VIP de balanceador de carga é associado a um grupo de segurança com base nas configurações do perfil de rede, a configuração do grupo de segurança é fornecida pelo perfil de rede.

A tabela a seguir ilustra alguns cenários de amostra.

| Topologia do design de modelo de nuvem - recursos associados | Configuração de perfil de rede | Associação ao grupo de segurança |
|---|---|--|
| Balanceador de carga de um braço com VIP na rede privada e uma máquina na mesma rede privada. | O perfil de rede selecionado usa a política de isolamento definida como um grupo de segurança sob demanda. | A NIC da máquina e o VIP do balanceador de carga são adicionados ao grupo de segurança de isolamento. |
| Balanceador de carga de um braço com VIP na rede privada e uma máquina na mesma rede privada. | O perfil de rede selecionado usa um grupo de segurança existente e usa a política de isolamento definida como um grupo de segurança sob demanda. | A NIC da máquina e o VIP do balanceador de carga são adicionados ao grupo de segurança de isolamento e ao grupo de segurança existente. |
| Balanceador de carga de dois braços com um VIP em uma rede pública e uma máquina em uma rede privada. | O perfil de rede selecionado usa um grupo de segurança existente e usa a política de isolamento definida como um grupo de segurança sob demanda. | A NIC da máquina e o VIP do balanceador de carga são adicionados ao grupo de segurança de isolamento e ao grupo de segurança existente. |
| Balanceador de carga de dois braços com um VIP em uma rede pública e uma máquina em uma rede privada. | O perfil de rede selecionado usa um grupo de segurança existente. | A NIC da máquina e o VIP do balanceador de carga são adicionados ao grupo de segurança existente. |
| Balanceador de carga de dois braços, VIP na rede 1 e máquina na rede 2. | Dois perfis de rede: <ul style="list-style-type: none"> ■ Perfil de rede 1: Usa um grupo de segurança 1 existente. ■ Perfil de rede 2: Usa um grupo de segurança 2 existente. | O balanceador de carga chega ao perfil de rede 1, e a máquina chega ao perfil de rede 2. O VIP do balanceador de carga é adicionado ao grupo de segurança 1, e a NIC da máquina é adicionada ao grupo de segurança 2. |

Saiba mais

Para obter informações sobre como adicionar recursos de balanceador de carga a um design de modelo de nuvem, consulte [Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation](#).

Para exemplos de designs de modelo de nuvem que incluem balanceadores de carga, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Como configurar um perfil de rede para oferecer suporte a uma rede sob demanda para uma integração de IPAM externa no vRealize Automation

Você pode configurar um perfil de rede para oferecer bloqueio de endereços IP para uma rede sob demanda quando esse perfil de rede é usado em um modelo de nuvem do vRealize Automation que usa a integração de IPAM externa.

Usando uma integração existente para um provedor de IPAM externo específico, você pode provisionar a rede sob demanda para criar uma nova rede no sistema IPAM externo.

Usando esse processo, você configura um bloco de endereços IP, em vez de inserir um CIDR principal (como é feito ao usar o IPAM interno do vRealize Automation). O bloco de endereços IP é usado durante o provisionamento de rede sob demanda para segmentar a nova rede. Os blocos de IP são coletados por dados do provedor IPAM externo, desde que a integração ofereça suporte à rede sob demanda. Por exemplo, ao usar uma integração IPAM do Infoblox, os blocos de IP representam os contêineres de rede Infoblox.

Quando você usa um perfil de rede sob demanda e uma integração de IPAM externa em um modelo de nuvem, os seguintes eventos ocorrem quando o modelo de nuvem é implantado:

- Uma rede é criada no provedor de IPAM externo.
- Uma rede também é criada no vRealize Automation, refletindo a nova configuração de rede do provedor de IPAM, incluindo configurações como as propriedades de CIDR e de gateway.
- O endereço IP da máquina virtual implantada é obtido com a rede recém-criada.

Nesse exemplo de rede sob demanda, você configura um perfil de rede para permitir que uma implantação de modelo de nuvem provisione uma máquina para uma rede sob demanda no vSphere usando o Infoblox como o provedor de IPAM externo.

Para obter informações relacionadas, consulte [Como configurar um perfil de rede para oferecer suporte a uma rede existente para uma integração de IPAM externa no vRealize Automation](#). Os dois exemplos de configuração de rede se encaixam no fluxo de trabalho geral específico do fornecedor para a integração de IPAM externa no [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#).

Pré-requisitos

Enquanto os pré-requisitos a seguir se aplicam à pessoa que cria ou edita o perfil de rede, o perfil de rede em si seria aplicável quando usado por uma implantação de modelo de nuvem que contenha uma integração IPAM. Para saber mais sobre os pontos de integração de IPAM específicos do fornecedor, consulte [Como configurar uma integração externa de IPAM no vRealize Automation](#).

Essa sequência de etapas é mostrada no contexto de um fluxo de trabalho de integração do provedor de IPAM. Consulte [Tutorial: configurando uma integração de IPAM externa específica do provedor para o vRealize Automation](#).

- Verifique se tem credenciais de administrador de nuvem. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Verifique se você tem uma conta com o provedor de IPAM externo, por exemplo, o [Infoblox](#) ou o [Bluecat](#), e se tem as credenciais de acesso corretas para a conta da sua organização com esse provedor de IPAM. Neste exemplo de fluxo de trabalho, o provedor de IPAM é o Infoblox.

- Verifique se você tem um ponto de integração de IPAM para o provedor de IPAM e se o pacote de IPAM usado para criar a integração de IPAM é compatível com redes sob demanda. Consulte [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#).

Embora o pacote de IPAM do Infoblox ofereça suporte a redes sob demanda, se você estiver usando uma integração de IPAM externa para um provedor diferente, verifique se o pacote de integração de IPAM é compatível com redes sob demanda.

Procedimentos

- 1 Para configurar um perfil de rede, clique em **Infraestrutura > Configurar > Perfis de rede**.

- 2 Clique em **Novo perfil de rede**.

- 3 Clique na guia **Resumo** e especifique as seguintes configurações de amostra:

- Especifique uma conta/região de nuvem do vSphere, por exemplo, **vSphere-IPAM-OnDemandA/Datacenter**.

Este exemplo presume o uso de uma conta de nuvem do vSphere que não está associada a uma conta de nuvem do NSX.

- Dê um nome para o perfil de rede, por exemplo, **Infoblox-OnDemandNP**.
- Adicione uma tag de capacidade para o perfil de rede, por exemplo, **infoblox_ondemandA**.

Anote o valor da tag de capacidade, já que você também deve usá-la como uma tag de restrição de modelo de nuvem para fazer com que a associação do perfil de rede seja usada ao provisionar o modelo de nuvem.

- 4 Clique na guia **Políticas de rede** e especifique as seguintes configurações de amostra:

- No menu suspenso **Política de isolamento**, selecione **Rede sob demanda**.

Essa opção permite que você use blocos de IP IPAM externos. Dependendo da conta de nuvem, novas opções são exibidas. Por exemplo, as seguintes opções aparecem ao usar uma conta de nuvem do vSphere associada a uma conta de nuvem do NSX:

- Zona de transporte
- Roteador lógico de camada 0
- Edge cluster

Para esse exemplo, a conta de nuvem do vSphere não está associada ao NSX, então a opção de menu **Domínio de rede** é exibida.

- Deixe a opção **Domínio de rede** em branco.

- 5 Clique em **Externo** como a **Prigem** do gerenciamento de endereços.

- 6 Clique em **Adicionar bloco de IP**, que abre a página **Adicionar bloco de IP IPAM**.

7 No menu **Provedor** na página **Adicionar bloco de IP IPAM**, selecione uma integração de IPAM externa existente. Por exemplo, selecione o ponto de integração *Infoblox_Integration* do [Adicionar uma integração de IPAM externo para Infoblox no vRealize Automation](#) no fluxo de trabalho de exemplo.

8 No menu **Espaços de endereços**, selecione um dos blocos de IP disponíveis e listados, por exemplo **10.23.118.0/24** e adicione-o.

Se o provedor de IPAM oferecer suporte a espaços de endereço, o menu **Espaços de endereços** será exibido. Para uma integração do Infoblox, os espaços de endereços são representados pelas visualizações de rede do Infoblox.

9 Selecione um **Tamanho de sub-rede**, como **/29 (-6 endereços IP)**.

10 Clique em **Criar**.

Resultados

É criado um perfil de rede que pode ser usado para provisionar uma rede sob demanda usando a integração de IPAM externa especificada. O modelo de nuvem de amostra a seguir mostra uma única máquina a ser implantada em uma rede definida por esse novo perfil de rede.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: private
```



```
constraints:
  - tag: infoblox_ondemanda
```

Observação Quando o modelo de nuvem é implantado, a primeira rede disponível no bloco de IP especificado é obtida e considerada como o CIDR de rede. Se você estiver usando uma rede de NSX no modelo de nuvem, poderá, em vez disso, definir o CIDR da rede manualmente usando a propriedade de rede `networkCidr`, conforme mostrado abaixo, para definir manualmente um CIDR e substituir as configurações de blocos de IP e tamanho de sub-rede especificadas no perfil de rede associado.

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```

Como configurar um perfil de rede para oferecer suporte a uma rede existente para uma integração de IPAM externa no vRealize Automation

Você pode configurar um perfil de rede para oferecer suporte a intervalos de endereços IP para uma rede existente quando esse perfil de rede é usado em um blueprint do vRealize Automation que usa a integração de IPAM externa.

Um exemplo é apresentado no contexto de um fluxo de trabalho de amostra específico do fornecedor em [Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente no vRealize Automation](#). O fluxo de trabalho geral específico do fornecedor para a integração de IPAM externa está em [Tutorial: configurando o VMware Cloud on AWS para o vRealize Automation](#).

Para obter informações relacionadas, consulte [Como configurar um perfil de rede para oferecer suporte a uma rede sob demanda para uma integração de IPAM externa no vRealize Automation](#).

Como adicionar perfis de armazenamento do Cloud Assembly que se referem a diferentes requisitos

Um perfil de armazenamento do Cloud Assembly descreve o tipo de armazenamento a ser implantado.

O armazenamento costuma ser perfilado de acordo com características como nível de serviço ou custo, desempenho ou finalidade, tal como backup.

Selecione **Infraestrutura > Configurar > Perfis de Armazenamento** e clique em **Novo Perfil de Armazenamento**.

Saiba mais sobre perfis de armazenamento no vRealize Automation

Uma região da conta de nuvem contém perfis de armazenamento que permitem que o administrador de nuvem defina o armazenamento da região no vRealize Automation.

O que um perfil de armazenamento faz

Os perfis de armazenamento incluem personalizações de disco e um meio de identificar o tipo de armazenamento através de tags de capacidade. Em seguida, as tags são correspondidas às restrições de solicitação de serviço de provisionamento para criar o armazenamento desejado no momento da implantação.

Os perfis de armazenamento são organizados em regiões específicas da nuvem. Uma conta de nuvem pode ter várias regiões, com vários perfis de armazenamento em cada.

A colocação independente do fornecedor é possível. Por exemplo, você pode ter três contas de fornecedores diferentes e uma região em cada uma. Cada região inclui um perfil de armazenamento marcado com a tag de recurso *rápido*. No momento do provisionamento, uma solicitação contendo uma tag de restrição rígida *rápido* procura por um recurso *rápido* correspondente, independentemente da nuvem do fornecedor que está fornecendo os recursos. Uma correspondência aplica as configurações do perfil de armazenamento associado durante a criação do item de armazenamento implantado.

Observação O armazenamento em nuvem diferente pode ter características de desempenho diferentes, mas ainda ser considerado a oferta *rápida* pelo administrador que a marcou.

As tags de capacidade adicionadas aos perfis de armazenamento não devem identificar destinos de recurso real. Em vez disso, elas descrevem tipos de armazenamento. Para obter mais informações sobre recursos reais, consulte [Recursos de armazenamento no vRealize Automation](#).

Tipo de provisionamento padrão

O tipo de provisionamento do perfil de armazenamento apenas estabelece um comportamento padrão. A configuração não afeta necessariamente o posicionamento e pode ser substituída por uma propriedade no modelo de nuvem.

Por exemplo, você pode definir o perfil de armazenamento para provisionamento dinâmico. Na maioria dos casos, as solicitações criariam o armazenamento de provisionamento dinâmico por padrão. No entanto, se o modelo de nuvem tiver a propriedade `provisioningType` definida como `eager-zero`, o modelo de nuvem substituirá o padrão dinâmico.

Observação Quando você deseja controle exato, é melhor adicionar tags de capacidade e restrição rotuladas para o tipo de provisionamento desejado.

Para o padrão de tipo de provisionamento, uma propriedade de modelo de nuvem substitui um padrão de perfil de armazenamento, e um padrão de perfil de armazenamento substitui um padrão de uma política de armazenamento do vCenter.

Alocação de disco com máquinas

Em um projeto com várias zonas de nuvem que pertencem a diferentes contas de nuvem, um disco segue a máquina, mesmo que não esteja conectado a ela. Esse comportamento mantém os recursos juntos para impedir falhas se você decidir anexar o disco mais tarde.

Por exemplo, o seguinte design não funcionará. O modelo de nuvem tenta usar restrições de localização para separar o disco, mas a implantação retorna um erro de `No matching placement` em vez disso.

Se for necessário colocar um disco em uma conta de nuvem diferente, use uma implantação separada para implantar esse disco.

```
resources:
  Machine1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      constraints:
        - tag: 'location:siteA'
  Disk1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      constraints:
        - tag: 'location:siteB'
```

Discos de primeira classe e padrão

Usando a opção **Tipo de disco** na página de perfil de armazenamento ou usando a API do vRealize Automation, você pode criar um perfil de armazenamento para oferecer suporte ao armazenamento em disco de primeira classe (FCD) ou em disco padrão. Na verdade, a opção de disco de primeira classe cria um perfil de armazenamento do vSphere.

■ Disco de primeira classe

Discos de primeira classe podem existir independentemente de uma máquina virtual vSphere. Um disco de primeira classe também possui recursos de gerenciamento de ciclo de vida que podem operar independentemente de uma máquina virtual. Discos de primeira classe estão disponíveis para o vSphere 6.7, Atualização 2 e posteriores, e estão atualmente implementados no vRealize Automation como um recurso apenas de API.

Para obter informações sobre o armazenamento FCD, incluindo os recursos que estão disponíveis na API do vRealize Automation e links para a própria documentação da API, consulte [O que posso fazer com o armazenamento em disco de primeira classe no vRealize Automation](#).

■ Disco padrão

O armazenamento em disco padrão é criado e gerenciado como um componente integrado de uma máquina virtual.

Para obter informações sobre o armazenamento em disco padrão, consulte [O que posso fazer com o armazenamento em disco padrão no vRealize Automation](#) e [O que posso fazer com o armazenamento em disco persistente no vRealize Automation](#).

Criptografia de disco no lado do servidor Azure

Para recursos do Azure, se você optar por oferecer suporte à criptografia em um perfil de armazenamento em disco gerenciado, também selecionará a criptografia de disco que possui uma chave associada. A criptografia e as chaves disponíveis correspondem aos conjuntos de criptografia de disco configurados no Azure para o local.

Microsoft Azure Search resources, services, and docs (G+)

Home > **Disk Encryption Sets**

+ Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == R&D Resource group == all Location == all Add filter

Showing 1 to 100 of 305 records.

| Name | Resource group | Location | Key |
|----------|--------------------|----------|--------------|
| MyDES | DiskEncryptionSets | West US | WestUSKey... |
| MyDES1 | DiskEncryptionSets | West US | WestUSKey... |
| MyDES10 | DiskEncryptionSets | West US | WestUSKey... |
| MyDES100 | DiskEncryptionSets | West US | WestUSKey... |
| MyDES101 | DiskEncryptionSets | West US | WestUSKey... |

Account / region AzureAcc / West US

Name SP-with-des

Description

Storage type Managed disks

Disk type Standard HDD

OS disk caching Read only

Data disk caching Read only

☒ Supports encryption

Encryption set Search for encryption set

- MyDES WestUSKeyForDisk EncryptDiskWestUS
- MyDES1 WestUSKeyForDisk EncryptDiskWestUS
- MyDES10 WestUSKeyForDisk EncryptDiskWestUS
- MyDES100 WestUSKeyForDisk EncryptDiskWestUS
- MyDES101 WestUSKeyForDisk EncryptDiskWestUS

Capability tags

CREATE CANCEL

Como usar cartões de preços no vRealize Automation

Cartões de preços do Cloud Assembly ajudam os administradores de nuvem a definir e atribuir a política de preços para o impacto monetário das suas implantações individuais, ajudando você a gerenciar recursos.

Observação Para que a definição de preços funcione em ambientes com vários tenants, você deve ter uma instância separada do vRealize Operations Manager para cada tenant do vRealize Automation.

Cartões de preço definem as taxas para uma política de preços. Em seguida, a política de preços pode ser atribuída a projetos específicos para definir um preço total. Após a criação de um endpoint do vRealize Operations Manager ou do CloudHealth, um cartão de taxa padrão predefinido estará disponível com uma configuração de custo igual ao preço na guia **Infraestrutura > Cartão de Preços**. Você pode criar cartões de preços que se aplicam apenas a projetos ou a zonas de nuvem. Por padrão, todos os novos cartões de preços são aplicados a projetos.

Observação Se você alterar a configuração **Todos os cartões de preços são aplicados a**, todas as atribuições de cartão de preço existentes serão excluídas. Além disso, se o endpoint do vRealize Operations Manager for excluído do Cloud Assembly, todos os cartões de preço e atribuições também serão excluídos.

O preço de uma implantação ao longo do tempo é exibido no cartão de implantação e no projeto como o preço acumulado do mês, que é redefinido como zero no início de cada mês. As divisões de custo do componente estão disponíveis nos detalhes da implantação. O fornecimento dessas informações no nível de implantação informa o administrador da nuvem, mas também ajuda os membros a compreender o impacto que o trabalho pode ter nos orçamentos e no desenvolvimento a longo prazo.

Você pode optar por exibir informações de preços de usuários no Cloud Assembly e no Service Broker, selecionando o botão **Exibir informações de preço**. Se desativadas, as informações de preços ficam ocultas dos usuários do Cloud Assembly e do Service Broker.

Como o preço é calculado

O preço inicial visto no nível de implantação para os recursos de processamento e armazenamento são baseados nas taxas de parâmetro de comparação padrão do setor e, em seguida, são calculados com o passar do tempo. A taxa é aplicada aos hosts, e o serviço calcula as taxas de CPU e memória. O servidor recalcula o preço a cada 6 horas.

As novas políticas, atribuições e preços antecipados serão definidos durante o próximo ciclo de coleta de dados. Por padrão, o ciclo de coleta de dados é executado a cada 5 minutos. Pode levar até 6 horas para novas políticas ou alterações serem atualizadas em projetos e implantações.

Como estimar o preço dos meus projetos e implantações

Antes de implantar um item de catálogo, você pode usar o preço antecipado como uma estimativa de preço para a sua implantação. Para exibir o preço no Cloud Assembly, você deve ter um endpoint de integração do vRealize Operations Manager configurado com a definição de preço habilitada e a moeda predefinida.

Daily Price Estimate



Guest OS and one time prices are excluded in this estimate.



price-service-f309c00

\$0.54



Cloud_vSphere_Machine_1

\$0.53

Compute

\$0.39

Storage

\$0.03

Additional charges

\$0.11



Cloud_vSphere_Disk_1

\$0.01

Storage

\$0.01

CLOSE

Para uma estimativa de preço antecipado, o tamanho do disco de inicialização por VM é sempre 8 GB.

O preço antecipado de uma implantação é uma estimativa diária de preços, com base na alocação de um recurso, para um determinado item de catálogo antes que ele seja implantado. Depois que um item de catálogo é implantado, você poderá exibir o preço acumulado do mês como um agregado do preço antecipado nas guias **Implantação** e **Infraestrutura > Projetos**. O preço antecipado é compatível com recursos de nuvem privada, como máquina do vSphere e disco do vSphere, itens de catálogo do Cloud Assembly e itens independentes de nuvem com o vCenter configurado para nuvem privada.

Observação Não há suporte de preço antecipado para recursos de nuvem pública ou para recursos de nuvem privada de discos e máquinas não vSphere.

Para estimar o custo da sua implantação, no Catálogo, selecione um item de catálogo e clique em **Solicitar > Calcular**. Se o preço for aceitável, clique em **Enviar**.

Você pode usar cartões de preços de projeto para estimar o preço total de todos os seus projetos.

Para estimar o custo de um projeto, na página Cartão de Preços em Infraestrutura, ao lado da configuração **Todos os cartões de preços são aplicados a**, clique em **Editar** e selecione **Projetos**.

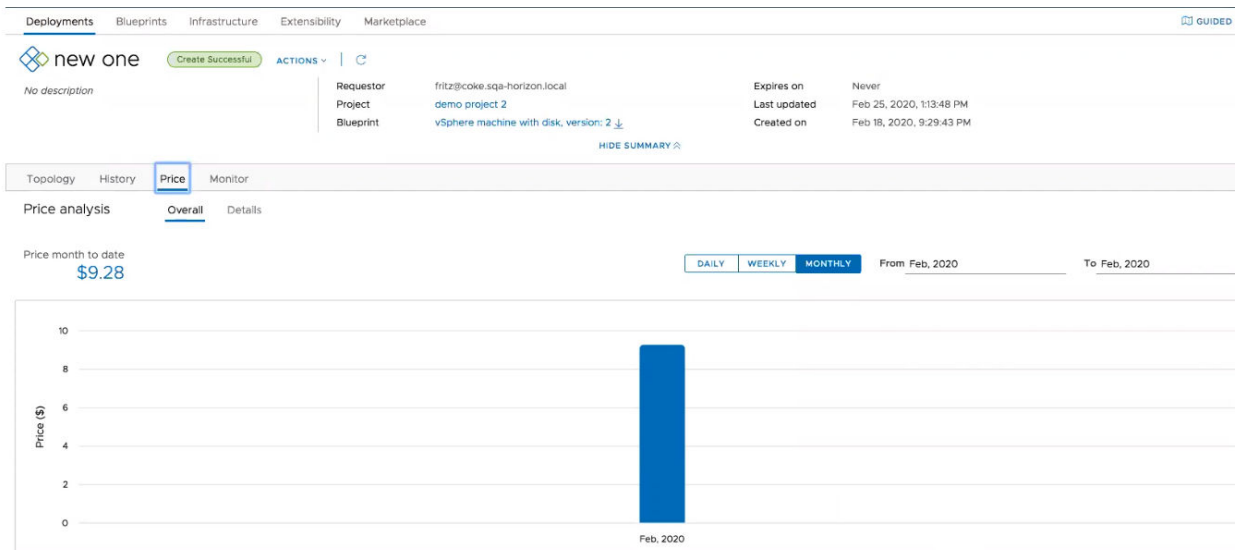
Se você alterar a configuração **Todos os cartões de preços são aplicados a**, todas as atribuições de cartão de preço existentes serão excluídas. Crie cartões de preços e atribuições usando uma abordagem baseada em custos.

Como criar cartões de preços para o vSphere e o VMC

Você pode criar e atribuir um cartão de preços a projetos ou zonas de nuvem, dependendo da estratégia de preços determinada pelo administrador da nuvem para implantações de nuvem privada.

Cartões de preços são personalizáveis com base nos parâmetros selecionados pelo usuário. Depois de configurar um cartão de preços, você pode atribuí-lo a um ou mais projetos e zonas de nuvem determinados pela estratégia de preços.

Você pode atualizar manualmente o servidor de preços a qualquer momento na página Endpoint do vROps, **Infraestrutura > Integrações > Endpoint do vROps > .** Na seção vCenter Servers, clique em **Sincronizar**. Ao atualizar manualmente o servidor de preços usando a opção **Sincronizar**, o preço é recalculado para todos os projetos na organização. Dependendo de quantos projetos a sua organização tiver, esse processo pode ser intensivo e demorado.



Depois de criar e atribuir um cartão de preços, você pode visualizar o histórico de preços de suas implantações e projetos. Para visualizar o histórico de preços, navegue até a sua implantação e clique em **Preço**. A análise de preços fornece uma visão geral e a exibição detalhada do preço de implantação, juntamente com o valor acumulado do mês. Você pode alterar a representação gráfica para exibir o preço de implantação como valores diários, semanais ou mensais. Além disso, pode especificar um intervalo de datas ou mês exato para o histórico de preços.

Para exibir a divisão de preços por componente de custo, clique em **Detalhes**.

Os preços são determinados por tipos de componentes com custo.

Tabela 4-1. Tipos de componente com custo

| Tipo de componente do blueprint | Nome do serviço/tipo de objeto | Tipo de recurso de blueprint | Comentários |
|---------------------------------|--------------------------------|------------------------------|--|
| Independente de nuvem | Máquina | Cloud.Machine | Se uma máquina independente estiver configurada com o vSphere, você poderá visualizar o custo da implantação. |
| | Disco | Cloud.Volume | Se um disco independente estiver conectado a uma máquina virtual configurada com o vSphere, você poderá visualizar o custo da implantação. |
| vSphere | Máquina vSphere | Cloud.vSphere.Machine | Implantado usando um blueprint específico de nuvem. |
| | Disco vSphere | Cloud.vSphere.Disk | Implantado usando um blueprint específico de nuvem anexado a uma máquina virtual. |
| VMware Managed Cloud (VMC) | Máquina vSphere | Cloud.vSphere.Machine | O VMC só é compatível com cartões de preço baseados em taxas (não há suporte para cartões de preço baseados em custo). |
| | Disco vSphere | Cloud.vSphere.Disk | |

Pré-requisitos

Antes de poder criar ou atribuir cartões de preços, você deve configurar e habilitar os preços e configurar a moeda no vRealize Operations para trabalhar com ovRealize Automation .

Ao configurar o vRealize Operations com o vRealize Automation , certifique-se de que ambos os aplicativos estejam definidos para o mesmo fuso horário. Para configurar o fuso horário no vRealize Operations, habilite o SSH e faça login em cada nó do vRealize Operations, edite o arquivo `$ALIVE_Base/user/conf/analytics/advanced.properties` e adicione `timeZoneUsedInMeteringCalculation =<time zone>`.

Para que a definição de preços funcione em ambientes de vários tenants, você deve ter uma instância do vROps separada para cada tenant do vRA.

Você deve configurar um endpoint do vRealize Operations antes de poder configurar cartões de preços. Para configurar o endpoint do vRealize Operations, navegue até **Infraestrutura > Conexões > Integrações > Adicionar Integração**.

Observação Quando vários endpoints do vRealize Operations são adicionados, eles não devem monitorar o mesmo vCenter.

Procedimentos

- 1 Navegue até **Infraestrutura > Cartões de Preços > Novo Cartão de Preços**.
- 2 Na guia Resumo, insira um nome e uma descrição para o cartão de preço. Quando a política estiver definida na guia de definição de preço, a tabela Visão Geral será preenchida com taxas de cartões de preço.

Observação A unidade monetária é determinada pelo valor selecionado no vRealize Operations.

- 3 Opcional. Marque a caixa de seleção **Padrão para projetos não atribuídos?** para atribuir esse cartão de preços a todos os projetos não atribuídos por padrão.

4 Clique em **Preços** e configure os detalhes da sua política de preços.

Tabela 4-2. Configuração da política de preços

| Parâmetro | Descrição |
|-------------------|--|
| Cobranças Básicas | <p>Insira um nome e uma descrição para a sua política. Selecione a opção com base em custo ou taxa.</p> <ul style="list-style-type: none"> ■ Custo - O custo é definido no vRealize Operations. Se selecionado, um fator de multiplicação será necessário. Por exemplo, se você selecionar 1,1 como fator, o custo será multiplicado por 1,1, resultando em um aumento de 10% no custo calculado. A equação de preço usando o custo é: $\text{<custo>} \times \text{<fator de multiplicação>} = \text{Preço}$ ■ Taxa - Se selecionada, você deverá usar valores absolutos para determinar o custo. A equação de preço usando a taxa é: $\text{<Taxa>} = \text{Preço}$. Selecione um intervalo de taxa na lista suspensa para especificar como essa taxa é cobrada. <p>Na seção Cobranças Básicas, você define o custo ou a taxa para a CPU, a memória, o armazenamento e os custos diversos adicionais.</p> |
| SOs Convidados | <p>Você pode definir uma cobrança de SO Convidado clicando em Adicionar Cobrança.</p> <p>Insira o nome do SO guest e defina o método de cobrança e a taxa base.</p> <ul style="list-style-type: none"> ■ Recorrente - Insira uma taxa base e defina o intervalo recorrente como o período de cobrança. O valor de taxa absoluta é necessário e é adicionado ao preço geral. ■ Único - Defina a cobrança da taxa base única. O valor absoluto é necessário e é adicionado como um preço único. ■ Fator de Taxa - É necessário um fator de multiplicação que é aplicado à categoria Selecionar Cobrança. Por exemplo, se você selecionar Cobrança da CPU e um fator de taxa de 2. A CPU do SO Convidado é cobrada como 2 vezes o valor de custo padrão. <p>Você pode adicionar vários SOs Convidados com taxas diferentes clicando em Adicionar Cobrança e configurando uma política de cobrança adicional.</p> <hr/> <p>Observação As cobranças iniciais para os SOs guests não são mostrados na página Resumo, mesmo que façam parte da política.</p> |

Tabela 4-2. Configuração da política de preços (continuação)

| Parâmetro | Descrição |
|-----------------------------|--|
| Tags | <p>Você pode definir uma cobrança de Tag clicando em Adicionar Cobrança.</p> <p>Selecione o nome da Tag e defina o método de cobrança e a taxa base.</p> <ul style="list-style-type: none"> ■ Recorrente - Insira uma taxa base e defina o intervalo recorrente como o período de cobrança. O valor de taxa absoluta é necessário e é adicionado ao preço geral. ■ Único - Defina a cobrança da taxa base única. O valor absoluto é necessário e é adicionado como um preço único. ■ Fator de Taxa - É necessário um fator de multiplicação que é aplicado à categoria Selecionar Cobrança. <p>Selecione como cobrar a Tag com base no estado ligado.</p> <p>Você pode adicionar várias Tags com taxas diferentes clicando em Adicionar Cobrança e configurando uma política de cobrança adicional.</p> <hr/> <p>Observação Cobranças adicionais no preço final calculado incluem tags em VMs e não inclui Tags em discos e redes.</p> |
| Propriedades personalizadas | <p>Você pode definir uma cobrança de Propriedade Personalizada clicando em Adicionar Cobrança.</p> <p>Insira o nome e o valor da propriedade e defina o método de carregamento e a taxa base.</p> <ul style="list-style-type: none"> ■ Recorrente - Insira uma taxa base e defina o intervalo recorrente como o período de cobrança. O valor de taxa absoluta é necessário e é adicionado ao preço geral. ■ Único - Defina a cobrança da taxa base única. O valor absoluto é necessário e é adicionado como um preço único. ■ Fator de Taxa - É necessário um fator de multiplicação que é aplicado à categoria Selecionar Cobrança. <p>Selecione como cobrar a propriedade personalizada com base no estado ligado.</p> <p>Você pode adicionar várias propriedades personalizadas com taxas diferentes clicando em Adicionar Cobrança e configurando uma política de cobrança adicional.</p> |
| Cobranças Gerais | <p>Defina qualquer cobrança adicional que você gostaria de adicionar à política de preços. É possível adicionar tanto cobranças únicas quanto recorrentes.</p> |

Cobranças únicas não são mostradas na estimativa de preço de um item de catálogo ou na guia Resumo. Somente a estimativa diária de preços para um determinado item de catálogo é exibida.

- 5 Clique na guia **Atribuições** e em **Atribuir Projetos**. Selecione um ou mais projetos aos quais atribuir o cartão de preços.

Observação Por padrão, cartões de preços são aplicados a projetos. Na guia **Infraestrutura > Cartões de Preços**, você pode selecionar para aplicar cartões de preços a zonas de nuvem. Se zonas de nuvem tiverem sido selecionadas, clique em **Atribuir Zonas de Nuvem** na guia Atribuições.

- 6 Clique em **Criar** para salvar e criar sua política de preços.

Resultados

Sua nova política de preços aparece na página Cartões de Preços. Para exibir ou editar os detalhes e a configuração da política, clique em **Abrir**.

Como usar tags para gerenciar recursos e implantações do Cloud Assembly

As tags são um componente crítico do Cloud Assembly que orienta o posicionamento das implantações por meio da correspondência entre capacidades e restrições. É necessário compreender e implantar tags de forma eficaz para fazer o uso ideal do Cloud Assembly.

Fundamentalmente, as tags são rótulos adicionados aos itens do Cloud Assembly. É possível criar qualquer tag que seja apropriada para sua organização e implantação. As tags funcionam muito mais do que rótulos, pois elas controlam como e onde o Cloud Assembly usará recursos e infraestrutura para compilar serviços implantáveis. As tags também oferecem suporte ao controle dentro do Cloud Assembly.

Estrutura das tags

Estruturalmente, as tags devem seguir a convenção de par `name:value`, fora isso, sua construção é muito livre. No Cloud Assembly, todas as tags são exibidas do mesmo modo e a funcionalidade da tag é determinada pelo contexto.

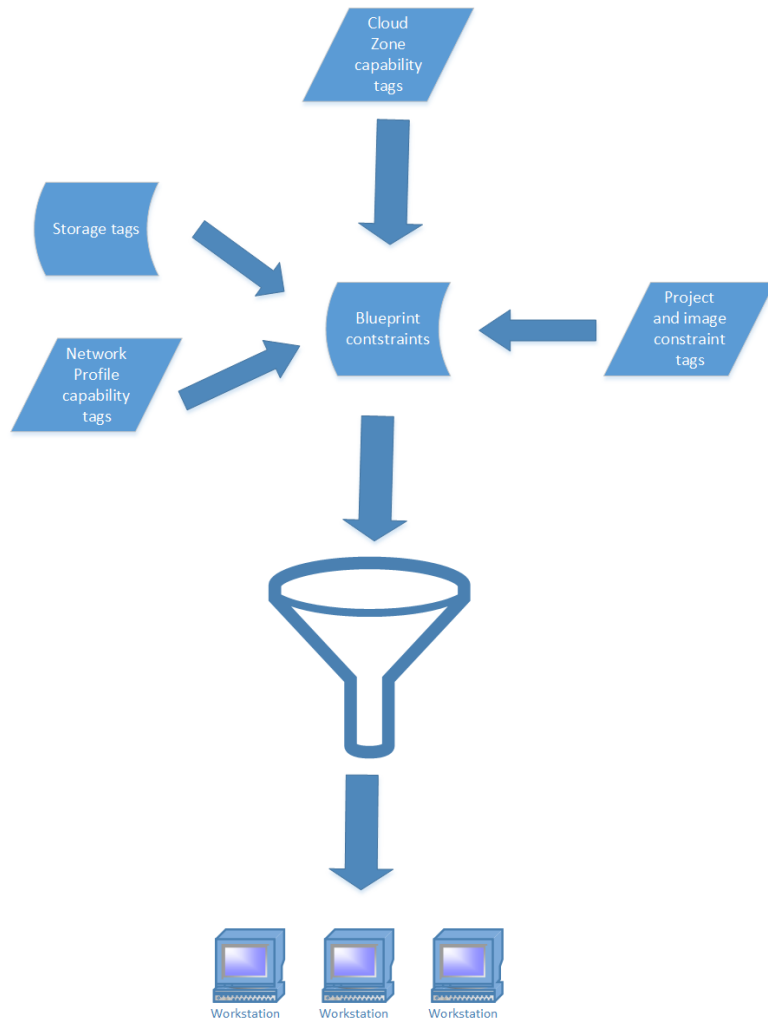
Por exemplo, tags em recursos de infraestrutura funcionam principalmente como tags de capacidade porque o Cloud Assembly as usa para corresponder recursos com implantações. Em segundo lugar, elas também identificam os recursos.

Função da tag

A função principal das tags é expressar recursos e restrições que o Cloud Assembly usa para definir implantações. O contexto determina a função das tags. As tags colocadas em zonas de nuvem, perfis de rede e armazenamento e recursos de infraestrutura individuais funcionam como tags de capacidade e definem os recursos desejados para a infraestrutura usada em implantações.

As tags colocadas em modelos de nuvem funcionam como restrições que definem recursos para implantações. Além disso, os administradores de nuvem podem colocar tags de restrição em projetos para exercer uma forma de controle sobre eles. Essas tags de restrição são adicionadas a outras restrições expressas nos modelos de nuvem.

Durante o provisionamento, o Cloud Assembly corresponde essas capacidades às restrições, também expressas como tags, nos modelos de nuvem para definir a configuração da implantação. Essa funcionalidade de recurso e restrição baseada em tags serve como base para a configuração de implantação no Cloud Assembly. Por exemplo, é possível usar tags para disponibilizar a infraestrutura somente nos recursos de PCI em uma determinada região.



Em um nível secundário, as tags também facilitam a pesquisa e identificação de itens de armazenamento, itens de rede e outros recursos de infraestrutura.

Por exemplo, suponha que esteja configurando as zonas de nuvem e tenha muitos recursos de processamento disponíveis. Se você marcou seus recursos de processamento adequadamente, poderá usar a função de pesquisa na guia Processamento da página Zona de Nuvem para filtrar os recursos associados a essa zona de nuvem específica.

Além disso, a página Gerenciamento de Tags e as páginas de configuração de recursos do Cloud Assembly contêm funções de pesquisa que permitem a localização de itens por nomes de tags. O uso de tags lógicas e legíveis para esses itens é fundamental para facilitar essa função de pesquisa e identificação.

Veja o seguinte vídeo do YouTube para obter mais informações e exemplos de uso de tags:

<https://youtu.be/4zNQ33RyQio>

Tags externas

O Cloud Assembly também pode conter tags externas. Essas tags são importadas automaticamente das contas de nuvem que são associadas a uma instância do Cloud Assembly. Essas tags podem ser importadas do vSphere, AWS, Azure ou outros produtos de software externos. Quando importadas, essas tags estão disponíveis para uso da mesma maneira que as tags criadas pelo usuário.

Como gerenciar tags

Você pode usar a página Gerenciamento de Tags no Cloud Assembly para monitorar e gerenciar sua biblioteca de tags. Também é possível criar tags nesta página. Além disso, a página Gerenciamento de Tags é a única página na qual é possível visualizar e identificar tags externas.

| Key | Value |
|---|--------------------------|
| <input type="checkbox"/> a | |
| <input type="checkbox"/> AAA | sofiaaaa |
| <input type="checkbox"/> aktag1 | vall |
| <input type="checkbox"/> alex | kris |
| <input type="checkbox"/> AppID | ABC |
| <input type="checkbox"/> AppID | XYZ |
| <input type="checkbox"/> applicationtier | tango-machine |
| <input type="checkbox"/> Application Tier | tango-machine |
| <input type="checkbox"/> Application Tier | |
| <input type="checkbox"/> astoyanov-rp | |
| <input type="checkbox"/> Atos-Tagging-Category | Atos-Storage-Tag |
| <input type="checkbox"/> AutomaticCleanExpirationTime | 2019-01-08T08:45:33.127Z |

Estratégia para tags

Para minimizar a confusão, antes de criar tags no Cloud Assembly, planeje uma estratégia e uma convenção de marcação adequada, para que todos os usuários que criam e usam tags compreendam o que elas significam e como devem ser usadas. Consulte [Criação de uma estratégia de marcação](#).

Criação de uma estratégia de marcação

É necessário planejar e implantar cuidadosamente uma estratégia de marcação apropriada com base na estrutura de TI e nas metas da organização, para maximizar a funcionalidade do Cloud Assembly e minimizar as possíveis confusões.

Embora a marcação atenda a várias finalidades comuns, a estratégia de marcação deve ser adaptada às necessidades da implantação, estrutura e metas.

Práticas recomendadas para marcação

Algumas características gerais de uma estratégia de tag eficiente:

- Projete e implante uma estratégia coerente para marcação, que esteja relacionado à estrutura da empresa e comunique esse plano para todos os usuários aplicáveis. Uma estratégia deve oferecer suporte a suas necessidades de implantação, usar um idioma claro legível e ser compreensível para todos os usuários aplicáveis.
- Use nomes e valores simples, claros e significativos para as tags. Por exemplo, os nomes de tag para itens de armazenamento e de rede devem ser claros e coerentes, para que os usuários possam rapidamente entender que estão selecionando ou revisando atribuições de tags para um recurso implantado.
- Embora seja possível criar tags usando um nome sem valor, como boas práticas, é mais apropriado criar um valor aplicável para cada nome de tag, para tornar claro o uso da tag para outros usuários.
- Evite criar tags duplicadas ou estranhas. Por exemplo, crie tags apenas em itens de armazenamento relacionados a problemas de armazenamento.

Implementação da marcação

Mapeie as considerações principais para uma estratégia básica de marcação. A lista a seguir mostra considerações típicas a serem consideradas ao mapear sua estratégia. Lembre-se de que essas considerações são representativas ao invés de definitivas. É possível ter outras considerações altamente relevantes para seus casos de uso. A estratégia específica deve ser apropriada para seus casos de uso específicos.

- Quantos ambientes diferentes você implanta. Normalmente, serão criadas tags que representam cada ambiente.
- Como os recursos de processamento são estruturados e usados para oferecer suporte a implantações.
- Quantas regiões ou localizações diferentes você implanta. Normalmente, serão criadas tags no nível do perfil, que representam cada uma dessas diferentes regiões ou localizações.
- Quantas opções de armazenamento diferentes estão disponíveis para implantações e como deseja-se caracterizá-las. Essas opções devem ser representadas por tags.
- Categorize as opções de rede e crie tags para acomodar todas as opções aplicáveis.

- Variáveis de implantação típicas. Por exemplo, quantos ambientes diferentes são implantados. Normalmente, muitas organizações têm no mínimo ambientes de teste, desenvolvimento e produção. Poderá se desejar criar e coordenar tags de restrição e tags de recurso da zona de nuvem correspondentes, para que seja possível configurar facilmente as implantações em um ou mais desses ambientes.
- Tags de coordenadas nos recursos de rede e de armazenamento, para que façam sentido lógico no contexto dos perfis de rede e de armazenamento nos quais elas são usadas. As tags de recursos podem servir como um nível mais refinado de controle sobre a implantação de recursos.
- Coordene as tags de recurso do perfil de rede e da zona de nuvem e outras tags de recurso com tags de restrição. Normalmente, seu administrador criará tags de recurso para zonas de nuvem e perfis de rede primeiro e, em seguida, outros usuários poderão projetar modelos de nuvem com restrições que correspondam a essas tags de recurso.

Depois de compreender as considerações importantes da organização, pode-se planejar os nomes de tag apropriados que abordam essas considerações de maneira lógica. Em seguida, crie uma descrição da sua estratégia e torne-a disponível para todos os usuários com privilégios para criar ou editar tags.

Como uma abordagem de implantação útil, é possível começar marcando individualmente todos os seus recursos de infraestrutura de cálculo. Conforme observado, use categorias lógicas para nomes de tag relacionados ao recurso específico. Por exemplo, pode-se marcar recursos de armazenamento como tier1, tier2, etc. Além disso, é possível marcar recursos de processamento com base no sistema operacional, como Windows, Linux, etc.

Depois de marcar os recursos, pode-se considerar a abordagem de criação de tags para a zona de nuvem e os perfis de rede e armazenamento que melhor atendam às necessidades.

Como usar tags de capacidade no Cloud Assembly

No Cloud Assembly, as tags de capacidade permitem definir recursos de implantação de componentes de infraestrutura. Juntamente com as restrições, elas funcionam como a base da lógica de posicionamento no vRealize Automation.

É possível criar tags de capacidade em recursos de processamento, zonas de nuvem, imagens e mapas de imagem, além de redes e perfis de rede. As páginas para criar esses recursos contêm opções para a criação de tags de capacidade. Como alternativa, é possível usar a página Gerenciamento de Tags no Cloud Assembly para criar tags de capacidade. As tags de capacidade em zonas de nuvem e perfis de rede afetam todos os recursos dentro da zona ou dos perfis. As tags de capacidade no armazenamento ou nos componentes de rede afetam apenas os componentes nos quais elas são aplicadas.

Normalmente, as tags de capacidade podem definir características, como localização para um recurso de processamento, tipo de adaptador para uma rede ou nível de camada para um recurso de armazenamento. Elas também podem definir o local ou o tipo de ambiente e outras considerações de negócios. Assim como na estratégia de marcação geral, é necessário organizar as tags de capacidade de maneira lógica para suas necessidades de negócios.

O Cloud Assembly corresponde tags de capacidade de zonas de nuvem com restrições em modelos de nuvem no momento da implantação. Portanto, ao criar e usar tags de capacidade, é necessário compreender e planejar para criar restrições de modelo de nuvem apropriadas para que a correspondência ocorra conforme o esperado.

Por exemplo, a seção da zona de nuvem no [Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo](#) incluído na documentação, descreve como criar tags de desenvolvimento e teste para as zonas de nuvem OurCo-AWS-US-East e OurCo AWS-US-West. Nesse tutorial, essas tags indicam que a zona OurCo-AWS-US-East é um ambiente de desenvolvimento e a zona OurCo-AWS-US_ West é um ambiente de teste. Se você criar tags de restrição análogas em modelos de nuvem, essas tags de capacidade permitirão direcionar implementações aos ambientes desejados.

Herança de tags

O Cloud Assembly usa a herança de tags para propagar tags seletivamente em contas de nuvem para outro recurso relacionado. Especificamente, quando você cria tags em uma conta de nuvem, elas também se tornam efetivas em todos os perfis de armazenamento e recursos de cálculo que correspondem a essa conta de nuvem.

Observação O comportamento de propagação de tag não se aplica a perfis de armazenamento. O vRealize Automation não selecionará automaticamente a restrição para perfis de armazenamento, portanto, os usuários devem adicionar manualmente a tag de restrição necessária para que ela seja selecionada e aplicada aos perfis de armazenamento.

O exemplo a seguir ilustra como funciona a herança de tags.

Recursos de processamento

- Cluster1 com a tag cluster-1
- Cluster2 com a tag cluster-2
- Cluster3 com a tag cluster-3

```
Vm resource:
  properties:
    constraints:
      - tag: 'cluster-01'
```

Perfis de armazenamento

- Perfil 1 para Datastorecluster1 com a tag storage-01
- Perfil 2 para Datastorecluster2 com a tag storage-02
- Perfil 3 para Datastorecluster3 com a tag storage-03

```
vm-resource:
  properties:
    storage:
```

```
constraints:
  - tag: 'storage-01'
```

Conta de Nuvem

Conta de nuvem do vSphere com todas as três tags: cluster-1, cluster-2 e cluster-3

Durante a consolidação de tags em perfis de armazenamento e recursos de processamento, o Cloud Assembly também leva em conta as tags no nível da conta de nuvem. Portanto, as tags efetivas em todos os perfis de armazenamento e processamentos são cluster-1, cluster-2 e cluster-3 e é por isso que, quando fornecemos qualquer uma dessas tags, como mostra o exemplo anterior, todos os perfis de armazenamento e processamentos se tornam elegíveis para posicionamento, e a máquina pode chegar em qualquer um dos hosts de processamento.

Como prática recomendada, para minimizar resultados inesperados e a aglomeração de tags, qualquer tag especificada deverá ser aplicada somente no nível da conta de nuvem se essa tag for um recurso apropriado para todos os recursos de processamento e armazenamento subordinados.

Como usar tags de restrição no Cloud Assembly

As tags adicionadas aos projetos e modelos de nuvem funcionam como tags de restrição quando são usadas para corresponder a tags de capacidade em recursos de infraestrutura, perfis e zonas de nuvem. No caso dos modelos de nuvem, o Cloud Assembly usa essa funcionalidade correspondente para alocar recursos para implantações.

O Cloud Assembly permite que você use as tags de restrição de duas maneiras principais. A primeira forma é ao configurar projetos e imagens. Você pode usar tags como restrições para associar recursos ao projeto ou imagem. A segunda está em modelos de nuvem em que as tags especificadas como restrições são usadas para selecionar recursos para implantações. As restrições aplicadas em ambas as formas são mescladas em modelos de nuvem para formar um conjunto de requisitos de implantação que definem os recursos disponíveis para uma implantação.

Como as tags de restrição funcionam em projetos

Ao configurar os recursos do Cloud Assembly, os administradores de nuvem podem aplicar tags de restrição em projetos. Dessa forma, os administradores podem aplicar restrições de governança diretamente no nível do projeto. Todas as restrições adicionadas neste nível são aplicadas a todos os modelos de nuvem solicitados para o projeto aplicável, e essas tags de restrição têm precedência sobre outras tags.

Se as tags de restrição estiverem em conflito com as tags de restrição no modelo de nuvem, as tags de projeto terão precedência, permitindo assim que o administrador de nuvem aplique regras de governança. Por exemplo, se os administradores de nuvem criarem uma tag `location:london` no projeto, mas um desenvolvedor colocar uma tag `location:boston` no modelo de nuvem, a primeira terá precedência e o recurso será implantado na infraestrutura que contém a tag `location:london`.

Existem três tipos de tags de restrições que os usuários podem aplicar em projetos: rede, armazenamento e extensibilidade. Você pode aplicar quantas instâncias de cada tipo de tag forem necessárias. As restrições do projeto podem ser rígidas ou flexíveis. Por padrão, elas são rígidas. As restrições rígidas permitem que você aplique restrições de implantação de forma rígida. Se uma ou mais restrições rígidas não forem atendidas, a implantação falhará. As restrições flexíveis oferecem uma maneira de expressar as preferências que serão selecionadas, se disponíveis, mas a implantação não falhará caso as restrições flexíveis não sejam atendidas.

Como tags de restrição funcionam em modelos de nuvem

Em modelos de nuvem, você adiciona tags de restrição a recursos como código do YAML para corresponder às tags de recurso apropriadas que seu administrador de nuvem criou nos recursos, nas zonas de nuvem e nos perfis de rede e armazenamento. Além disso, há outras opções mais complexas para implantar tags de restrição. Por exemplo, é possível usar uma variável para preencher uma ou mais tags em uma solicitação. Isso permite que especifique uma ou mais tags no momento da solicitação.

Crie tags de restrição usando o rótulo `tag` sob um título de restrição no código YAML do modelo de nuvem. As tags de restrição de projetos são adicionadas às tags de restrição criadas em modelos de nuvem.

O Cloud Assembly suporta uma formatação de cadeia de caracteres simples para facilitar o uso de restrições nos arquivos YAML:

```
[!]tag_key[:tag_value][:hard|:soft]
```

Por padrão, o Cloud Assembly cria uma restrição positiva com aplicação rígida. O valor da tag é opcional, embora recomendado, como no restante do aplicativo.

O exemplo a seguir do WordPress com MySQL mostra tags de restrição do YAML com informações de localização específicas para recursos de processamento.

```
name: "wordpressWithMySQL"
components:
  mysql:
    type: "Compute"
    data:
      name: "mysql"
      # ... skipped lines ...
  wordpress:
    type: "Compute"
    data:
      name: "wordpress"
      instanceType: small
      imageType: "ubuntu-server-1604"
      constraints:
        - tag: "!location:eu:hard"
        - tag: "location:us:soft"
        - tag: "!pci"
      # ... skipped lines ...
```

Para obter mais informações sobre como trabalhar com modelos de nuvem, consulte [Parte 3: Projetar e implantar o exemplo de modelo do Cloud Assembly](#).

Como restrições rígidas e flexíveis funcionam em projetos e modelos de nuvem

As restrições em projetos e modelos de nuvem podem ser rígidas ou flexíveis. O trecho de código anterior mostra exemplos de restrições rígidas e flexíveis. Por padrão, todas as restrições são rígidas. As restrições rígidas permitem que você aplique restrições de implantação de forma rígida. Se uma ou mais restrições rígidas não forem atendidas, a implantação falhará. Restrições flexíveis expressam preferências aplicáveis, se disponíveis, mas não implicam em falha da implantação se não forem atendidas.

Se houver uma série de restrições rígidas e flexíveis em relação a um tipo de recurso específico, as restrições flexíveis também poderão servir como fator de decisão. Ou seja, se vários recursos atenderem a uma restrição rígida, as restrições flexíveis serão usadas para selecionar o recurso real usado na implantação.

Por exemplo, digamos que você crie uma restrição de armazenamento rígida com uma tag de `location:boston`. Se nenhum armazenamento no projeto corresponder a essa restrição, qualquer implantação relacionada falhará.

Tags padrão

O Cloud Assembly aplica tags padrão a algumas implantações para oferecer suporte à análise, ao monitoramento e ao agrupamento de recursos implantados.

As tags padrão são exclusivas no Cloud Assembly. Ao contrário de outras tags, os usuários não funcionam com elas durante a configuração da implantação e nenhuma restrição é aplicada. Essas tags são aplicadas automaticamente durante o provisionamento em implantações do AWS, Azure e vSphere. Essas tags são armazenadas como propriedades personalizadas do sistema e são adicionadas às implantações após o provisionamento.

A lista de tags padrão é exibida abaixo.

Tabela 4-3. Tags padrão

| Descrição | Tag |
|--|---|
| Organização | <code>org:orgID</code> |
| Projeto | <code>project:projectID</code> |
| Solicitante | <code>requester:username</code> |
| Implantação | <code>deployment:deploymentID</code> |
| Referência de modelo de nuvem (se aplicável) | <code>blueprint:blueprintID</code> |
| Nome do componente no blueprint | <code>blueprintResourceName:CloudMachine_1</code> |
| Restrições de colocação: aplicadas no blueprint, parâmetros de solicitação ou por política de TI | <code>constraints:key:value:soft</code> |

Tabela 4-3. Tags padrão (continuação)

| Descrição | Tag |
|------------------------------|--|
| Conta de Nuvem | cloudAccount:accountID |
| Zona ou perfil, se aplicável | zone:zoneID, networkProfile:profileID, storageProfile:profileID |

Como o Cloud Assembly processa tags

No Cloud Assembly, as tags expressam capacidades e restrições expressas que determinam como e onde os recursos são alocados para implantações provisionadas durante o processo de provisionamento.

O Cloud Assembly usa uma ordem específica e uma hierarquia de operações na resolução de tags para criar implantações provisionadas. A compreensão dos fundamentos desse processo ajudará a implantar tags de forma eficiente para criar implantações previsíveis.

A lista a seguir resume as operações de alto nível e a sequência que o Cloud Assembly usa para resolver tags e definir uma implantação:

- As zonas de nuvem são filtradas por vários critérios, incluindo disponibilidade e perfis; as tags nos perfis da região à qual zona pertencem devem ser compatíveis neste ponto.
- As tags de capacidade de zona e processamento são usadas para filtrar as zonas de nuvem restantes por restrições rígidas.
- Das zonas filtradas, a prioridade é usada para selecionar uma zona de nuvem. Se houver várias zonas de nuvem com a mesma prioridade, elas serão classificadas por restrições flexíveis, usando uma combinação da zona de nuvem e das capacidades de processamento.
- Após a seleção de uma zona de nuvem, um host é selecionado combinando uma série de filtros, incluindo as restrições rígidas e flexíveis, como expressas em modelos de nuvem.

Como configurar uma estrutura de marcação simples

Este tópico descreve uma abordagem básica e opções para uma estratégia lógica de adição de tags do Cloud Assembly. É possível usar esses exemplos como ponto de partida para uma implantação real ou planejar uma estratégia diferente que atenda melhor às suas necessidades.

Normalmente, o administrador de nuvem é a principal pessoa responsável pela criação e manutenção de tags.

Este tópico se refere ao caso de uso do WordPress descrito em algum lugar na documentação do Cloud Assembly para ilustrar como as tags podem ser adicionadas a alguns itens principais. Ele também descreve possíveis alternativas e extensões para os exemplos de marcação que aparecem no caso de uso do WordPress.

Consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#) para obter mais informações sobre o caso de uso do WordPress.

O caso de uso do WordPress descreve como colocar tags em zonas de nuvem e perfis de rede e armazenamento. Esses perfis são como pacotes organizados de recursos. As tags colocadas nos perfis se aplicam a todos os itens no perfil. Também é possível criar e colocar tags em recursos de armazenamento e itens de rede individuais, bem como em recursos de processamento, mas essas tags se aplicam apenas aos recursos específicos nos quais elas são colocadas. Ao configurar tags, normalmente é melhor começar marcando os recursos de processamento e depois é possível adicionar tags a perfis e zonas de nuvem mais tarde. Além disso, essas tags são usadas para filtrar a lista de recursos de processamento para uma zona de nuvem.

Por exemplo, embora seja possível colocar tags em perfis de armazenamento conforme mostrado neste caso de uso, também é possível colocar tags em políticas de armazenamento individuais, armazenamentos de dados e contas de armazenamento. As tags nesses recursos permitem exercer um melhor controle sobre como os recursos de armazenamento são implantados. Durante o processamento na preparação para implantação, essas tags são resolvidas como um nível seguinte de processamento após as tags de perfil.

Como exemplo de como é possível configurar um cenário típico do cliente, coloque uma tag de `region: eastern` em um perfil de rede. Essa tag se aplicaria a todos os recursos nesse perfil. Em seguida, é possível colocar uma tag de `networktype: pci` em um recurso de rede PCI no perfil. Um modelo de nuvem com restrições de leste e PCI criaria implantações que usam esta rede PCI para a região leste.

Procedimentos

- 1 Marque os recursos de infraestrutura de processamento de maneira lógica e apropriada.

É especialmente importante marcar os recursos de processamento de forma lógica para que possa encontrá-los usando a função de pesquisa na guia Processamento da página Criar Zona de Nuvem. Usando essa função de pesquisa, é possível filtrar rapidamente os recursos de processamento associados a uma zona de nuvem. Se você marcar o armazenamento e as redes no nível do perfil, talvez não seja necessário marcar os recursos individuais de armazenamento e rede.

- a Selecione **Recursos > Processamento** para exibir os recursos de processamento importados para sua instância do Cloud Assembly.
- b Selecione cada recurso de processamento conforme apropriado e clique em **Tags** para adicionar uma tag ao recurso. É possível adicionar mais de uma tag a cada recurso, se apropriado.
- c Repita a etapa anterior para recursos de armazenamento e rede conforme apropriado.

- 2 Crie tags de capacidade do perfil de rede e da zona de nuvem.

É possível usar as mesmas tags para zonas de nuvem e perfis de rede ou criar tags exclusivas para cada item, caso isso faça mais sentido para a sua implementação.

Em perfis de rede, é possível colocar tags em todo o perfil, bem como em sub-redes no perfil. As tags aplicadas no nível do perfil aplicam-se a todos os componentes, como sub-redes, nesse perfil. As tags nas sub-redes aplicam-se apenas à sub-rede específica na qual elas são colocadas. Durante o processamento de tags, as tags de nível de perfil têm precedência sobre as tags de nível de sub-rede.

Para obter informações sobre como adicionar tags a zonas de nuvem ou perfis de rede, consulte as seções de rede e zona de nuvem do [Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo](#).

Neste exemplo, foram criadas três tags simples que aparecem ao longo da documentação sobre tags de zona de nuvem e perfil de rede do Cloud Assembly. Essas tags identificam o ambiente dos componentes do perfil.

- `zone:test`
- `zone:dev`
- `zone:prod`

3 Crie tags de perfil de armazenamento para os componentes de armazenamento.

Normalmente, as tags de armazenamento identificam o nível de desempenho dos itens de armazenamento, como tier1 ou tier2, mas também identificam a natureza dos itens de armazenamento, como PCI.

Para obter informações sobre como adicionar tags a perfis de armazenamento, consulte a seção de armazenamento do [Parte 1: Configurar a infraestrutura do Cloud Assembly de exemplo](#).

- `usage:general`
- `usage:fast`

Resultados

Depois de criar uma estrutura básica de adição de tags, será possível começar a trabalhar com ela e adicionar ou editar tags conforme apropriado para refinar e estender as capacidades de marcação.

Como trabalhar com recursos no vRealize Automation

Um administrador de nuvem pode revisar recursos do vRealize Automation que são expostos por meio da coleta de dados.

O administrador de nuvem pode rotular recursos com tags de capacidade para afetar onde os modelos de nuvem do vRealize Automation são implantados.

Além das exibições fornecidas aqui, você também pode gerenciar vários recursos usando a guia Recursos. Consulte [Gerenciando recursos no Cloud Assembly](#).

Recursos de processamento no vRealize Automation

Um administrador de nuvem pode revisar os recursos de processamento que são expostos por meio da coleta de dados.

O administrador de nuvem pode optar por aplicar tags diretamente nos recursos, para rotular capacidades para fins de correspondência no provisionamento do vRealize Automation.

Recursos de rede no vRealize Automation

No vRealize Automation, os administradores de nuvem podem visualizar e editar os recursos de rede que foram coletados por dados das contas de nuvem e integrações que são mapeadas para o seu projeto.

Depois de adicionar uma conta de nuvem à sua infraestrutura do Cloud Assembly, por exemplo, usando a sequência de menus **Infraestrutura > Conexões > Contas de Nuvem**, a coleta de dados descobre as informações de rede e segurança da conta de nuvem. Essas informações são disponibilizadas para uso em redes, perfis de rede e outras definições.

As redes são os componentes específicos de IP de um domínio de rede ou zona de transporte disponível. Se você for um usuário do Amazon Web Services ou Microsoft Azure, pense nas redes como sub-redes.

Você pode exibir informações sobre as redes no seu projeto usando a página **Infraestrutura > Recursos > Redes**.

A página **Redes** do Cloud Assembly contém informações como:

- Redes e balanceadores de carga definidos externamente no domínio de rede da conta de nuvem, por exemplo, no vCenter, no NSX-T ou no Amazon Web Services.
- Redes e balanceadores de carga implantados pelo administrador da nuvem.
- Intervalos de IP e outras características de rede definidas ou modificadas pelo administrador de nuvem.
- Os intervalos de IP do provedor de IPAM externo para um determinado espaço de endereço em uma integração de IPAM externa específica do provedor.

Para obter mais informações sobre redes, consulte as seguintes informações, a ajuda de sinalização para várias configurações na página **Redes** e o [Saiba mais sobre perfis de rede no vRealize Automation](#).

Redes

É possível visualizar e editar redes e suas características, por exemplo, para adicionar tags ou remover o suporte ao acesso IP público. Você também pode gerenciar configurações de rede como DNS, CIDR, gateway e valores de tag. Você também pode definir novos intervalos de IPs, e gerenciar os existentes, dentro de uma rede.

Para redes existentes, é possível alterar o intervalo de IP e as configurações de marca selecionando a caixa de seleção da rede e selecionando **Gerenciar Intervalos de IP** ou **Tags**. Caso contrário, é possível selecionar a rede em si para editar as informações.

As tags fornecem um meio para corresponder redes apropriadas e opcionalmente perfis de rede a componentes de rede em modelos de nuvem. As tags de rede são aplicadas a cada instância dessa rede, independentemente de qualquer perfil de rede no qual a rede possa residir. As redes podem ser modeladas em qualquer número de perfis de rede. Independentemente da residência do perfil de rede, uma tag de rede será associada a essa rede onde quer que a rede seja usada. A correspondência de tags de rede ocorre com outros componentes no modelo de nuvem depois que o modelo de nuvem é correspondido com um ou mais perfis de rede.

Para redes globais, as redes existentes e públicas têm suporte para as contas de nuvem de gerenciador global e gerenciador local do NSX-T e para as contas de nuvem do vCenter que estão associadas aos gerenciadores locais. A representação do gerenciador local de redes estendidas é definida dentro de uma zona de transporte. A zona de transporte é uma construção do gerenciador local do NSX-T que define a extensão de redes do NSX-T para hosts e clusters do vCenter Server.

O Cloud Assembly enumera as redes existentes e públicas ou faz a coleta de dados dessas redes. Você pode criar uma rede global adicionando uma rede existente ou pública a um gerenciador global do NSX-T. Essa rede global pode então ser consumida por todos os gerenciadores locais associados. Redes globais podem abranger um, todos ou um subconjunto dos gerenciadores locais associados.

Você pode provisionar uma máquina em uma rede global usando uma atribuição de IP estático. Não há suporte para o DHCP.

É possível criar os seguintes tipos de redes globais em um gerenciador global:

- 1 Sobreposição: uma rede de sobreposição está associada a um gerenciador local de Camada 0/Camada 1 e se estende automaticamente a todos os sites conectados ao gerenciador local de Camada 0/Camada 1. Para cada gerenciador local, a zona de transporte de sobreposição padrão é usada.
- 2 VLAN: uma rede VLAN aplica-se a um único gerenciador local, e a zona de transporte pode ser selecionada manualmente.

Redes globais estão listadas na página **Infraestrutura > Recursos** com todas as contas de nuvem às quais elas se aplicam.

As seguintes operações de Dia 2 são compatíveis com redes globais:

- Reconfigurar uma rede em uma definição de modelo de nuvem a partir de uma rede global para uma rede local, e vice-versa.
- Expandir máquinas horizontalmente/verticalmente em redes globais.

Para obter mais informações sobre o uso de redes em modelos de nuvem, consulte [Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation](#).

Para obter informações sobre como atualizar redes do vSphere no vRealize Automation após a migração do NSX-T de N-VDS para C-VDS, consulte [Atualizando recursos de rede no vRealize Automation após a migração de N-VDS para C-VDS no NSX-T](#).

Intervalos de IPs

Use um intervalo de IPs para definir ou fazer alterações nos endereços IP inicial e final de uma determinada rede na sua organização. É possível exibir e gerenciar intervalos de IPs para redes listadas. Se a rede for gerenciada por um provedor de IPAM externo, você poderá gerenciar intervalos de IPs em conexão com o ponto de integração de IPAM associado.

Clique em **Novo Intervalo de IP** para adicionar outro intervalo de IPs à rede. É possível especificar um **intervalo de IPs interno** ou, se houver uma integração válida de IPAM disponível, você poderá especificar um **Intervalo de IPs externo**.

Não é possível incluir o gateway padrão em um intervalo de IPs. O intervalo de IPs de sub-rede não pode incluir o valor do gateway de sub-rede.

Se você estiver usando uma integração de IPAM externo para um provedor de IPAM específico, poderá usar o **Intervalo de IPs externo** para selecionar um intervalo de IPs de um ponto de integração de IPAM externo disponível. Esse processo está descrito no contexto de um fluxo de trabalho de integração de IPAM externo geral em [Configurar uma rede e um perfil de rede para usar o IPAM externo em uma rede existente no vRealize Automation](#).

Observação Quando um intervalo de IPs de um provedor IPAM externo é excluído no aplicativo IPAM externo, esse intervalo é excluído automaticamente durante a enumeração no vRealize Automation. O intervalo de IPs excluído não fica mais visível ou disponível para associação de rede no vRealize Automation, evitando assim intervalos de endereços IP órfãos.

O vRealize Automation permite que você aplique e gerencie um intervalo de endereços IP em várias redes do vSphere e do NSX. O suporte a intervalos de IP compartilhados é fornecido para o IPAM interno e externo. Você pode definir um único intervalo de IPs em uma rede ampliada do NSX de tal forma que as máquinas nessa rede possam usar endereços IP atribuídos a partir de um único endereço IP, mesmo que sejam implantados em vCenters diferentes.

Endereços IP

É possível ver os endereços IP que estão sendo usados pela sua organização e exibir seu status, por exemplo `available` ou `allocated`. Os endereços IP exibidos são endereços IP gerenciados internamente por vRealize Automation ou endereços IP designados para implantações que contêm uma integração de provedor de IPAM externo. Os provedores de IPAM externos gerenciam sua própria alocação de endereços IP.

Se a rede for gerenciada internamente pelo vRealize Automation e não por um provedor de IPAM externo, você também poderá liberar endereços IP.

Ao usar o IPAM interno e liberar endereços IP, por exemplo, depois de excluir uma máquina que estava usando os endereços IP ou clicar em **Liberar endereço IP** para uma rede selecionada, há um período de espera entre o momento em que os endereços não utilizados são liberados e o momento em que eles ficam disponíveis para reutilização. O período de espera, ou o tempo limite de liberação, permite que o cache de DNS seja apagado. Os endereços IP podem então ser alocados a uma nova máquina. Por padrão, o período de espera para liberação do endereço IP é de 30 minutos. Você pode alterar esse período de espera clicando na opção **Configurações** no canto superior direito da página **Redes** e alterando o valor de **Tempo limite de liberação**.

- Durante o tempo limite de liberação, os endereços IP relevantes são listados como liberados. Quando o período de tempo limite para liberação tiver expirado, eles serão listados como disponíveis.
- O sistema verifica a cada 5 minutos os endereços IP recém-lançados e, portanto, mesmo que o valor do tempo limite para liberação seja 1 minuto, pode levar de 1 a 6 minutos para que os endereços IP liberados se tornem disponíveis, dependendo de quando a última verificação foi executada. O intervalo de verificação de 5 minutos aplica-se a todos os valores diferentes de 0.
- Se você definir o valor de tempo limite para liberação como 0, os endereços IP serão liberados imediatamente e se tornarão disponíveis imediatamente.
- O valor de tempo limite de liberação aplica-se a todas as contas de nuvem na organização.

Balanceadores de carga

Você pode gerenciar informações sobre balanceadores de carga disponíveis para as contas de nuvem de conta/região na sua organização. Você pode abrir e exibir as configurações definidas para cada balanceador de carga disponível. Também pode adicionar e remover tags para um balanceador de carga.

Para obter mais informações sobre como usar balanceadores de carga em modelos de nuvem, consulte [Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation](#).

Domínios de Rede

A lista de domínios de rede contém redes relacionadas e não sobrepostas.

Recursos de segurança no vRealize Automation

Depois de adicionar uma conta de nuvem no Cloud Assembly, a coleta de dados descobre as informações de rede e segurança da conta na nuvem e as disponibiliza para uso em perfis de rede e outras opções.

Grupos de segurança e regras de firewall oferecem suporte ao isolamento de rede. Grupos de segurança são coletados por dados. Regras de firewall não são coletadas por dados.

Usando a sequência de menu **Infraestrutura > Recursos > Segurança**, é possível visualizar grupos de segurança sob demanda que foram criados em designs de modelo de nuvem do Cloud Assembly e grupos de segurança existentes que foram criados em aplicativos de origem, como o NSX-T e o Amazon Web Services. Os grupos de segurança disponíveis são expostos pelo processo de coleta de dados.

Você pode usar uma tag para corresponder a interface de máquina (NIC) com um grupo de segurança em uma definição de modelo de nuvem ou em um perfil de rede. Você pode visualizar os grupos de segurança disponíveis e adicionar ou remover tags para os grupos de segurança selecionados. Um autor de modelo de nuvem pode atribuir um ou mais grupos de segurança a uma NIC de máquina para controlar a segurança da implantação.

No design de modelo de nuvem, o parâmetro `securityGroupType` no recurso de grupo de segurança é especificado como `existing` para um grupo de segurança existente ou como `new` para um grupo de segurança sob demanda.

Grupos de segurança existentes

Os grupos de segurança existentes são exibidos e classificados na coluna **Origem** como `Discovered`.

Os grupos de segurança existentes do endpoint da conta de nuvem subjacente, como aplicativos NSX-V, NSX-T ou Amazon Web Services, estão disponíveis para uso.

Um administrador de nuvem pode atribuir uma ou mais tags a um grupo de segurança existente para permitir que ele seja usado em um modelo de nuvem. Um autor de modelo de nuvem pode usar um recurso `Cloud.SecurityGroup` em um design de modelo de nuvem para alocar um grupo de segurança existente usando restrições de tag. Um grupo de segurança existente requer que pelo menos uma tag de restrição seja especificada no recurso de segurança no design de modelo de nuvem.

Se você editar um grupo de segurança existente diretamente no aplicativo de origem, como no aplicativo NSX de origem, em vez de no Cloud Assembly, as atualizações não ficarão visíveis no Cloud Assembly até que a coleta de dados seja executada e os dados colem a conta de nuvem associada ou o ponto de integração de dentro do Cloud Assembly. A coleta de dados é executada automaticamente a cada 10 minutos.

Grupos de segurança existentes têm suporte para contas de nuvem de gerenciadores globais e locais do NSX-T e para as contas de nuvem do vCenter que estão associadas aos gerenciadores locais. O Cloud Assembly enumera grupos de segurança existentes, ou faz a coleta de dados desses grupos, e os anexa às interfaces de rede (NICs) da máquina. Você pode criar um grupo de segurança global adicionando um grupo de segurança existente a um gerenciador global do NSX-T. Em seguida, o grupo de segurança global pode ser consumido pelos gerenciadores locais associados. Grupos de segurança globais podem abranger um, todos ou um subconjunto dos gerenciadores locais associados.

- Grupos de segurança existentes globais são suportados e enumerados para todas as regiões definidas.

- Grupos de segurança globais estão listados na página **Infraestrutura > Recursos** com todas as contas de nuvem às quais eles se aplicam.
- Você pode associar uma interface de máquina (NIC) a um grupo de segurança global existente diretamente em um modelo de nuvem ou no perfil de rede selecionado.
- As seguintes operações de Dia 2 são compatíveis com grupos de segurança globais:
 - Reconfiguração do grupo de segurança em um modelo de nuvem de um grupo de segurança global para local, e vice-versa.
 - Expansão horizontal/vertical de máquinas que estão associadas a grupos de segurança globais.

Grupos de segurança sob demanda

Os grupos de segurança sob demanda que você cria no Cloud Assembly, seja em um modelo de nuvem ou em um perfil de rede, são exibidos e classificados na coluna **Origem** como *Managed by Cloud Assembly*. Os grupos de segurança sob demanda que você cria como parte de um perfil de rede são classificados internamente como um grupo de segurança de isolamento com regras de firewall pré-configuradas e não são adicionados a um design de modelo de nuvem como um recurso de grupo de segurança. Os grupos de segurança sob demanda que você cria em um design de modelo de nuvem e que podem conter regras de firewall expressas são adicionados como parte de um recurso de grupo de segurança que é classificado como *new*.

Observação Você pode criar regras de firewall para grupos de segurança sob demanda para o NSX-V e o NSX-T diretamente em um recurso de grupo de segurança no código do design de modelo de nuvem. A coluna **Aplicado a** não contém grupos de segurança classificados ou gerenciados por um Firewall Distribuído (DFW) do NSX. Regras de firewall válidas para aplicativos são para o tráfego do DFW leste/oeste. Algumas regras de firewall apenas podem ser gerenciadas no aplicativo de origem e não podem ser editadas no Cloud Assembly. Por exemplo, as regras de Ethernet, emergência, infraestrutura e ambiente são gerenciadas no NSX-T.

Grupos de segurança sob demanda não têm suporte no momento para contas de nuvem de gerenciadores globais do NSX-T.

Saiba mais

Para obter mais informações sobre como usar grupos de segurança em perfis de rede, consulte [Saiba mais sobre perfis de rede no vRealize Automation](#).

Para obter informações sobre como definir regras de firewall, consulte [Usando configurações de grupos de segurança em perfis de rede e designs de modelo de nuvem no vRealize Automation](#).

Para obter mais informações sobre como usar grupos de segurança em um modelo de nuvem, consulte [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#).

Para obter exemplos de códigos de design de modelo de nuvem que contêm grupos de segurança, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Recursos de armazenamento no vRealize Automation

Um administrador de nuvem pode trabalhar com recursos de armazenamento e suas capacidades descobertas por meio da coleta de dados do vRealize Automation das contas de nuvem associadas.

As capacidades dos recursos de armazenamento são expostas por meio de tags que normalmente são originadas na conta de nuvem de origem. Um administrador de nuvem pode optar por aplicar tags adicionais diretamente aos recursos de armazenamento, usando o Cloud Assembly. As tags adicionais podem rotular um recurso específico para fins de correspondência no momento do provisionamento.

O vRealize Automation é compatível com o disco padrão e com os recursos de disco de primeira classe. Os discos de primeira classe estão disponíveis apenas para vSphere.

- [O que posso fazer com o armazenamento em disco padrão no vRealize Automation](#)
- [O que posso fazer com o armazenamento em disco de primeira classe no vRealize Automation](#)

As capacidades dos recursos de armazenamento tornam-se visíveis como parte da definição de um perfil de armazenamento do Cloud Assembly. Consulte [Saiba mais sobre perfis de armazenamento no vRealize Automation](#).

Os discos de primeira classe cujos dados foram coletados aparecem na exibição **Recursos > Recursos > Volumes**.

Saiba mais sobre os recursos no Cloud Assembly

O Cloud Assembly pode expor informações adicionais sobre recursos coletados por dados, como cartões de preços.

Como a coleta de dados funciona no vRealize Automation

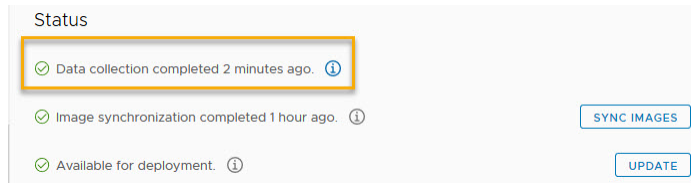
Após a coleta de dados inicial, a coleta de dados de recursos ocorre automaticamente a cada 10 minutos. O intervalo de coleta de dados não é configurável, e não é possível iniciá-la manualmente.

Você pode descobrir informações sobre coleta de dados de recursos e sincronização de imagens para uma conta de nuvem existente na seção Status de sua respectiva página. Para fazer isso, selecione **Infraestrutura > Conexões > Contas de Nuvem** e, em seguida, clique em **Abrir** na conta de nuvem existente de sua escolha.

É possível abrir uma conta de nuvem existente e ver sua versão de endpoint associada na seção **Status** dessa página. Se o endpoint associado tiver sido atualizado, sua nova versão será descoberta durante a coleta de dados e se refletirá na seção **Status** na página da conta de nuvem.

Coleta de dados de recursos

A coleta de dados ocorre a cada 10 minutos. Cada conta de nuvem exibe quando sua coleta de dados foi concluída pela última vez.

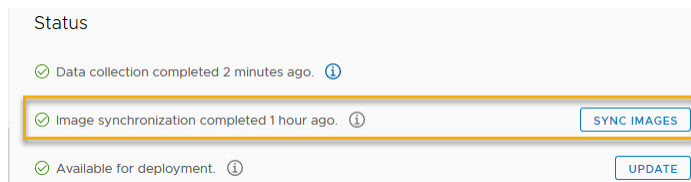


Coleta de dados de imagem

A sincronização de imagens ocorre a cada 24 horas. Você pode iniciar a sincronização de imagens para alguns tipos de conta de nuvem. Para iniciar a sincronização de imagens, abra a conta de nuvem (**Infraestrutura > Contas de Nuvem** e selecione e abra a conta de nuvem existente) e clique no botão **Sincronizar Imagens**. Não há opção de sincronização de imagem para contas de nuvem do NSX.

Observação As imagens são classificadas internamente como públicas ou privadas. Imagens públicas são compartilhadas e não são específicas para uma determinada organização ou assinatura de nuvem. Imagens privadas não são compartilhadas e são específicas para uma assinatura específica. Imagens públicas e privadas são sincronizadas automaticamente a cada 24 horas. Uma opção na página da conta de nuvem permite acionar a sincronização de imagens privadas.

A página da conta de nuvem é exibida quando a sincronização de imagem foi concluída pela última vez.



Para facilitar a tolerância a falhas e a alta disponibilidade em implantações, cada um dos endpoints de centro de dados do NSX-T representa um cluster de três gerenciadores do NSX. Para obter informações relacionadas, consulte [Criar uma conta de nuvem do NSX-T no vRealize Automation](#).

Contas de nuvem e planos de integração

Quando você cria uma conta de nuvem, os dados de todas as máquinas que estão associadas a ela são coletados e, em seguida, exibidos na página **Recursos > Recursos > Máquinas**. Se a conta de nuvem tiver máquinas que foram implantadas fora do Cloud Assembly, será possível usar um plano de integração para permitir que o Cloud Assembly gerencie as implantações de máquina.

Para obter informações sobre como adicionar contas de nuvem, consulte [Como adicionar contas de nuvem ao Cloud Assembly](#).

Para obter informações sobre como integrar máquinas não gerenciadas, consulte [O que são planos de integração no Cloud Assembly](#).

Atualizando recursos de rede no vRealize Automation após a migração de N-VDS para C-VDS no NSX-T

Após a migração do NSX-T do Switch Virtual Distribuído NSX (N-VDS) para o VDS Convergado (C-VDS), você deverá atualizar os recursos de rede afetados do vSphere no vRealize Automation para continuar usando esses recursos em implantações e modelos de nuvem novos e existentes.

Após a migração do N-VDS para o C-VDS, suas redes do vSphere podem parecer estar ausentes dos perfis de rede do vRealize Automation dos quais elas são membros. Para evitar a perda dessas redes do tipo vSphere e continuar a alocá-las em implantações novas e existentes, você deve atualizar manualmente todas as redes C-VDS listadas no vRealize Automation Cloud Assembly.

Observação Esse procedimento é específico para ações necessárias no vRealize Automation para atualizar redes do *vSphere* após a execução da migração do N-VDS para o C-VDS no NSX-T. Nenhuma ação é necessária no vRealize Automation em redes *NSX* após a migração do N-VDS para o C-VDS. Redes *NSX* não exigem intervenção manual após a migração do N-VDS para o C-VDS.

Se um administrador do NSX-T puder migrar tipos de rede NSX-T on VDS (N-VDS) para tipos de rede VDS Convergado (C-VDS) no NSX, essa ação afetará os recursos de rede existentes do vSphere no vRealize Automation. O administrador do vRealize Automation pode executar ações pós-migração para reconciliar esses recursos no vRealize Automation com as alterações associadas no NSX-T e no vCenter Server. Observe que o C-VDS, ou simplesmente VDS, também é chamado de Switch Virtual Distribuído (VDS) vSphere 7.

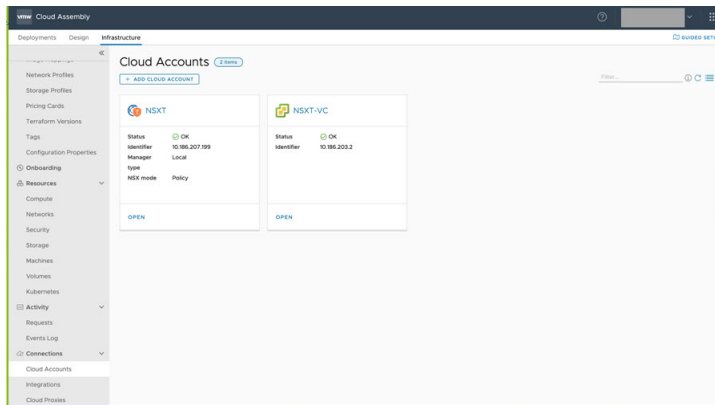
Para obter informações relacionadas sobre o VDS Convergado NSX-T, consulte os artigos da Base de Dados de Conhecimento da VMware [NSX-T on VDS \(79872\)](#) e [Migração do VMware Cloud on AWS \(VMConAWS\) e do VMware Cloud on Dell EMC do N-VDS para o VDS \(82487\)](#).

Observação Este cenário de amostra ilustra as etapas necessárias para reconciliar recursos em um ambiente do vRealize Automation após a migração do N-VDS para o C-VDS. Você pode usar esse exemplo e procedimento no vRealize Automation 8.5 e versões posteriores para reconciliar alterações feitas no vCenter Server após a migração do N-VDS para o C-VDS no NSX-T.

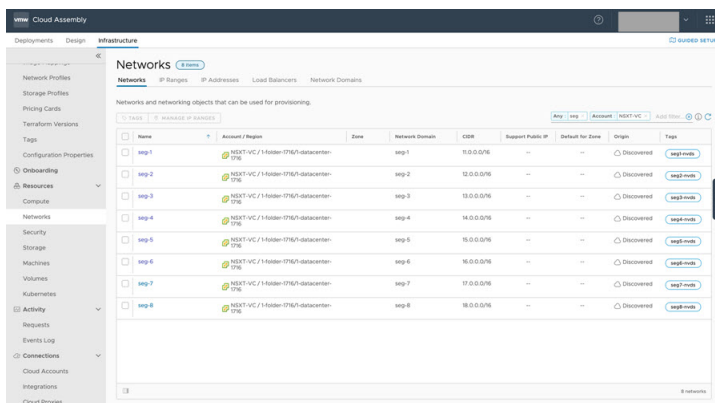
Exemplo: recursos do vRealize Automation pré-migração

Este exemplo ilustra recursos de amostra do NSX-T em um ambiente de amostra do vRealize Automation antes da migração do N-VDS para o C-VDS.

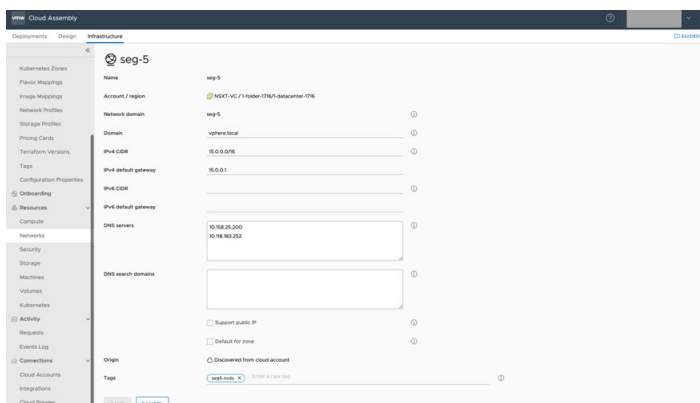
- Este exemplo contém contas de nuvem do NSX-T e do vCenter, conforme mostrado abaixo.



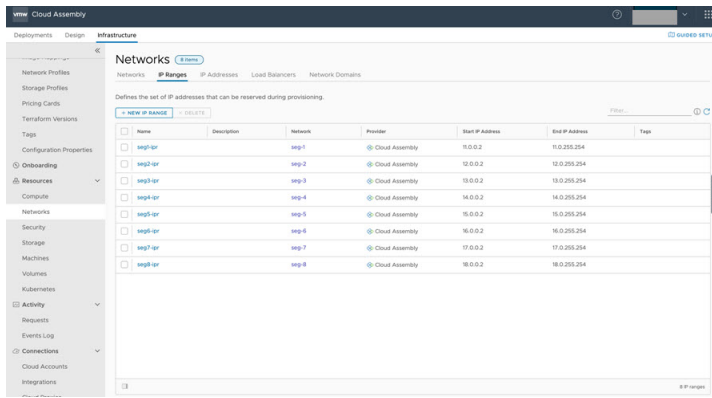
- O exemplo contém várias redes do vSphere, conforme mostrado abaixo.



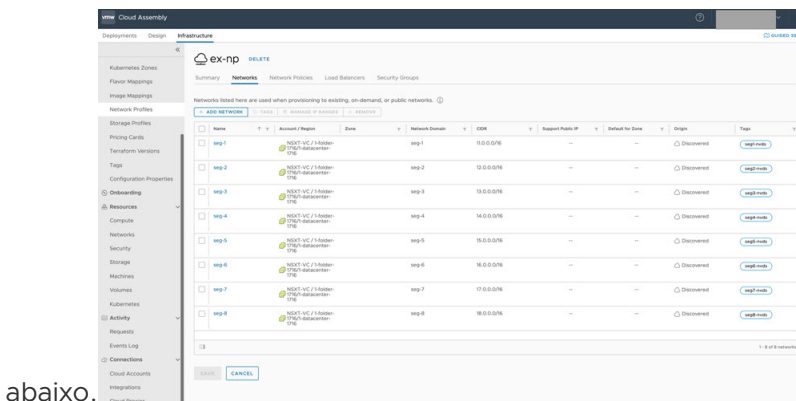
- O exemplo de configuração de rede contém configurações de CIDR e DNS, conforme mostrado abaixo.



- O exemplo também inclui intervalos de IPs existentes, conforme mostrado abaixo.

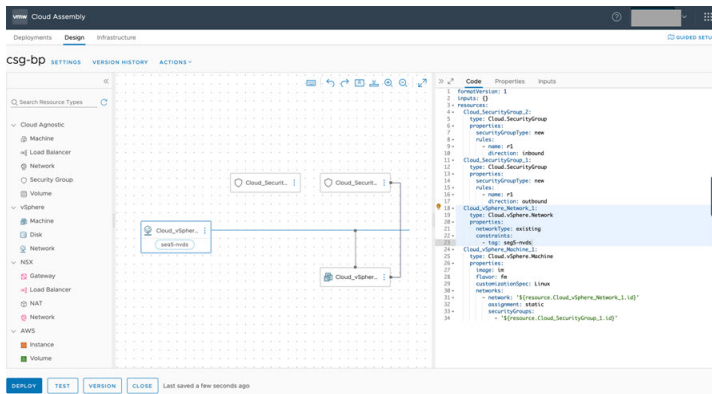


- O exemplo contém um perfil de rede (**ex-np**), que contém várias redes N-VDS (N-VDS), incluindo **seg-5**, conforme mostrado

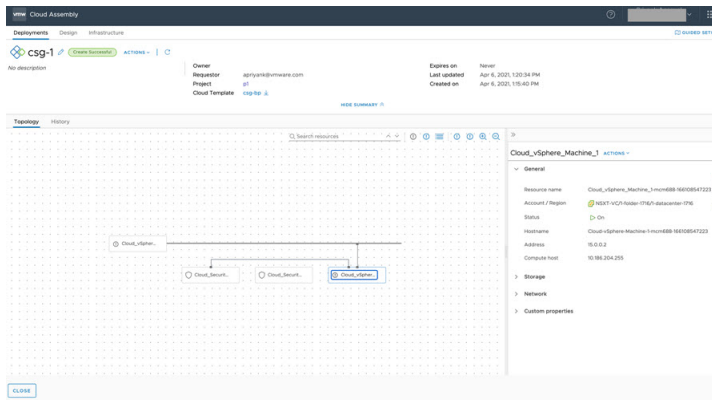


abaixo.

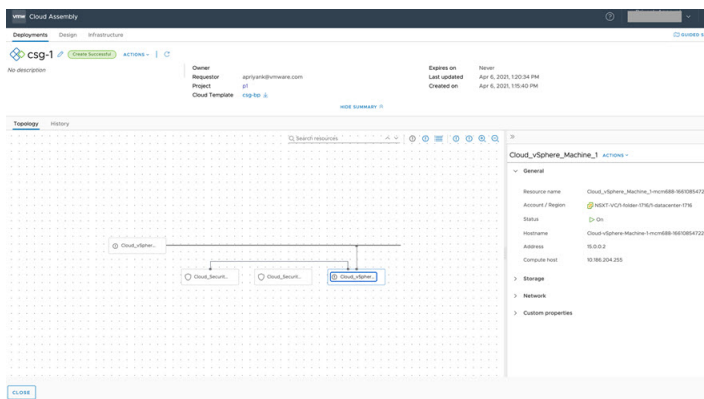
- Neste exemplo, o componente de rede **seg5** existente é mostrado na sintaxe de amostra do modelo de nuvem a seguir. A rede está marcada como uma rede N-VDS. Ilustraremos as atualizações pós-migração necessárias para a rede **seg5** mais adiante neste exemplo.



- O exemplo de modelo de nuvem gera a implantação, conforme mostrado abaixo.



- Os exemplos de endereços IP da máquina são exibidos na implantação de amostra, conforme mostrado abaixo.



Exemplo: Etapa 1 pós-migração – Executar coleta de dados após a migração e a enumeração do N-VDS para o C-VDS

Na seção acima, capturas de tela foram usadas para ilustrar a infraestrutura usada em um exemplo de ambiente do vRealize Automation, concluindo com o modelo de nuvem de saída e a implantação.

Quando você ou outro administrador executar a migração do N-VDS para o C-VDS no NSX-T, aguarde pelo menos 10 minutos para permitir que o vRealize Automation execute seu processo periódico de enumeração e coleta de dados para obter e exibir os recursos afetados no vRealize Automation.

Depois de permitir que a coleta de dados do vRealize Automation seja concluída, clique em **Infraestrutura > Redes** para visualizar e acessar as redes C-VDS disponíveis. Observe a rede **seg5**, conforme mostrado abaixo.

| Name | Account / Region | Zone | Network domain | CIDR | Support public IP | Default for zone | Origin | Tags |
|--------|--|------|------------------------------------|-------------|-------------------|------------------|------------|--------|
| seg-1 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-1 |
| seg-2 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 17.0.0.0/16 | -- | -- | Discovered | seg-2 |
| seg-3 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-3 |
| seg-4 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-4 |
| seg-5 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-5 |
| seg-6 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-6 |
| seg-7 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-7 |
| seg-8 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-8 |
| seg-9 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-9 |
| seg-10 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-10 |
| seg-11 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-11 |
| seg-12 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-12 |
| seg-13 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-13 |
| seg-14 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-14 |
| seg-15 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-15 |
| seg-16 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-16 |
| seg-17 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-17 |
| seg-18 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-18 |
| seg-19 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-19 |
| seg-20 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-20 |
| seg-21 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-21 |
| seg-22 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-22 |
| seg-23 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-23 |
| seg-24 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-24 |
| seg-25 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-25 |
| seg-26 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-26 |
| seg-27 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-27 |
| seg-28 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-28 |
| seg-29 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-29 |
| seg-30 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-30 |
| seg-31 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-31 |
| seg-32 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-32 |
| seg-33 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-33 |
| seg-34 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-34 |
| seg-35 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-35 |
| seg-36 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-36 |
| seg-37 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-37 |
| seg-38 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-38 |
| seg-39 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-39 |
| seg-40 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-40 |
| seg-41 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-41 |
| seg-42 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-42 |
| seg-43 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-43 |
| seg-44 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-44 |
| seg-45 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-45 |
| seg-46 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-46 |
| seg-47 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-47 |
| seg-48 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-48 |
| seg-49 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-49 |
| seg-50 | NEXT-VC / 1 folder-17864-datacenter-1786 | 4 | CVDS-nova-switch-1-datacenter-1786 | 10.0.0.0/16 | -- | -- | Discovered | seg-50 |

Exemplo: Etapa 2 pós-migração – Adicionar CIDR e DNS previamente definidos a redes C-VDS migradas

Edite uma rede C-VDS migrada para adicionar detalhes de CIDR e DNS que foram especificados na definição do N-VDS pré-migração e altere a marcação da rede.

- 1 Adicionar detalhes de CIDR e DNS que foram definidos em sua definição do N-VDS pré-migração
- 2 Adicione uma nova tag para a rede **seg-5** C-VDS de amostra como *seg5-cvds*.

Observe que a rede **seg-5** N-VDS original foi marcada como *seg5-nvds*, conforme visto nas telas anteriores. A alteração nos detalhes de marcação de recursos é necessária pela reconfiguração da rede. O vRealize Automation requer que você inclua no modelo de nuvem para a rede C-VDS um nome de tag diferente da tag usada na rede N-VDS original. A marcação alterada identifica uma alteração no modelo de nuvem ao gerar uma reimplantação válida.

Exemplo: Etapa 3 pós-migração – Adicionar informações atualizadas do intervalo de IPs

Você pode editar intervalos de IPs de rede para obter detalhes de intervalo de IPs que foram especificados na definição do N-VDS pré-migração, usando uma API de linha de comando ou uma sequência de menus no vRealize Automation.

- Opção 1: use a API para atualizar dados do intervalo de IPs, conforme exibido na tela de amostra a seguir.

PATCH : `{{host}}/iaas/api/network-ip-ranges/{{subnet-range-id}}`

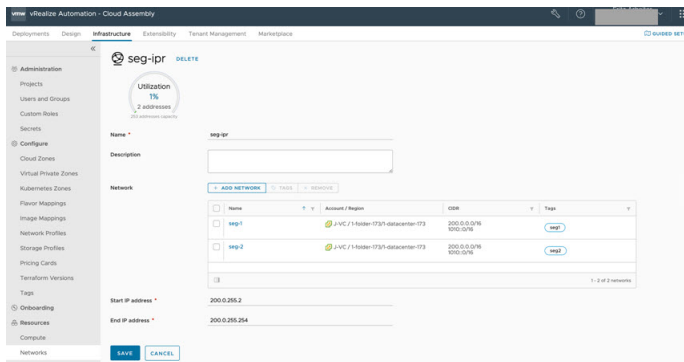
Headers :

- Authorization : Bearer `{{token}}`

Payload :

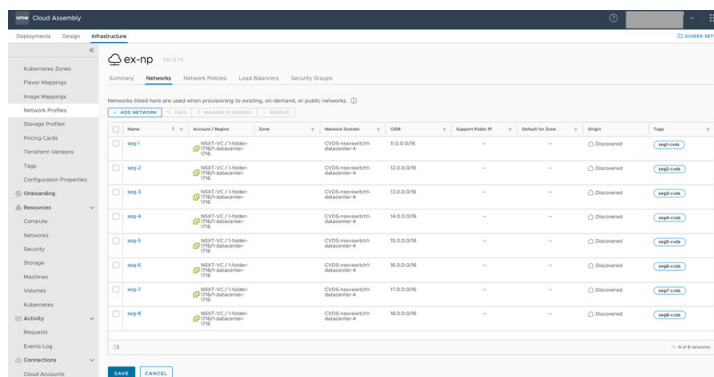
```
{
  "fabricNetworkIds": ["{{subnet-id}}"]
}
```

- Opção 2: use a interface do usuário para atualizar dados do intervalo de IPs, conforme exibido na tela de amostra a seguir.



Exemplo: Etapa 4 pós-migração – Atualizar perfis de rede para corrigir redes ausentes

Após a migração, as redes N-VDS são reconciliadas e excluídas do vRealize Automation Cloud Assembly após a enumeração e a coleta dos dados. Os perfis de rede afetados (como o exemplo **ex-np**) têm redes ausentes. Para corrigir o problema de redes ausentes, atualize cada rede N-VDS como uma rede C-VDS, conforme mostrado abaixo.

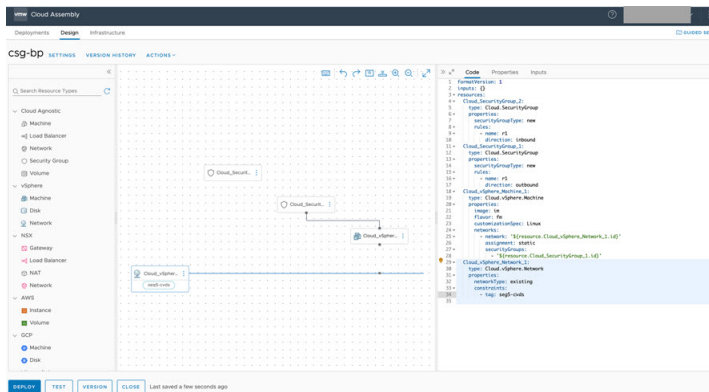


Exemplo: Etapa 5 pós-migração – Atualizar restrições de rede em modelos de nuvem

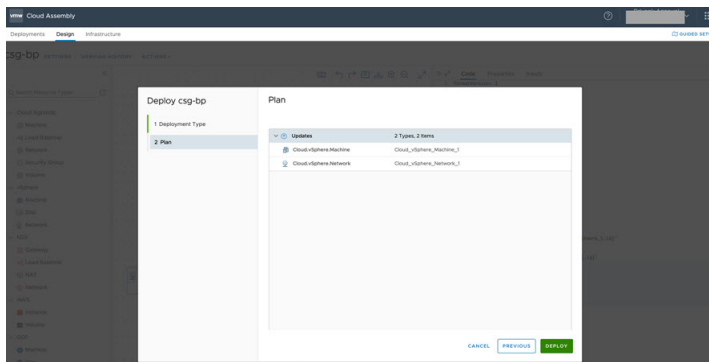
Para implantações existentes, você deve atualizar as restrições de rede no modelo de nuvem para corresponder às novas redes C-VDS nos perfis de rede atualizados. Restrições de rede atualizadas também são necessárias para realizar implantações iterativas e reconfigurar redes de sua representação original do vSphere N-VDS para a representação do vSphere C-VDS.

Para novas implantações, os recursos C-VDS especificados são usados e, portanto, essa etapa não é necessária. Implantações iterativas e a reconfiguração da rede simplesmente funcionam conforme projetado.

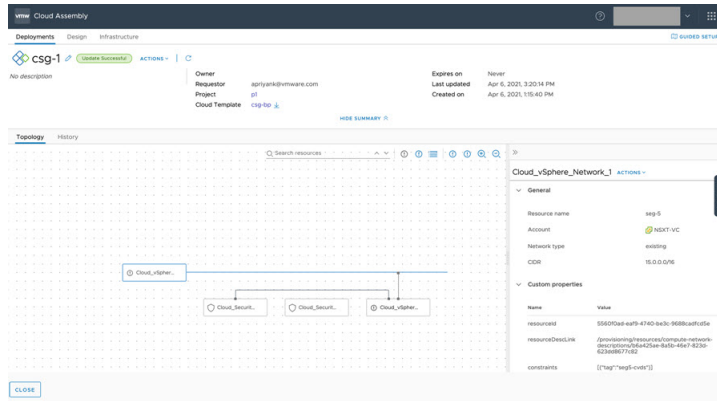
- 1 Para este exemplo, altere as restrições de rede no modelo de nuvem de *seg5-nvds* para *seg5-cvds*, como mostrado abaixo.



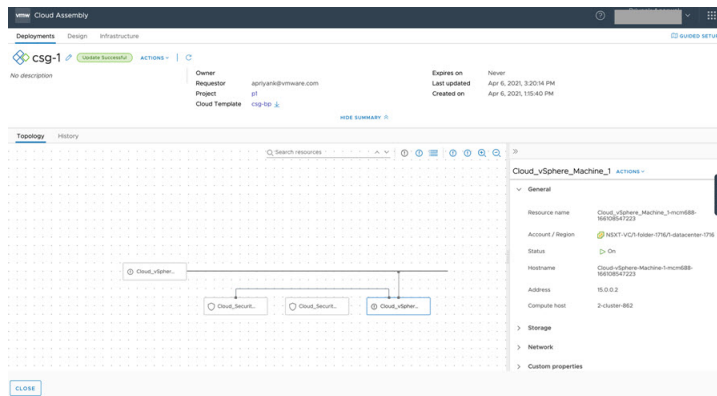
- 2 Realize uma implantação iterativa para reconfigurar a rede, conforme mostrado abaixo.



- 3 Após a reimplantação bem-sucedida, observe que as propriedades personalizadas de rede exibem as restrições atualizadas, conforme mostrado abaixo.



Como o intervalo de IPs foi atualizado anteriormente com os novos dados do C-VDS, o endereço IP da máquina não é alterado corretamente na reimplantação, conforme mostrado abaixo.



Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation

Um administrador de nuvem pode monitorar e gerenciar recursos de infraestrutura e otimizações de implantação em cada zona de nuvem. Ao visualizar insights em tempo real e revisar as ações sugeridas para os recursos compatíveis, você pode ajudar proativamente os proprietários de projetos a gerenciar sua capacidade de recursos e otimizar suas implantações.

Você pode usar o dashboard **Insights** para explorar dados de métrica para os recursos e implantações em zonas de nuvem nos projetos que você gerencia. Use essas informações, fornecidas por uma combinação do vRealize Automation e do seu aplicativo vRealize Operations Manager integrado, para fazer quaisquer ajustes necessários na memória, em CPUs e assim por diante ou compartilhe essas informações com a sua equipe para que ela possa ter um embasamento melhor e fazer quaisquer ajustes necessários.

O dashboard Insights permite que você entre em contato com alguns ou todos os proprietários do projeto que têm implantações na zona da nuvem que contêm capacidade de recursos recuperável. Os insights da zona de nuvem exibem capacidade recuperável para projetos e implantações.

Os proprietários de projetos contatados visualizam a notificação na página **Alertas** de suas implantações. A notificação contém seu nome e o nome de (e link para) cada implantação que pode ser otimizada.

O dashboard **Insights** está disponível para zonas de nuvem do vSphere e do VMware Cloud on AWS, desde que as contas de nuvem estejam configuradas tanto no vRealize Automation quanto no vRealize Operations Manager e estejam sendo monitoradas no vRealize Operations Manager.

Pré-requisitos

- Reveja [Gerenciamento de recursos e otimização de implantação usando métricas do vRealize Operations Manager no vRealize Automation](#).
- Verifique se você tem credenciais de administrador de nuvem do vRealize Automation e acesso HTTPS ativado na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem do vRealize Automation. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Configure a integração do vRealize Automation com o vRealize Operations Manager.
- Configure o adaptador do vRealize Automation no vRealize Operations Manager.

Sobre o vRealize Operations Manager e as métricas de capacidade de recurso coletadas

O vRealize Operations Manager coleta métricas de capacidade para os mesmos recursos de infraestrutura utilizados por você e as equipes às quais você oferece suporte no vRealize Automation. Ao integrar o vRealize Automation com o vRealize Operations Manager, os dados de métricas do vRealize Operations Manager são disponibilizados e exibidos para cada projeto gerenciado em um painel **Insights** em cada zona de nuvem.

Os dados do projeto são analisados no painel do vRealize Automation a partir do aplicativo vRealize Operations Manager integrado. O painel Insights exibe as seguintes informações:

- Porcentagem de utilização da CPU relativa à capacidade
- Porcentagem de utilização da memória relativa à capacidade
- Porcentagem de utilização do armazenamento em relação à capacidade
- Histórico de demanda de CPU e memória calculada e demanda projetada
- Opção para entrar em contato com os proprietários de algumas ou todas as implantações em uma zona de nuvem que podem ser otimizadas pela recuperação de recursos, por exemplo, redimensionando ou excluindo máquinas. Os dados de otimização são calculados na ordem de dias.

O painel Insights está disponível para recursos do vSphere.

Um widget de tendências exibe os componentes de processamento de uma zona de nuvem (como clusters e hosts), o uso de GHz da CPU em relação à capacidade da CPU e o uso de GB de memória em relação à capacidade de memória.

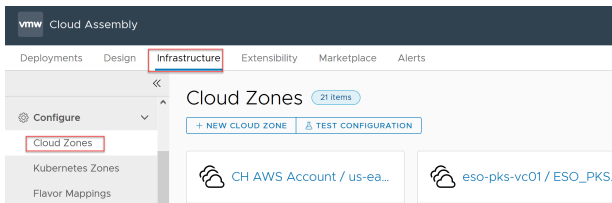
As informações sobre as funções necessárias para usar alertas estão disponíveis em [Personalizar funções de usuário no vRealize Automation](#).

Para obter informações relacionadas, consulte [Gerenciamento de recursos e otimização de implantação usando métricas do vRealize Operations Manager no vRealize Automation](#).

Procedimento

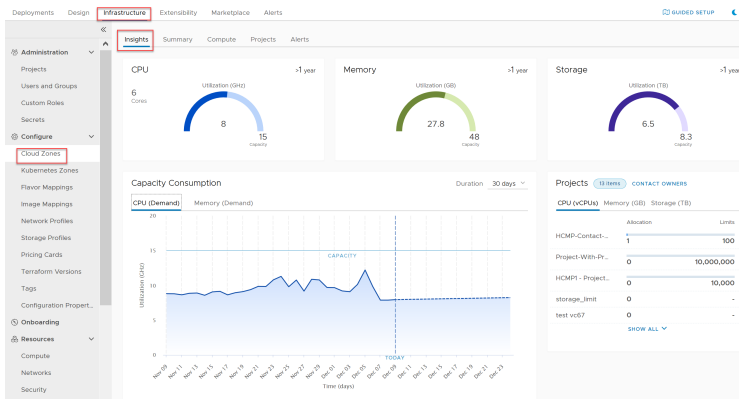
Abra uma zona de nuvem para descobrir suas métricas de capacidade e, opcionalmente, obter informações sobre as implantações de projeto que podem ser otimizadas. Os dados são coletados e fornecidos pelo aplicativo vRealize Operations Manager associado.

- 1 Em Cloud Assembly, clique em **Infraestrutura > Configurar > Zonas de Nuvem** e selecione uma zona de nuvem.

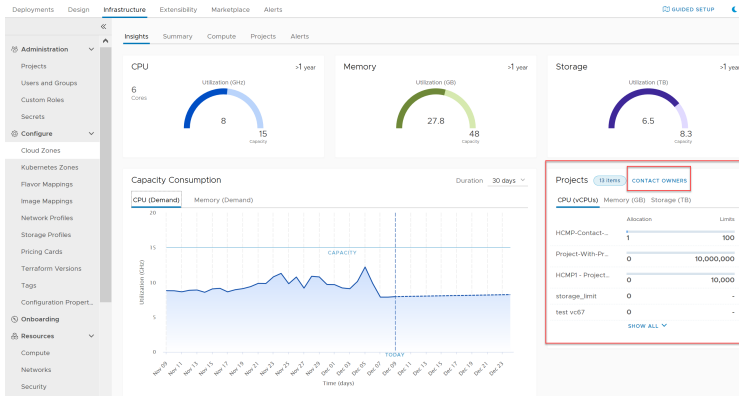


- 2 Clique na guia **Insights** e examine o painel Insights.

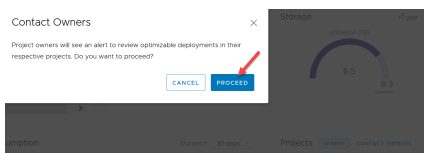
O exemplo a seguir exibe informações sobre CPU, memória e capacidade de armazenamento para os recursos usados por projetos na zona de nuvem.



- 3 Para notificar o proprietário do projeto sobre todas as implantações que podem ser otimizadas, clique em **Entrar em Contato com o Proprietário** na seção **Projetos**. As notificações aparecem na página da guia **Alertas**.

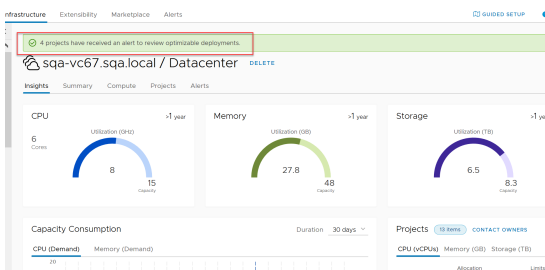


- 4 Para obter as informações de otimização sobre cada implantação do projeto, clique em **Continuar**.

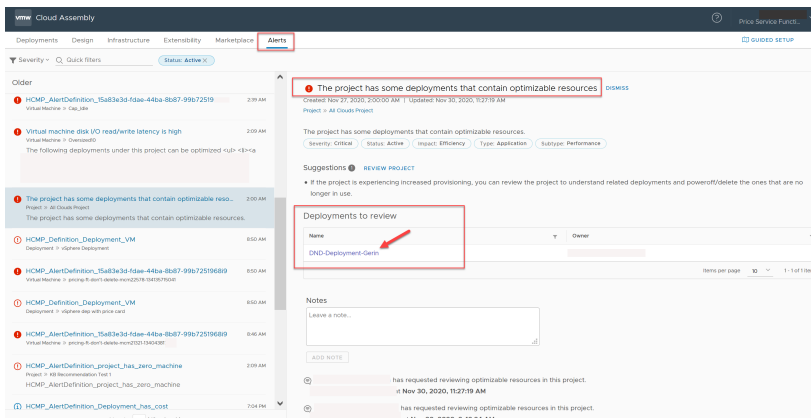


Se o projeto contiver implantações que podem ser otimizadas, essas informações serão transmitidas ao proprietário do projeto na guia **Alertas** do Cloud Assembly.

- 5 Uma mensagem aparece indicando o número de implantações que podem ser otimizadas.



As informações de notificação sobre esses recursos e implantações estão disponíveis para o proprietário do projeto na guia Cloud Assembly **Alertas**. Neste exemplo, essas informações de notificação incluem o nome de, e um link para, cada implantação que pode ser otimizada, como mostrado no exemplo a seguir:



Próximas etapas

Use as informações obtidas no painel **Insights** para fazer quaisquer ajustes necessários nos recursos que você gerencia. Abra a página **Alertas** para obter informações adicionais, ações sugeridas e links para implantações que podem ser otimizadas. Consulte [Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation](#).

Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation

Como administrador da nuvem, você precisa saber quando a capacidade, o desempenho e a disponibilidade do vRealize Automation estão se tornando problemáticos para poder reagir de forma proativa antes que os usuários comecem a ficar sem recursos.

Você pode exibir uma variedade de alertas fornecidos pelo aplicativo vRealize Operations Manager associado. Alertas estão disponíveis para objetos de recursos do vSphere e do VMware Cloud on AWS. Use as informações em alertas para modificar os recursos e implantações que você gerencia ou compartilhe essas informações com sua equipe para que eles possam modificar os objetos que estão gerenciando.

Observação Para examinar e agir em implantações de projeto que você deve considerar otimizar, consulte [Como usar Alertas para otimizar implantações no vRealize Automation](#).

No momento, alertas estão disponíveis apenas para objetos de recursos do vSphere e do VMware Cloud on AWS. A guia **Alertas** só estará disponível se o acesso a vRealize Operations Manager estiver configurado.

Os valores de limite de alertas do vRealize Automation são definidos no vRealize Operations Manager. Alguns alertas do vRealize Automation estão atualmente predefinidos. Notificações de alertas também são definidas no vRealize Operations Manager. Para obter informações sobre como configurar definições de alerta e notificações, consulte a [documentação do produto](#) vRealize Operations Manager.

Pré-requisitos

- Reveja [Gerenciamento de recursos e otimização de implantação usando métricas do vRealize Operations Manager no vRealize Automation](#).
- Verifique se você tem credenciais de administrador de nuvem do vRealize Automation e acesso HTTPS ativado na porta 443. Consulte [Credenciais necessárias para trabalhar com contas de nuvem no vRealize Automation](#).
- Verifique se tem a função de usuário de administrador de nuvem do vRealize Automation. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Configure a integração do vRealize Automation com o vRealize Operations Manager.
- Configure o adaptador do vRealize Automation no vRealize Operations Manager.
- Configure as funções necessárias para gerenciar alertas. Consulte [Personalizar funções de usuário no vRealize Automation](#).

As capacidades da função incluem:

- Os administradores de nuvem podem gerenciar alertas de zona de nuvem.
- Os administradores de projeto podem gerenciar alertas de projeto.
- Os administradores do Service Broker podem gerenciar alertas de implantação.

Sobre o vRealize Operations Manager e alertas de recursos

O vRealize Operations Manager coleta métricas de integridade e uso, entre outras, para os mesmos recursos de infraestrutura e as implantações que você gerencia no vRealize Automation. Ao integrar o vRealize Automation com o vRealize Operations Manager, esses dados monitorados são disponibilizados para você no vRealize Automation por meio da guia **Alertas** no menu principal do Cloud Assembly.

Os dados de alertas fornecidos pelo vRealize Operations Manager incluem preocupações relacionadas a limites de riscos e integridade para modelos de nuvem, implantações, organizações e projetos. Ele também contém informações sobre implantações que podem ser otimizadas, com base no proprietário que está sendo contatado por uma ação realizada na guia **Insights** da zona de nuvem. Consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#).

Os detalhes do alerta de cada implantação incluem:

- Nome do projeto
- Nome da implantação (e link para a implantação) que contém recursos que podem ser otimizados
- Ações sugeridas
- Possíveis economias de custos com a recuperação e a otimização
- Número total de CPUs virtuais usadas pela implantação
- Quantidade total de memória RAM usada pela implantação
- Quantidade total de armazenamento usado pela implantação
- Máquinas virtuais na implantação recomendadas para recuperação e otimização, incluindo nome de recurso, máquinas ociosas, máquinas desligadas, máquinas dimensionadas em excesso e em falta, máquinas subutilizadas e snapshots de máquinas

Usando a opção **Entrar em contato com os proprietários do projeto** no dashboard Insights da zona da nuvem, você pode ver um resumo de todos os projetos que têm capacidade recuperável (CPU, memória e armazenamento) na zona da nuvem e fornecer um alerta para alguns ou todos os proprietários do projeto.

Contact Project Owners

Contact project owners to suggest resources that can potentially be reclaimed. Which project owners do you want to contact?

Search projects | Sort: Optimizable deployments (descending) ▼

| Projects | Optimizable Deployments | Allocation (Reclaimable) v/s Limit (CPU (vCPUs), Memory (GB), Storage (TB)) |
|---|-------------------------|---|
| <input checked="" type="checkbox"/> Ansible-Project | 6 | 1(0) - 1(0) - 0.008(0.008) |
| <input checked="" type="checkbox"/> vc05 project | 2 | 12(4) - 20 6(2) - 9.8 0.02(0.009) - 0.977 |

1 - 2 of 2 projects

[CANCEL](#) [CONTACT PROJECT OWNERS](#)

Procedimento

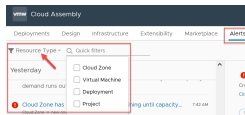
Você pode exibir informações de limites de alertas sobre os recursos que gerencia usando as opções de filtragem na página **Alertas**. Dados de alertas são fornecidos pelo seu aplicativo vRealize Operations Manager associado. Ações sugeridas são fornecidas para cada alerta.

Você também pode selecionar uma implantação na seção **Implantações a serem revisadas** para abrir e otimizar essa implantação. Consulte [Como usar Alertas para otimizar implantações no vRealize Automation](#).

- 1 No serviço Cloud Assembly, clique na guia **Alertas** no menu principal.



- 2 Para controlar como os alertas são exibidos, experimente os filtros disponíveis. Por exemplo, selecione a opção **Recursos** no menu suspenso de filtros.



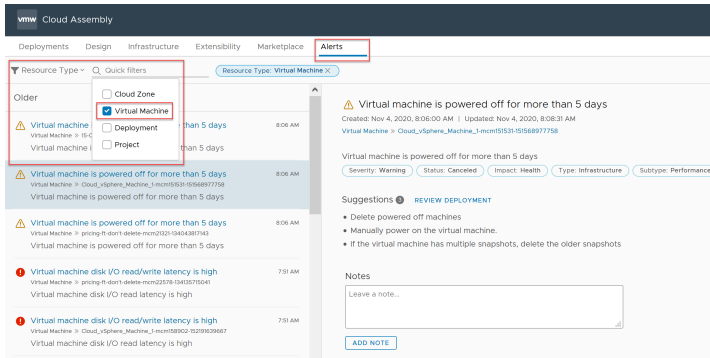
- 3 Para exibir alertas e ações sugeridas para esses alertas, use opções de filtro rápido no painel seletor.

- Exiba alertas sobre recursos de zonas de nuvem.

The screenshot shows the 'Alerts' page in vRealize Cloud Assembly. On the left, a list of alerts is displayed, including 'Cloud Zone has less than 60 days remaining until capacity runs out'. The main panel shows the details of this alert, including the message 'Cloud Zone has less than 60 days remaining until capacity runs out', the time remaining, and suggestions for action. The suggestions include removing capability tags, selecting an appropriate placement policy, adding more CPU and memory capacity, and analyzing associated projects.

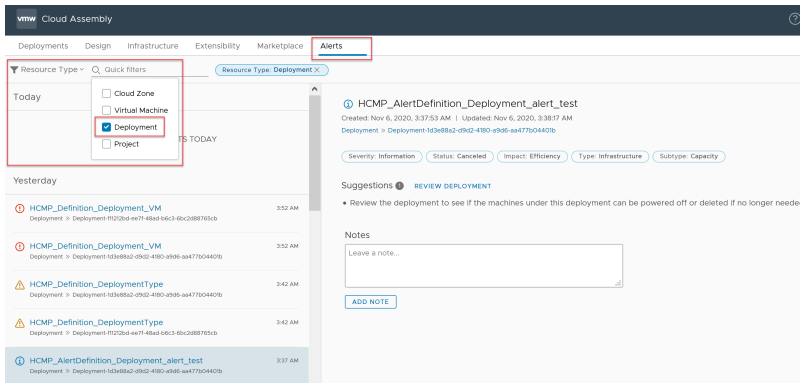
O vRealize Operations Manager pode monitorar o tempo restante, a capacidade restante, a capacidade recuperável etc.

- Exiba alertas sobre recursos de máquina virtual.



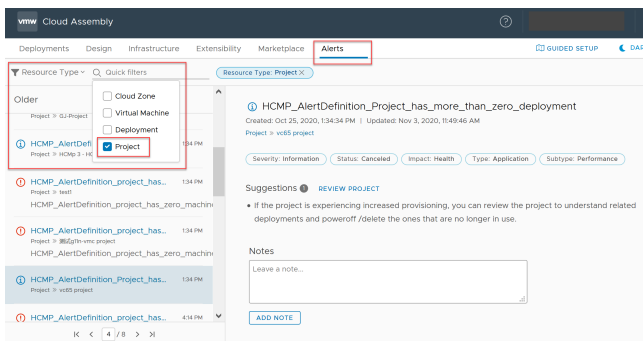
A maioria dos alertas de máquina virtual diz respeito ao status ativado/desativado, à latência e assim por diante.

- Exiba alertas sobre recursos de implantação.



Os alertas de implantação dizem respeito referem a recursos recuperáveis e ao dimensionamento apropriado.

- Exiba alertas sobre recursos de projeto.



Os alertas de projeto estão relacionados a recursos recuperáveis e limites de alocação.

- 4 Explore outros tipos de filtro e suas opções de filtragem rápida para controlar ainda mais a lista de alertas.

- Use os filtros rápidos de **Impactos** de integridade, risco e eficiência.
- Use os filtros rápidos de **Gravidade** de crítico, imediato, aviso e informações.

- Use os filtros rápidos de **Status** de ativo, cancelado e ignorado.
- Use os filtros de **Subtipo** com os valores Disponibilidade, Desempenho e Capacidade.
- Use os filtros rápidos de **Tipo** com de aplicativo, hardware, infraestrutura, armazenamento e rede.

5 Tome as ações necessárias com base em dados de alertas e sugestões.

Próximas etapas

Para saber mais sobre outras ações disponíveis, consulte [Como usar Alertas para otimizar implantações no vRealize Automation](#).

Você também pode exibir **Insights** de capacidade para recursos com base na zona de nuvem nos projetos que você gerencia. Para obter informações sobre como usar dados de **Insights** fornecidos pelo vRealize Operations Manager no vRealize Automation, consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#).

Como usar Alertas para otimizar implantações no vRealize Automation

Como administrador de nuvem ou proprietário de projeto, você pode monitorar e gerenciar os recursos da máquina para a melhor otimização possível usando dados obtidos do vRealize Operations Manager e exibidos no vRealize Automation.

Quando você conecta vRealize Automation ao vRealize Operations Manager, pode acessar informações coletadas de dados sobre recursos nos projetos que você gerencia. Os dados de alertas e insights são fornecidos para informá-lo de várias preocupações sobre os projetos que você gerencia e fornecem um meio fácil de comunicar sugestões de otimização e dados de suporte coletados de vRealize Operations Manager para os proprietários do projeto de forma fácil e eficiente, sem nunca deixar o aplicativo vRealize Automation. Por exemplo, você pode ver a capacidade de recursos recuperáveis, com economias de custo específicas, para cada implantação em uma zona de nuvem. Onde uma zona de nuvem contém várias implantações que podem ser otimizadas, você pode notificar alguns ou todos os proprietários do projeto e da implantação.

Os alertas de otimização de implantação podem ser gerados a partir do painel Insights. Consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#). Você pode entrar em contato com os proprietários do projeto para que eles possam abrir uma implantação nomeada para ser otimizada a partir de um link fornecido na página **Alertas**. Além disso, os proprietários de projetos podem

abrir suas implantações diretamente e usar a guia **Otimizar** para executar tarefas de otimização disponíveis. As ações que um proprietário do projeto pode realizar incluem a recuperação de recursos excluindo implantações não críticas e interrompendo o provisionamento adicional dentro de uma zona de nuvem.

Observação Para saber mais sobre outras ações de correção de recursos que você pode realizar, consulte [Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation](#).

Pré-requisitos

Consulte [Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation](#) para obter as credenciais e as informações de configuração necessárias para acessar os dados do vRealize Operations Manager no vRealize Automation.

Para solicitar que os proprietários de projetos sejam alertados sobre implantações que são otimizadas, consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#).

Sobre

Cada implantação contém uma guia **Otimizar**. Os seguintes parâmetros de otimização estão disponíveis:

- Máquinas que podem ser redimensionadas: exibe informações e ações para máquinas superdimensionadas e subdimensionadas na implantação, junto com a economia de custos de otimização.
- Máquinas subutilizadas: exibe informações e ações para máquinas inativas ou desligadas na implantação, junto com economia de custos de otimização.
- Snapshots de máquina: exibe informações e ações para snapshots de máquina se as máquinas na implantação contêm snapshots, juntamente com a economia de custos de otimização.

Como administrador, você pode notificar os proprietários do projeto de que eles têm implantações para otimizar. As notificações aparecem na guia **Alertas** no Cloud Assembly.

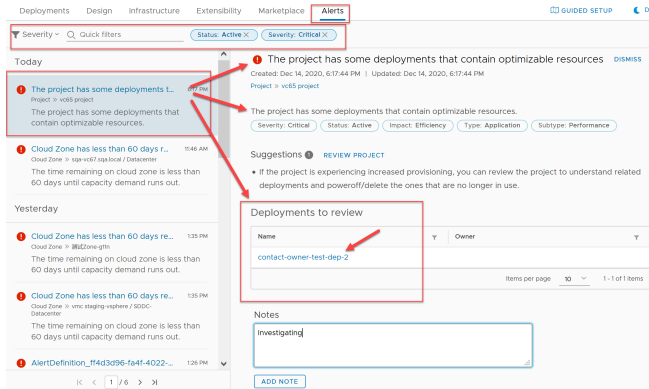
A guia **Alertas** só estará disponível se o acesso a vRealize Operations Manager estiver configurado. Os proprietários de projetos podem abrir e otimizar suas implantações para responder aos alertas.

Procedimento

Você pode exibir informações de limites de alertas sobre os recursos que gerencia usando as opções de filtragem na página **Alertas**. Dados de alertas são fornecidos pelo seu aplicativo vRealize Operations Manager associado. Ações sugeridas são fornecidas para cada alerta. Neste exemplo, o proprietário do projeto abre a implantação a partir de um link fornecido em uma notificação de alerta. A guia **Otimizar** da implantação exibe os parâmetros de máquina disponíveis para otimização.

- 1 Como proprietário ou administrador do projeto, clique na guia **Alertas** no menu principal.

- Encontre um alerta que contenha informações sobre uma implantação que pode ser otimizada e clique no nome da implantação em **Implantações a serem revisadas** para abrir essa implantação e exibir sua guia **Otimizar**.



- Quando a implantação for aberta, clique na guia **Otimizar**.



- Se houver máquinas subutilizadas, examine e aja em máquinas ociosas e desligadas. É possível desligar ou excluir uma implantação dimensionada em falta.
- Se houver máquinas que podem ser dimensionadas corretamente, examine e aja em quaisquer máquinas dimensionada em excesso e em falta na implantação.
- Se uma ou mais máquinas na implantação contiver um snapshot, você poderá excluir ou exportar cada snapshot.
- Quando terminar, confirme se a implantação foi otimizada para sua satisfação e feche-a

Próximas etapas

Para saber mais sobre outras ações disponíveis, consulte [Como usar alertas para gerenciar a capacidade, o desempenho e a disponibilidade de recursos no vRealize Automation](#).

Você também pode exibir **Insights** de capacidade para recursos com base na zona de nuvem nos projetos que você gerencia. Para obter informações sobre como usar dados de **Insights** fornecidos pelo vRealize Operations Manager no vRealize Automation, consulte [Como usar o dashboard Insights para monitorar a capacidade dos recursos e notificar os proprietários do projeto no vRealize Automation](#).

O que posso fazer com o armazenamento em disco padrão no vRealize Automation

Os discos padrão podem ser persistentes ou não persistentes.

O vRealize Automation é compatível com duas categorias de armazenamento: disco padrão e disco de primeira classe. O primeiro disco de classe só está disponível para vSphere.

■ vSphere

O vSphere oferece suporte a discos padrão dependentes (padrão), persistentes e independentes, e não persistentes e independentes. Para obter informações relacionadas, consulte [O que posso fazer com o armazenamento em disco persistente no vRealize Automation](#).

Quando você exclui uma máquina virtual, seus discos não persistentes dependentes e independentes também são excluídos.

Quando você exclui uma máquina virtual, seus discos permanentes independentes não são excluídos.

Você pode criar um snapshot de discos não persistentes dependentes e independentes. Não é possível criar um snapshot de um disco permanente independente.

■ Amazon Web Services (AWS) EBS

Você pode anexar um volume EBS a uma instância de processamento do AWS ou desanexar um volume EBS de uma instância de processamento do AWS.

Quando você exclui uma máquina virtual, seu volume EBS anexado é desanexado, mas não é excluído.

■ Microsoft Azure VHD

Os discos anexados são sempre persistentes.

Ao excluir uma máquina virtual, você especifica se deseja remover seus discos de armazenamento anexados.

■ Google Cloud Platform (GCP)

Os discos anexados são sempre persistentes.

Os discos persistentes são localizados de forma independente das instâncias da máquina virtual, para que você possa desanexar ou mover discos persistentes para manter os dados mesmo depois de excluir as instâncias.

Quando você exclui uma máquina virtual, seu disco anexado é desanexado, mas não é excluído.

Para obter informações relacionadas, consulte [Saiba mais sobre perfis de armazenamento no vRealize Automation](#).

O que posso fazer com o armazenamento em disco persistente no vRealize Automation

Os discos persistentes preservam dados valiosos de uma exclusão acidental.

Em um modelo de nuvem, em um volume, você pode adicionar a propriedade `persistent: true` para que o disco fique imune a exclusões pelo Cloud Assembly ou Service Broker. Discos persistentes não são removidos durante a exclusão da implantação ou em operações de Dia 2 para excluir ou remover discos.

Por isso, esses discos persistentes podem permanecer na sua infraestrutura mesmo após uma exclusão de implantação ou exclusão de disco. Para removê-los, você pode usar as técnicas a seguir.

- Passe transmitir explicitamente o sinalizador de limpeza como um parâmetro de consulta usando a API DELETE.
- Exclua-os diretamente do seu endpoint de nuvem.

Observe que não há uma interface de usuário do Cloud Assembly ou Service Broker para removê-los.

O que posso fazer com o armazenamento em disco de primeira classe no vRealize Automation

Um disco de primeira classe (FCD) oferece gerenciamento de ciclo de vida de armazenamento em discos virtuais como um disco como serviço ou como armazenamento em disco semelhante ao EBS, que permite criar e gerenciar discos independentemente das máquinas virtuais do vSphere.

O vRealize Automation é compatível com duas categorias de discos de armazenamento: disco padrão e disco de primeira classe. A funcionalidade do disco de primeira classe tem suporte apenas para vSphere. O vRealize Automation atualmente fornece funcionalidade de disco de primeira classe como um recurso somente de API.

Um disco de primeira classe tem seus próprios recursos de gerenciamento de ciclo de vida, que operam de forma independente de uma VM. Uma das diferenças entre um disco de primeira classe e um disco persistente independente é que você pode usar um disco de primeira classe para criar e gerenciar snapshots independentes de uma VM.

Você pode criar um novo perfil de armazenamento no vRealize Automation para oferecer suporte a recursos de disco de primeira classe ou recursos de disco padrão. Consulte [Saiba mais sobre perfis de armazenamento no vRealize Automation](#) e [Recursos de armazenamento no vRealize Automation](#).

Você também pode adicionar um elemento de disco de primeira classe `Cloud.vSphere.Disk` em seus modelos de nuvem e implantações do vRealize Automation para oferecer suporte a discos de primeira classe do vSphere. Os discos de primeira classe cujos dados foram coletados aparecem na página **Recursos > Recursos > Volumes**.

Em vCenter, os discos de primeira classe também são referidos como *Discos virtuais aprimorados (IVD)* ou *Discos virtuais gerenciados*.

Recursos

Usando os recursos de API do vRealize Automation, você pode:

- Criar, listar e excluir um disco de primeira classe.

- Redimensionar um primeiro disco de classe.
- Anexar e desanexar um disco de primeira classe.
- Criar e gerencia snapshots do disco de primeira classe.
- Converter um disco padrão existente para o disco de primeira classe

Os seguintes cenários não têm suporte:

- Provisionamento de VMs de snapshots em um cluster de armazenamento de dados.
- Gerar e compartilhar blocos de armazenamento baseados em dispositivo por usuários e tenants.
- Criar e restaurar snapshots da VM.
- Anexar o armazenamento em várias VMs e clusters.

Informações de API relacionadas para criar e gerenciar o armazenamento do disco de primeira classe (FCD) usando a API do vRealize Automation, inclusive para definir um perfil de armazenamento para usar os recursos do disco de primeira classe, estão disponíveis em code.vmware.com em [Quais são as APIs do vRealize Automation Cloud e como utilizá-las](#) ou navegando aos seguintes locais:

- A documentação da API para o FCD está disponível na seção [Disco de primeira classe \(FCD\)](#) do [Guia de programação do kit de desenvolvimento do disco virtual](#).
- Links para a documentação do caso de uso da API para FCD no vRealize Automation estão disponíveis na [página de documentação da API do vRealize Automation](#) da sua versão do vRealize Automation.

Considerações e limitações

Atualmente, as considerações e as limitações do disco de primeira classe incluem:

- O discos de primeira classe está disponíveis apenas para VMs vSphere.
- O vSphere 6.7, atualização 2 ou posterior, é necessário para usar os primeiros discos de classe.
- Não há suporte para o provisionamento de discos de primeira classe em clusters de repositório de dados.
- O volume de múltiplos anexos não é compatível com discos de primeira classe.
- Discos de primeira classe com snapshots não podem ser redimensionados.
- Discos de primeira classe com snapshots não podem ser excluídos.
- A hierarquia de snapshots do disco da primeira classe só pode ser construída usando a opção de API `createdAt`.
- A versão mínima de hardware da VM necessária para anexar um disco de primeira classe é vmx-13 (compatível com ESX 6.5).

Configurando recursos de tenant de vários provedores com o vRealize Automation

Em ambientes de multilocação, os clientes podem gerenciar a alocação de recursos por tenant usando Zonas Privadas Virtuais (VPZs).

No vRealize Automation 8.x, os clientes podem configurar ambientes de multilocação usando o VMware Lifecycle Manager e o Workspace ONE Access. Essas ferramentas permitem que os usuários configurem a multilocação e criem e configurem tenants. Depois que os tenants são configurados, os administradores do provedor podem criar Zonas privadas virtuais no Cloud Assembly e então podem atribuir Zonas a tenants usando a funcionalidade Gerenciar tenants do Cloud Assembly.

A multilocação depende da coordenação e configuração de três produtos da VMware diferentes, conforme descrito abaixo:

- **Workspace ONE Access** - Este produto fornece o suporte de infraestrutura para multilocação e as conexões de domínios do Active Directory que fornecem gerenciamento de usuários e grupos em organizações de tenants.
- **vRealize Suite Lifecycle Manager** - Este produto oferece suporte à criação e à configuração de tenants para produtos com suporte, como o vRealize Automation. Além disso, ele fornece alguns recursos de gerenciamento de certificados.
- **vRealize Automation** - Provedores e usuários fazem login no vRealize Automation para acessar tenants nos quais eles criam e gerenciam implantações.

Ao configurar a multilocação, os usuários devem estar familiarizados com todos esses três produtos e com a documentação associada.

Para obter mais informações sobre como trabalhar com o vRealize Suite Lifecycle Manager e o Workspace ONE Access, consulte o seguinte.

Como criar uma zona privada virtual para o vRealize Automation

Os administradores do provedor podem criar uma zona privada virtual (VPZ) para alocar recursos de infraestrutura para tenants em um ambiente de vRealize Automation de várias organizações. Os administradores também podem usar o VPZ para controlar a alocação de recursos em implantações de tenant único.

Você pode usar as Zonas Privadas Virtuais para alocar recursos, como imagens, redes e recursos de armazenamento. As VPZs funcionam bem como zona de nuvem em uma base por tenant, mas são projetados especificamente para uso com implantações de vários tenants. Para um projeto específico, você pode usar zonas de nuvem ou VPZs, mas não ambos. Além disso, existe uma relação de um para um entre os tenants e VPZs. Ou seja, um VPZ pode ser atribuído a apenas um tenant de cada vez.

Observação Configure os mapeamentos de tipo e imagem para uma VPZ na página Gerenciamento de Tenants.

Você pode criar um VPZ com ou sem o NSX. Se você criar uma zona sem o NSX, haverá limites relacionados à funcionalidade do NSX nos endpoints do vSphere.

- Segurança (grupos, firewall)
- Componentes de rede (NAT)

Pré-requisitos

- Habilite e configure vários tenants na sua implantação do vRealize Automation usando o VMware Life Cycle Manager e o VMware Workspace ONE Access.
- Crie administradores de tenant conforme apropriado para a configuração do tenant.
- Se você quiser usar o NSX, deverá criar uma conta de nuvem do NSX apropriada na organização do seu provedor.

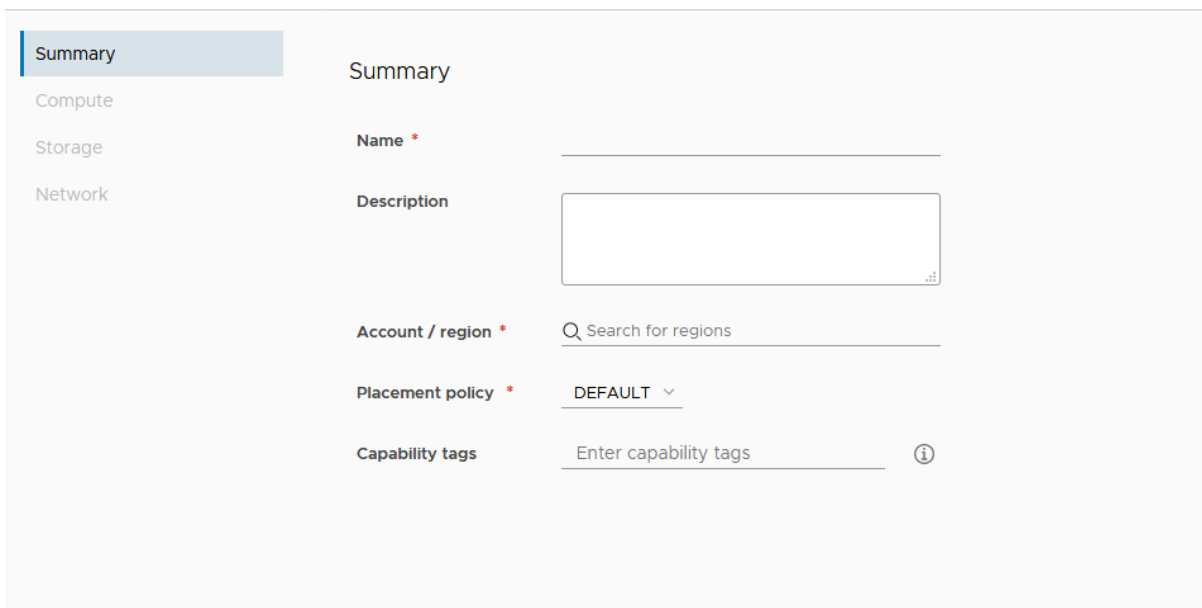
Procedimentos

- 1 Selecione **Infraestrutura > Configurar > Zonas virtuais privadas**

A página VPZ mostra todas as zonas existentes e permite a criação de zonas.

- 2 Clique em **Nova zona virtual privada**.

New Virtual Private Zone



Summary
Compute
Storage
Network

Summary

Name *

Description

Account / region *

Placement policy * DEFAULT ▾

Capability tags ⓘ

Existem quatro seleções no lado esquerdo da página, que podem se usadas para configurar informações de resumo e componentes de infraestrutura para a zona.

3 Digite as informações de resumo para a nova zona.

- a Adicione um nome e uma descrição.
- b Selecione uma conta à qual a zona se aplica.
- c Selecione uma política de colocação.

A política de posicionamento orienta a seleção de hosts para implantações na zona de nuvem especificada.

- **Padrão** - Distribui os recursos de processamento aleatoriamente em clusters e hosts. Essa seleção funciona em nível de máquina individual. Por exemplo, todas as máquinas em uma implantação específica são distribuídas aleatoriamente entre os clusters e hosts disponíveis que atendem aos requisitos.
- **binpack** - Coloca recursos de processamento no host mais carregado que possui recursos disponíveis suficientes para executar o processamento fornecido.
- **spread** - Provisiona recursos de processamento para implantação ao cluster ou host com o menor número de máquinas virtuais. Para o vSphere, o Distributed Resource Scheduler (DRS) distribui as máquinas virtuais pelos hosts. Por exemplo, todas as máquinas solicitadas em uma implantação são colocadas no mesmo cluster, mas a próxima implantação pode selecionar outro cluster do vSphere, dependendo da carga atual.

4 Selecione o recurso de processamento para a zona.

Adicione recursos de processamento conforme apropriado para a zona de nuvem. Inicialmente, a seleção de filtro inclui todo o processamento e a lista a seguir mostra todos os recursos de processamento disponíveis, e eles são alocados para a zona aplicável. Você tem duas opções adicionais para adicionar recursos de processamento a uma zona de nuvem.

- **Selecionar o processamento manualmente** - Selecione este item de menu se quiser selecionar manualmente os recursos de processamento na lista abaixo. Depois de selecioná-los, clique em Adicionar processamento para adicionar os recursos à zona.
- **Incluir dinamicamente o processamento por Tags** - Selecione este item de menu se você quiser selecionar o recurso de processamento a ser adicionado à zona com base nas tags. Todos os recursos de processamento são mostrados até que você adicione as tags apropriadas. Você pode selecionar ou inserir uma ou mais tags na opção Incluir processamento com essas tags.

Para qualquer uma das seleções de processamento, você pode remover um ou mais dos recursos de processamento mostrados na página marcando a caixa à direita e clicando em Remover.

5 Digite ou selecione as tags conforme apropriado.

6 Selecione armazenamento no menu à esquerda e selecione a política de armazenamento e outras configurações de armazenamento para a zona.

- 7 No menu à esquerda, selecione rede e defina as redes e, opcionalmente, uma política de rede a ser usada com essa zona. Você também pode configurar balanceadores de carga e grupos de segurança para as políticas de rede selecionadas.

| | |
|------------------------|--|
| Rede | <ul style="list-style-type: none"> ■ Todas as redes existentes associadas a este VPZ aparecem na tabela na guia Redes. ■ Clique em Adicionar rede para ver todas as redes associadas à região selecionada. Adicione uma rede para uso com esta zona. ■ Selecione uma rede e clique em Tags para adicionar uma ou mais tags à rede especificada. ■ Selecione Gerenciar intervalos de IP para especificar o intervalo de IP por meio do qual os usuários podem acessar essa rede. ■ Se aplicável, clique na guia Políticas de rede e selecione uma política de isolamento. |
| Políticas de rede | <p>Se configurado, selecione uma política de rede a ser usada com essa zona para aplicar uma política de isolamento para redes de saída e privadas.</p> <ul style="list-style-type: none"> ■ Selecione uma política de isolamento, se desejado. ■ Selecione um roteador lógico de camada 0 e um Edge Cluster, se desejar. |
| Balanceadores de carga | Clique em Adicionar balanceador de carga para configurar balanceadores de carga para as contas de nuvem de conta/região. |
| Grupos de segurança | Clique em Adicionar grupo de segurança para usar grupos de segurança e aplicar regras de firewall às máquinas provisionadas. |

Resultados

A zona virtual privada é criada com as alocações de recursos especificadas.

Próximo passo

Os administradores de nuvem podem associar o VPZ a um projeto.

- 1 No Cloud Assembly, selecione **Administração > Projetos**
- 2 Selecione a guia Provisionamento.
- 3 Clique em **Adicionar zona** e escolha Adicionar Zona Virtual Privada.
- 4 Selecione o VPZ desejado na lista.
- 5 Você pode definir a prioridade de provisão e os limites no número de instâncias, a quantidade de memória disponível e o número de CPUs disponíveis.
- 6 Clique em **Adicionar**.

Gerenciar a configuração da Zona Privada Virtual para tenants do vRealize Automation

Os administradores de provedor podem gerenciar zonas privadas virtuais (VPZs) dentro do Cloud Assembly para controlar a alocação de recursos de infraestrutura para cada tenant. Usando a página de Gerenciamento de Tenant, os administradores podem exibir tenants e zonas de VPZ e ativar ou desativar VPZs para tenants.

Por padrão, as Zonas Privadas Virtuais não são alocados para tenants. Você deve alocar as VPZ nesta página para usá-las com seus tenants.

Quando criadas inicialmente, as VPZ estão ativadas por padrão. Uma VPZ ativada está pronto para ser alocada e usada com o tenant especificado. Quando as VPZ estão desativadas, elas não podem ser usadas para provisionamento ou alocação a um tenant. Uma VPZ pode ser desativada, mas ainda alocado para um tenant.

Quando um administrador de provedor navega até a página Gerenciamento de Tenant, a página mostra todos os tenants disponíveis e o administrador pode selecionar um deles. Depois que um tenant é selecionado, a página mostra VPZs atualmente alocadas para ele, se houver. O administrador pode usar essa página para alocar VPZs ao tenant selecionado.

Quando uma VPZ é alocada, os administradores de tenants podem adicioná-la aos seus projetos e se tornam disponíveis para provisionamento por usuários de Tenant. Depois que um VPZ é alocado a um tenant, ela pode ser alocado a outro Tenant.

Após a ativação de uma VPZ, ela estará pronta para uso dentro do tenant especificado. Os administradores do provedor podem desativar a VPZ para facilitar a manutenção ou a reconfiguração do tenant e podem fornecer notificações aos usuários sobre a desativação. Se quiser tornar uma VPZ indisponível para um tenant de forma mais permanente, você poderá desalocá-la. Se uma VPZ existente for desalocada de um tenant por algum motivo, ela não poderá ser usada para criar implantações a partir desse tenant.

Pré-requisitos

- Configure vários tenants e crie Zonas Privadas Virtuais conforme apropriado para a sua implantação.
- Configure os mapeamentos globais de tipo e imagem para a configuração da VPZ e do tenant usando as seleções de menu de mapeamento de imagem e mapeamento de tipo no lado esquerdo da página Gerenciamento de Tenants no Cloud Assembly. Consulte [Criar mapeamento global de tipo e imagem para tenants do vRealize Automation](#).

Você pode substituir essas atribuições globais agora ou posteriormente usando as seleções de mapeamento de tipo e imagem específicas de tenant no topo da página Gerenciamento de Tenants. Consulte [Configurar mapeamentos de tipo e imagem específicos do tenant para vRealize Automation](#).

Procedimentos

- 1 No Cloud Assembly, selecione Gerenciar Tenants.

A página Gerenciamento de Tenant mostra todos os tenants configurados para a organização do administrador em uma exibição de cartão.

- 2 Clique em um tenant para selecioná-lo.
- 3 Clique na guia de gerenciamento de infraestrutura para ver todas as VPZ alocadas do tenant
- 4 Selecione **Alocar Zona Virtual Privada** para abrir uma caixa de diálogo que mostra todas as zonas não alocadas atualmente aos tenants. alocue a zona para um tenant.
- 5 Selecione uma ou mais zonas na caixa de diálogo e clique em **Alocar para o Tenant**.

Próximo passo

Após a alocação de VPZs, os administradores de tenants podem atribuí-las a projetos.

Os administradores de provedor podem usar a exibição de cartão de tenants para monitorar e gerenciar o status de VPZs.

- Se quiser desativar um tenant, clique em **Desativar** no cartão do tenant.
- Para ativar um tenant, clique em **Ativar** no cartão do tenant.
- Se quiser desalocar um tenant, clique em **Desalocar** no cartão desse tenant.

Criar mapeamento global de tipo e imagem para tenants do vRealize Automation

Os administradores de provedor podem selecionar ou criar mapeamentos globais de imagem e tipo que podem ser atribuídos aos tenants do vRealize Automation.

O mapeamento global de tipo e imagem permite que você configure rapidamente os mapeamentos que se aplicam a vários tenants. Você também pode atualizar esses mapeamentos rapidamente. A página de gerenciamento de tenants também permite criar mapeamentos de tipo e imagem específicos do tenant que podem substituir as configurações padrão.

Observação Os mapeamentos de tipo e imagem configurados na página Gerenciamento de Tenants se aplicam somente aos tenants conforme configurados e não são aplicáveis à organização de provedor mais ampla.

Pré-requisitos

Procedimentos

- 1 No Cloud Assembly, selecione Gerenciar Tenants.

A página Gerenciamento de Tenant mostra todos os tenants configurados para a organização do administrador em uma exibição de cartão.

- 2 Selecione Mapeamento de Imagem no menu à esquerda da página Gerenciamento de Tenants.

A página Mapeamento de Imagem exibe toda a imagem configurada atualmente para tenants no Cloud Assembly e indica se os mapeamentos são globais ou associados a um tenant específico.

Create Image Mapping ×

Account / region *

Search for regions

Image Name *

Image *

Search for images

Constraints

Example: !license:none:hard

Scope *

All tenants

Cloud Configuration

| | |
|---|--|
| 1 | |
|---|--|

CANCEL

CREATE

- 3 Selecione **Adicionar Mapeamento de Imagem** para adicionar um mapeamento de imagem para uso com tenants.
 - a Selecione a Conta/Região à qual o mapeamento de imagem será aplicado.
 - b Insira um nome para o mapeamento de imagem e selecione a instância ou a versão de imagem específica à qual ele está relacionado.
 - c Insira quaisquer tags de restrição desejadas.
 - d Selecione o escopo para o mapeamento de imagem. O escopo pode ser Todos os tenants ou global, ou você pode selecionar um tenant específico ao qual o mapeamento de imagem se aplicará.
- 4 Se desejar, é possível usar um script de configuração de nuvem para definir características do sistema operacional personalizadas para implantações.

Por exemplo, baseado na escolha de implantação de um modelo de nuvem em uma nuvem pública ou privada, é possível aplicar permissões de usuário específicas, permissões de SO ou outras condições à imagem. Um script de configuração de nuvem adere a um formato `cloud-init` para imagens baseadas no Linux ou a um formato `cloudbase-init` para imagens baseadas no Windows. Consulte [Saiba mais sobre mapeamentos de imagem no vRealize Automation](#) para obter mais informações.
- 5 Clique **Criar** para criar o mapeamento de imagem.

- 6 Selecione **Adicionar Mapeamento de Tipo** para adicionar um mapeamento de tipo para uso com tenants.

- a Selecione a Conta/Região à qual o mapeamento de tipo será aplicado.
 - b Insira um nome para o mapeamento de tipo que você está criando.
 - c Selecione os parâmetros Tamanho para o mapeamento de tipo que você está criando.
Você pode especificar o número de processadores e a quantidade de memória para esse tipo.
 - d Selecione o escopo para o mapeamento de tipo. O escopo pode ser Todos os tenants ou global, ou você pode selecionar um tenant específico ao qual o mapeamento de tipo se aplicará. A opção Todos os tenants se aplica a todos os tenants na organização do administrador do provedor.
- 7 Clique **Criar** para criar o mapeamento de tipo.

Resultados

Depois que você criar os mapeamentos globais, esse mapeamento será exibido nas guias Mapeamento de Tipo ou Mapeamento de Tenant na página Gerenciamento de Tenants para tenants aplicáveis.

Próximo passo

Você pode editar ou excluir mapeamentos globais de tipo e imagem nesta página. Para editar um mapeamento, selecione-o e faça as alterações desejadas.

Configurar mapeamentos de tipo e imagem específicos do tenant para vRealize Automation

O Cloud Assembly permite configurar mapeamentos globais de tipo e imagem que estão disponíveis para todas as Zonas Privadas Virtuais (VPZs) na sua organização. Como alternativa, você pode substituir as configurações globais e configurar mapeamentos de tipo e imagem específicos do tenant, conforme apropriado para suas implantações.

Normalmente, um administrador de nuvem configura mapeamentos globais de imagem e tipo usando os links de navegação à esquerda na página Gerenciamento de Tenants, e esses mapeamentos se aplicam em todos os seus tenants. Em alguns casos, você pode querer criar mapeamentos de tipo e imagem personalizados, específicos de tenant para tenants específicos, e a página Gerenciamento de Tenants mostra essa opção.

Os mapeamentos de tipo e imagem são exibidos em suas respectivas guias na página Gerenciamento de Tenants. Clique em qualquer um dos mapeamentos de tipo e imagem existentes para editá-los. Para excluir um mapeamento de tipo ou imagem, selecione o mapeamento e clique em **Excluir**.

Pré-requisitos

- Ative vários tenants e configure tenants para a sua implantação.
- Crie VPZs apropriadas.

Procedimentos

- 1 Selecione Gerenciamento de Tenants no menu principal do Cloud Assembly.
- 2 Selecione o tenant para o qual você deseja configurar o mapeamento de tipo ou imagem personalizado.
- 3 Selecione o link de Mapeamento de Imagem no topo da página e clique em **Adicionar Mapeamento de Imagem**.

A caixa de diálogo Criar Mapeamento de Imagem é exibida.

- 4 Verifique se a Conta/Região especificada está correta e adicione um nome para o mapeamento na caixa de texto **Nome da Imagem**.
- 5 Selecione a imagem da máquina subjacente a ser usada no menu suspenso **Imagem**.
- 6 Adicione tags de restrição, se aplicável, para o uso de imagem.
- 7 Selecione o **Escopo** apropriado para a imagem.
 - Clique no botão de opção Disponível somente para este tenant se você quiser que esse mapeamento de imagem fique disponível apenas para uso pelo tenant selecionado.
 - Clique no botão de opção Compartilhado entre tenants se quiser que este mapeamento de imagem seja disponibilizado para uso por outros tenants.
- 8 Clique **Criar** para salvar o mapeamento de imagem conforme configurado.

- 9 Selecione o link Mapeamento de Tipo no topo da página e clique em **Adicionar Mapeamento de Tipo** para criar um mapeamento de tipo.

A caixa de diálogo Criar Mapeamento de Tipo é exibida.

- 10 Verifique se a Conta/Região especificada está correta e adicione um nome para o mapeamento na caixa de texto **Nome**.
- 11 Especifique as configurações de CPU e de memória do tipo no campo **Valor**.
- 12 Selecione o **Escopo** apropriado para a imagem.
 - Clique no botão de opção Disponível somente para este tenant se você quiser que esse mapeamento de imagem fique disponível apenas para uso pelo tenant selecionado.
 - Clique no botão de opção Compartilhado entre tenants se quiser que este mapeamento de imagem seja disponibilizado para uso por outros tenants.
- 13 Clique **Criar** para salvar o mapeamento de tipo conforme configurado.

Resultados

Os mapeamentos de tipo e imagem específicos do tenant são configurados conforme especificado.

Criar assinaturas de extensibilidade para provedores ou tenants

Administradores de provedor e tenant podem criar assinaturas de extensibilidade para acessar fluxos de trabalho do vRealize Orchestrator. Os fluxos de trabalho do vRealize Orchestrator são disparados com base em eventos quando há uma assinatura para alguns tópicos de eventos que corresponda a uma determinada fase do ciclo de vida do aplicativo.

As características de uma assinatura de extensibilidade diferem dependendo de a assinatura ter sido criada por um administrador de provedor ou por um administrador de tenant.

- O administrador de tenant pode criar uma assinatura, mas não pode especificar o escopo da organização. Essa assinatura será ativada em eventos disparados somente pelo tenant.
- O administrador de provedor pode criar uma assinatura e especificar o escopo do provedor. A assinatura se comportará exatamente como a assinatura do tenant ou um ambiente não multitenant. Ela será ativada com base em eventos provenientes do provedor.
- O provedor pode criar uma assinatura e especificar o escopo do tenant. A assinatura é ativada com base em eventos provenientes de qualquer tenant. Ela não é ativada por eventos provenientes do provedor.

Assinaturas disparam fluxos de trabalho do vRealize Orchestrator com base em eventos específicos. Elas não invocam ações de extensibilidade. Atualmente, apenas uma instância do vRealize Orchestrator tem suporte para qualquer organização de provedor específica. Para obter mais informações sobre eventos, tópicos de eventos e assinaturas, consulte [Terminologia de extensibilidade](#).

Pré-requisitos

Configure tenants e zonas privadas virtuais conforme apropriado para a sua implantação.

Procedimentos

- 1 No vRealize Automation, navegue até a página Assinatura e clique em **Nova Assinatura**.
- 2 Insira um **Nome** e uma **Descrição** para a assinatura.
- 3 Certifique-se de que o botão de opção Ativar Assinatura esteja ativado.
Você poderá deixar esse botão na posição Desativado se não quiser que a assinatura fique ativa imediatamente.
- 4 Se você for um administrador de provedor, selecione o **Escopo da Organização** apropriado.
As opções de escopo da organização são Provedor ou Tenant. Se você selecionar Tenant, o escopo do projeto será qualquer projeto e não poderá ser alterado. Se você selecionar Provedor, poderá especificar o escopo do projeto usando a seleção na parte inferior da página Assinaturas.
- 5 Selecione o **Tópico de evento** que você deseja assinar.
- 6 Selecione um ou mais fluxos de trabalho.

Resultados

Provedores e tenants podem exibir os eventos retornados para uma implantação específica na página Eventos do Cloud Assembly. Os resultados exibidos dependem da sua função e do escopo da organização.

- Se o escopo da organização for Provedor, os provedores verão eventos com base em suas ações na mesma organização de provedor.
 - Se o escopo da organização for Tenant, os tenants verão os eventos, mas o provedor não. Eventos sempre residem na organização do publicador.
- 1 Selecione **Extensibilidade > Eventos** no Cloud Assembly.
 - 2 Na caixa de pesquisa da página Eventos, insira o ID da implantação cujos eventos você deseja visualizar.

A página exibe eventos que correspondem aos critérios de pesquisa.

Como trabalhar com zonas privadas virtuais legadas em versões mais recentes do vRealize Automation

As opções de configuração para VPZs mudaram no Cloud Assembly. Você pode atualizar ou trabalhar com Zonas Privadas Virtuais legadas nas versões atuais do vRealize Automation.

No vRealize Automation 8.2, os usuários configuravam mapeamentos de imagem e tipos dentro de VPZs. Em versões mais recentes do vRealize Automation, os usuários criam mapeamentos de imagens e tipos de acordo com cada tenant, o que aumenta a eficiência e a flexibilidade da configuração, especialmente em implantações com um grande número de tenants. Embora não haja uma maneira de migrar os VPZs herdados criados no vRealize Automation 8.2, há várias opções para usá-los com versões mais recentes do vRealize Automation.

A primeira opção, e a mais flexível, é excluir a imagem herdada e os mapeamentos de tipos das VPZs mais antigas e reconfigurá-las com novos mapeamentos criados na página Gerenciamento de Tenants.

- 1 Selecione **Infraestrutura > Configurar > Zonas Virtuais Privadas** para abrir a página VPZ.
- 2 Selecione Mapeamento de Imagens para visualizar o mapeamento existente.
- 3 Selecione mapeamentos e clique para excluí-los.
- 4 Selecione Mapeamento de Imagens para visualizar o mapeamento existente.
- 5 Selecione mapeamentos e clique para excluí-los.
- 6 Feche a página VPZ.
- 7 Selecione Mapeamento de tenants e selecione um mapeamento global para os tenants aplicáveis ou crie um mapeamento específico de tenant.

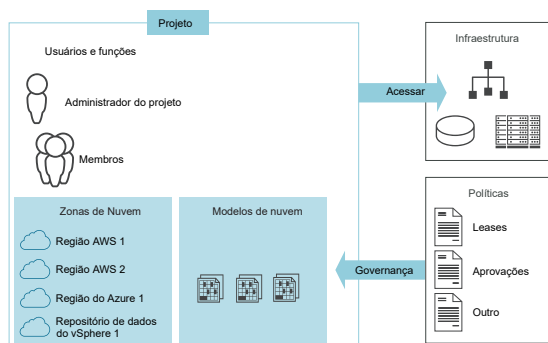
Como alternativa, você pode usar VPZs legadas com versões mais recentes do vRA na sua configuração existente. A imagem herdada e os mapeamentos de tipo ainda funcionam como configurados, mas suas opções de configuração são somente leitura na página VPZ. Essas opções oferecem menos flexibilidade que a primeira opção.

Como adicionar e gerenciar projetos do Cloud Assembly

5

Os projetos controlam quem tem acesso a modelos de nuvem do Cloud Assembly e onde esses modelos são implantados. É possível usar projetos para organizar e determinar o que seus usuários podem fazer e para quais zonas de nuvem podem implantar modelos de nuvem na infraestrutura em nuvem.

Os administradores de nuvem configuram os projetos aos quais eles podem adicionar usuários e zonas de nuvem. Qualquer pessoa que cria e implanta modelos de nuvem deve ser membro de pelo menos um projeto.



Este capítulo inclui os seguintes tópicos:

- [Como adicionar um projeto para minha equipe de desenvolvimento do Cloud Assembly](#)
- [Saiba mais sobre projetos do Cloud Assembly](#)

Como adicionar um projeto para minha equipe de desenvolvimento do Cloud Assembly

Crie um projeto no qual são adicionados membros e zonas de nuvem para que os membros do projeto possam implantar modelos de nuvem nas zonas associadas. Como administrador do Cloud Assembly, cria-se um projeto para uma equipe de desenvolvimento. Em seguida, é possível atribuir o administrador de projeto ou operar como administrador do projeto.

Ao criar um modelo de nuvem, você primeiro seleciona o projeto ao qual associá-lo. O projeto deve existir antes que seja possível criar o modelo de nuvem.

Certifique-se de que seus projetos atendam às necessidades de negócios da equipe de desenvolvimento.

- O projeto fornece os recursos que oferecem suporte às metas da equipe? Para obter um exemplo de como os recursos de infraestrutura e um projeto oferecem suporte a um modelo de nuvem, consulte [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).
- Os membros do seu projeto exigem ou esperam que suas implantações sejam compartilhadas ou privadas? As implantações compartilhadas estão disponíveis para todos os membros do projeto na página Implantações, não apenas para o membro responsável pela implantação. É possível alterar o estado de compartilhamento da implantação a qualquer momento.

Quando você compartilha a implantação com os membros do projeto, estes podem executar a mesma ação de dia 2. Para gerenciar a capacidade dos membros de executar ações de dia 2, você pode criar políticas de dia 2 no Service Broker. As políticas se aplicam a implantações do Cloud Assembly e do Service Broker.

Para saber mais sobre as políticas de dia 2, consulte [Como autorizar usuários de implantações a ações de Dia 2 usando políticas](#).

Esse procedimento é baseado na criação de um projeto inicial que inclui apenas as configurações básicas. À medida que a sua equipe de desenvolvimento cria e implanta seus modelos de nuvem, você pode modificar o projeto. É possível adicionar restrições, propriedades personalizadas e outras opções para melhorar a eficiência da implantação. Consulte os artigos disponíveis em [Saiba mais sobre projetos do Cloud Assembly](#).

Pré-requisitos

- Verifique você se configurou as zonas de nuvem. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).
- Verifique se você configurou os mapeamentos e perfis para as regiões que incluem as zonas de nuvem para este projeto. Consulte [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#).
- Verifique se você tem as permissões necessárias para realizar essa tarefa. Consulte [Quais são as funções de usuário do vRealize Automation](#).
- Determine quem foi designado como administrador de projeto. Para entender o que o administrador do projeto pode fazer no Cloud Assembly, consulte [Quais são as funções de usuário do vRealize Automation](#).
- Se você estiver adicionando grupos do Active Directory a projetos, verifique se configurou esses para a sua organização. Consulte [Editar atribuições de funções de grupo no vRealize Automation](#), em *Administrando o vRealize Automation*. Se os grupos não forem sincronizados, eles não ficarão disponíveis quando você tentar adicioná-los a um projeto.

Procedimentos

- 1 Selecione **Infraestrutura > Administração > Projetos** e clique em **Novo projeto**.

2 Digite o nome do projeto.

3 Clique na guia **Usuários**.

- a Para tornar as implantações pelos membros do projeto acessíveis apenas ao usuário solicitante, desative **Compartilhamento de implantação**. Para garantir que você possa atribuir a propriedade de uma implantação a outro membro do projeto, certifique-se de que o **Compartilhamento de implantação** esteja ativado.
- b Adicione usuários com funções atribuídas.

4 Clique na guia **Provisionamento** e adicione uma ou mais zonas de nuvem.

Adicione zonas de nuvem e zonas virtuais privadas que contenham os recursos que suportam os modelos de nuvem implantados pelos usuários do projeto.

Para cada zona, você pode definir uma prioridade de zona e pode limitar a quantidade de recursos que o projeto pode usar. Os limites possíveis incluem o número de instâncias, memória e CPUs. Apenas para zonas de nuvem do vSphere, você pode configurar limites de armazenamento para recursos implantados que são baseados em modelos de VM do vSphere. Os limites de armazenamento são avaliados com a sua implantação de solicitações e quando você faz alterações usando as ações de redimensionar disco, redimensionar disco de inicialização, remover disco e atualizar contagem. Esses limites de armazenamento não se aplicam a outros tipos de recursos, como AWS, Microsoft Azure ou Google Cloud Platform.

Ao adicionar cada zona e aplicar os limites, não limite os recursos do projeto a ponto de os membros não conseguirem implantar seus modelos de nuvem.

Quando seus usuários enviam uma solicitação de implantação, as zonas são avaliadas para determinar quais têm os recursos para oferecer suporte à implantação. Se mais de uma zona oferecer suporte à implantação, a prioridade será avaliada e a carga de trabalho será colocada na que tem a prioridade mais alta, que é o menor número inteiro.

5 Se as cargas de trabalho solicitadas para esse projeto levarem mais de duas horas para implantar, insira um valor mais longo para **Tempo limite**.

O valor padrão é duas horas.

6 Clique em **Criar**.

7 Para testar o projeto com as zonas de nuvem do projeto, clique em **Configuração de Teste** na página Projetos.

A simulação executa um teste de implantação hipotética padronizado em relação aos recursos da zona de nuvem do projeto. Se ele falhar, será possível revisar os detalhes e corrigir a configuração do recurso.

Próximo passo

Introdução a modelos de nuvem. Consulte [Capítulo 6 Como projetar suas implantações do Cloud Assembly](#).

Saiba mais sobre projetos do Cloud Assembly

Os projetos conectam os modelos de nuvem aos recursos. Quanto maior seu entendimento sobre como eles funcionam e sobre como aplicá-los, mais eficaz será o processo de desenvolvimento e implantação do Cloud Assembly.

Usando tags de projeto e propriedades personalizadas do Cloud Assembly

Como administrador, você pode adicionar restrições de governança ou propriedades personalizadas em nível de projeto quando os requisitos do projeto forem diferentes dos modelos de nuvem do Cloud Assembly. Além de tags de restrição, você pode adicionar tags de recursos que são adicionadas aos recursos implantados durante o processo de provisionamento, para que você possa gerenciar os recursos.

O que são tags de recursos de projeto

Uma tag de recurso de projeto opera como uma tag de identificação padronizada que você pode usar para gerenciar os recursos implantados e garantir a conformidade.

As tags de recursos definidas em um projeto são adicionadas a todos os recursos de componentes implantados como parte desse projeto. Em seguida, você pode usar a marcação padrão para gerenciar os recursos usando outros aplicativos, por exemplo, monitorar o custo de gastos usando o CloudHealth e, mais importante, para garantir a conformidade.

Por exemplo, como administrador de nuvem, você deseja usar um aplicativo como o CloudHealth para gerenciar custos. Você adiciona a tag `costCenter:eu-cc-1234` a um projeto dedicado ao desenvolvimento de uma ferramenta de recursos humanos da União Europeia. Quando a equipe do projeto implanta a partir desse projeto, a tag é adicionada aos recursos implantados. Em seguida, você configura a ferramenta de cálculo de custos para identificar e gerenciar os recursos que incluem essa tag. Outros projetos com outros centros de custo teriam valores alternativos para acompanhar a chave.

O que são tags de restrição de projeto

Uma restrição de projeto opera como uma definição de governança. É uma tag `key:value` que define quais recursos a solicitação de implantação consome ou evita nas zonas de nuvem do projeto.

O processo de implantação procura tags para as redes e o armazenamento que são correspondidos às restrições do projeto e implanta com base em tags correspondentes.

A restrição de extensibilidade é usada para especificar qual instância integrada do vRealize Orchestrator será usada para fluxos de trabalho de extensibilidade.

Considere os seguintes formatos quando você configurar as restrições do projeto.

- **key:value** e **key:value:hard**. Use essa tag em qualquer formato quando o modelo de nuvem tiver que ser provisionado em recursos com a tag de recurso correspondente. O processo de implantação falhará quando nenhuma tag correspondente for encontrada. Por exemplo,

um modelo de nuvem implantado pelos membros de um projeto deve ser provisionado em uma rede compatível com PCI. É usado `security:pci`. Se nenhuma rede for encontrada nas zonas de nuvem do projeto, a implantação falhará, garantindo que não seja feita nenhuma implantação não segura.

- **key:value:soft.** Use essa tag quando preferir um recurso correspondente, mas desejar que o processo de implantação prossiga sem falhas e aceite recursos nos quais a tag não corresponde. Por exemplo, se for preferível que os membros do projeto implantem os modelos de nuvem em um armazenamento mais barato, mas não for desejável que a disponibilidade de armazenamento interfira em na capacidade de implantação. É usado `tier:silver:soft`. Se não houver uma camada marcada de `tier:silver` nas zonas de nuvem do projeto, o modelo de nuvem ainda será implantado em outros recursos de armazenamento.
- **!key:value.** Use essa tag, com rígida ou flexível, quando quiser evitar a implantação de recursos com uma tag correspondente.

Além disso, as tags de restrição de projeto têm prioridade mais alta do que as tags de restrição de modelo de nuvem, substituindo-as no momento da implantação. Se houver um modelo de nuvem no qual isso nunca deve acontecer, será possível usar `failOnConstraintMergeConflict:true` no modelo. Por exemplo, se o projeto tiver uma restrição de rede `loc:london`, mas o modelo de nuvem for `loc:mumbai`, mas, em vez de o local do projeto ter precedência, você deseja que a implantação falhe com uma mensagem de conflito de restrição, adicione uma propriedade semelhante à do exemplo a seguir.

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

Como posso usar as propriedades personalizadas de projeto

É possível usar uma propriedade personalizada de projeto para relatórios, para disparar e preencher ações de extensibilidade e fluxo de trabalho e para substituir as propriedades no nível do modelo de nuvem.

Adicionar uma propriedade personalizada a uma implantação permite usar o valor na interface do usuário ou recuperá-la usando a API para que se possa gerar relatórios.

A extensibilidade também pode usar uma propriedade personalizada para uma assinatura de extensibilidade. Para obter mais informações sobre extensibilidade, consulte [Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade](#).

Um modelo de nuvem pode ter um determinado valor de propriedade desejado para alterar em um projeto. É possível fornecer um nome e um valor alternativos como uma propriedade personalizada.

Você também pode criptografar o valor da propriedade para que nem você e nem seus usuários possam ver o valor incluído na implantação. Por exemplo, você pode criptografar uma senha que todos os usuários no projeto usam, mas que você não deseja que seja visível. Depois de criptografar o valor e salvar o projeto, você não poderá desmascarar ou substituir o valor. Se você desmarcar a caixa de seleção **Criptografado**, o valor será removido. Você deve inserir um valor novamente.

Como as políticas de posicionamento em nível de projeto afetam a alocação de recursos no vRealize Automation

Como administrador, você pode definir a política de posicionamento para projetos em que mais de uma zona de nuvem esta qualificada como a zona de destino da implantação. Por exemplo, você pode ter um projeto no qual deseja implantar modelos de nuvem com base na prioridade definida. Ou você pode querer balancear os recursos implantados em várias zonas com base em qual delas tem a melhor proporção entre VM e host.

Considerações de alocação

Para uma política de colocação padrão ou de dispersão.

- Se o usuário de implantação tiver permissão para gerenciar contas de nuvem que estão no modo de manutenção, o processo de alocação poderá selecionar uma conta de nuvem que esteja no modo de manutenção, pois o usuário pode precisar executar uma implantação de teste antes de fechar a janela de manutenção.
- Se o usuário não tiver permissão para gerenciar contas de nuvem, as contas de nuvem que estão no modo de manutenção serão filtradas do processo de alocação.
- Os hosts que estão no modo de manutenção são contados como parte da proporção de propagação. Para excluir um host em manutenção do cálculo de proporção, você deve definir o estado de energia como desligado.

Para uma política de propagação.

- As proporções são calculadas com base nos hosts. Os hosts podem ser autônomos ou fazer parte de um cluster.
- Se um host autônomo estiver desligado, ele não será contado como parte da proporção.
- Se um host que faz parte de um cluster estiver desligado, o estado desligado não será refletido no cluster e o host ainda será considerado ao calcular a proporção.

Como definir a política de posicionamento

Se você tiver várias zonas de nuvem em um projeto que estejam igualmente qualificadas como destino para uma implantação, a solicitação de implantação avaliará onde colocá-las com base na configuração da **Política de posicionamento**.

- 1 Selecione **Infraestrutura > Projetos** e crie ou selecione um projeto.
- 2 No projeto, clique na guia **Provisionamento**.

3 Selecione uma política.

| Política de colocação | Descrição |
|-----------------------|--|
| Padrão | <p>Implanta os recursos solicitados na primeira zona de nuvem que corresponde aos requisitos.</p> <p>Selecione Padrão quando você quiser que as cargas de trabalho sejam implantadas na ordem de prioridade e não se importar em usar todos os recursos em um host.</p> <p>Se essa opção estiver selecionada, os valores de VM e Hosts não serão recuperados.</p> |
| Dispersão | <p>Implanta os recursos solicitados na zona de nuvem com o menor número de máquinas virtuais por host.</p> <p>Selecione Dispersão quando quiser distribuir as cargas de trabalho entre os hosts utilizando os recursos amplamente entre esses hosts.</p> <p>Se essa opção estiver selecionada, o número de VMs e hosts será recuperado dos recursos da zona de nuvem e avaliado.</p> |

4 Clique em **Salvar**.

Revisar como a política é aplicada

Depois de configurar a política de posicionamento em nível de projeto, você pode ver onde o sistema planeja implantar o modelo de nuvem em um diagrama de provisionamento.

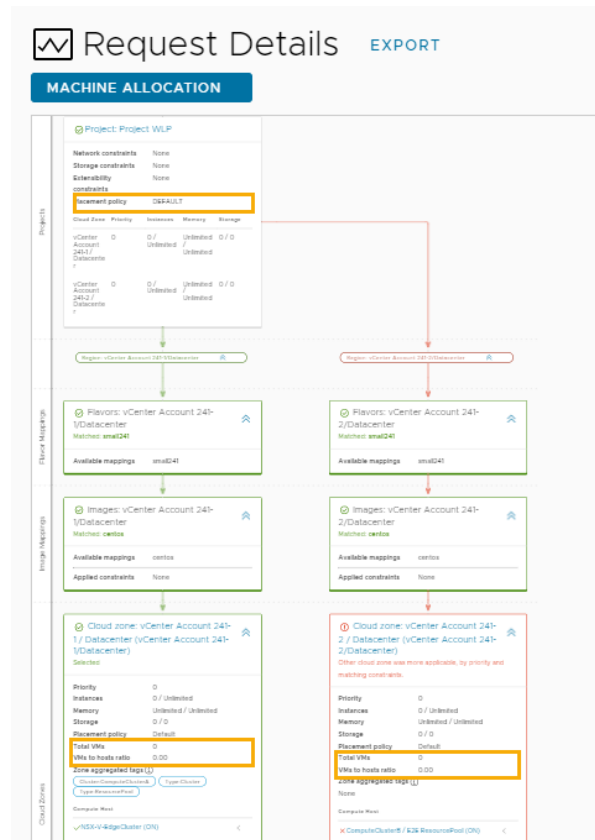
- 1 Selecione **Projetar > Modelos de Nuvem** e selecione ou configure um modelo que use o projeto para o qual você selecionou uma política.
- 2 Clique em **Testar**.
- 3 Quando o teste for concluído com êxito, clique em **Diagrama de Provisionamento** nos resultados do teste.

4 O diagrama será semelhante a um dos dois exemplos.

Tipo de Política

Diagrama de provisionamento

Padrão



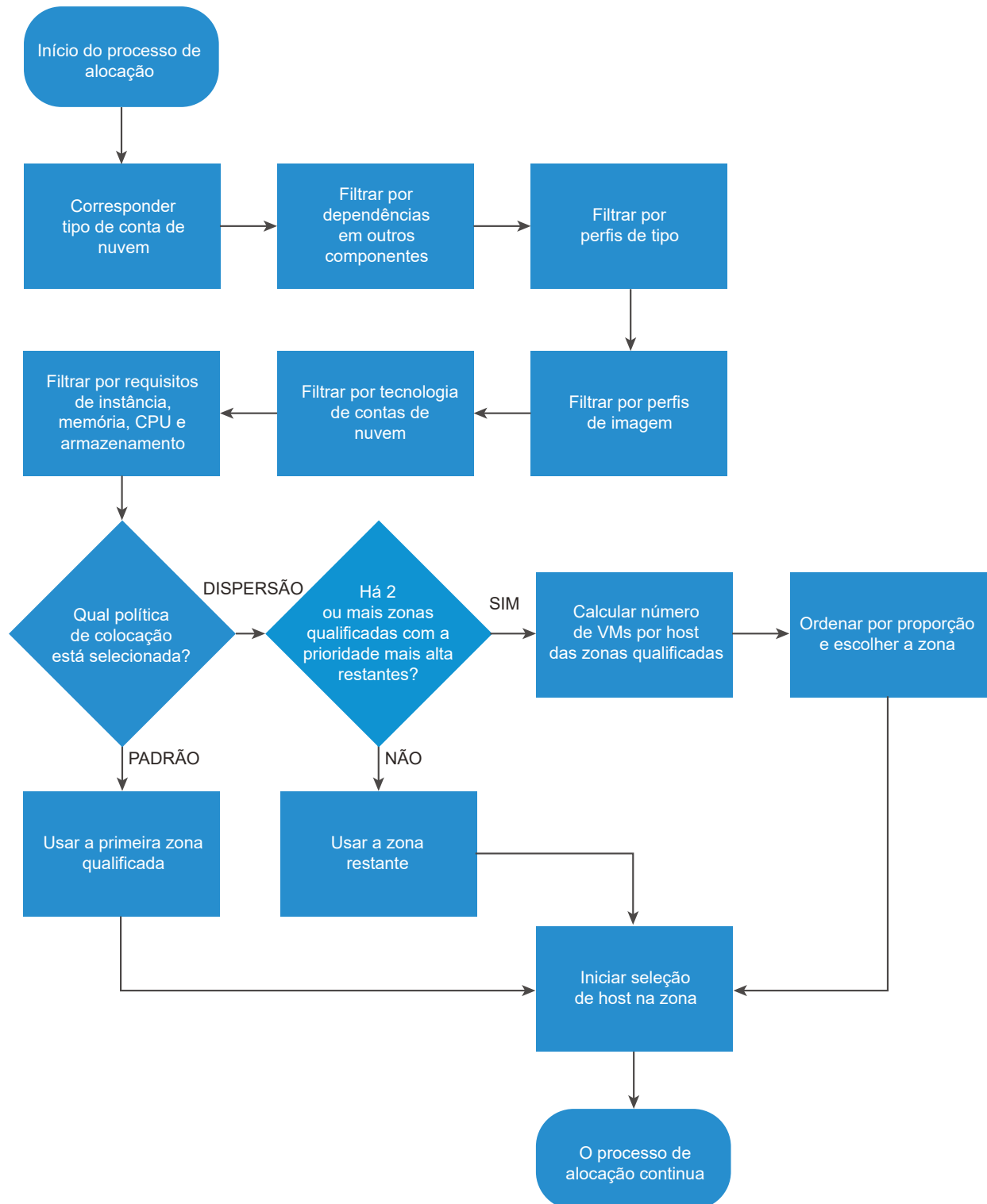
Dispersão



5 Se você estiver pronto para implantar, retorne ao modelo de nuvem e clique em **Implantar**.

Avaliação da política de posicionamento durante o processo de alocação

O diagrama a seguir ajuda você a compreender quando a política é avaliada durante o processo de alocação e quando a zona de destino e o host são identificados.



Quais são os preços de projetos no Cloud Assembly

Os custos disponíveis nos projetos do Cloud Assembly ajudam a gerenciar as despesas de recursos associadas a projetos inteiros. O projeto também inclui os custos de implantação individuais.

Ansible-Project DELETE

Summary Users Provisioning Kubernetes Provisioning **Price** Integrations

Price Analysis **\$10.81**
Month to date (private cloud only)

| Deployment Name | Description | Requestor | Created On | Expiring In | Price |
|---------------------------|-------------|----------------|--------------|---------------|--------|
| AnsibleTower-Demo | | slu@vmware.com | Jan 26, 2021 | Never expires | \$3.07 |
| Check-Delete | | ks@vmware.com | Jan 18, 2021 | Never expires | \$3.04 |
| Ansible vSphere | | slu@vmware.com | Jan 19, 2021 | Never expires | \$3.01 |
| WT with 2 machines | | slu@vmware.com | Feb 14, 2021 | Never expires | \$0.61 |
| Create with templates | | slu@vmware.com | Feb 14, 2021 | Never expires | \$0.32 |
| Ansible | | slu@vmware.com | Jan 07, 2021 | Never expires | \$0.31 |
| Create with job templates | | slu@vmware.com | Feb 14, 2021 | Never expires | \$0.31 |

7 deployments

SAVE CANCEL

As informações de custo visualizadas para um projeto e para as implantações individuais aparecem após pelo menos uma implantação associada ao projeto ser provisionada. Os custos são calculados e atualizados diariamente para ser possível rastrear o custo de uma implantação ao longo do tempo. Os valores iniciais são baseados em parâmetros de comparação do setor.

Os administradores de nuvem podem ajustar os valores para refletir os custos reais.

Para obter mais informações, consulte [Como usar cartões de preços no vRealize Automation](#).

Como funcionam os projetos do Cloud Assembly no momento da implantação

Os projetos controlam o acesso do usuário às zonas de nuvem e à propriedade do usuário dos recursos provisionados. Seja você um administrador de nuvem ou um desenvolvedor de modelo de nuvem, é necessário compreender como os projetos funcionam no momento da implantação para poder gerenciar as implantações e solucionar quaisquer problemas.

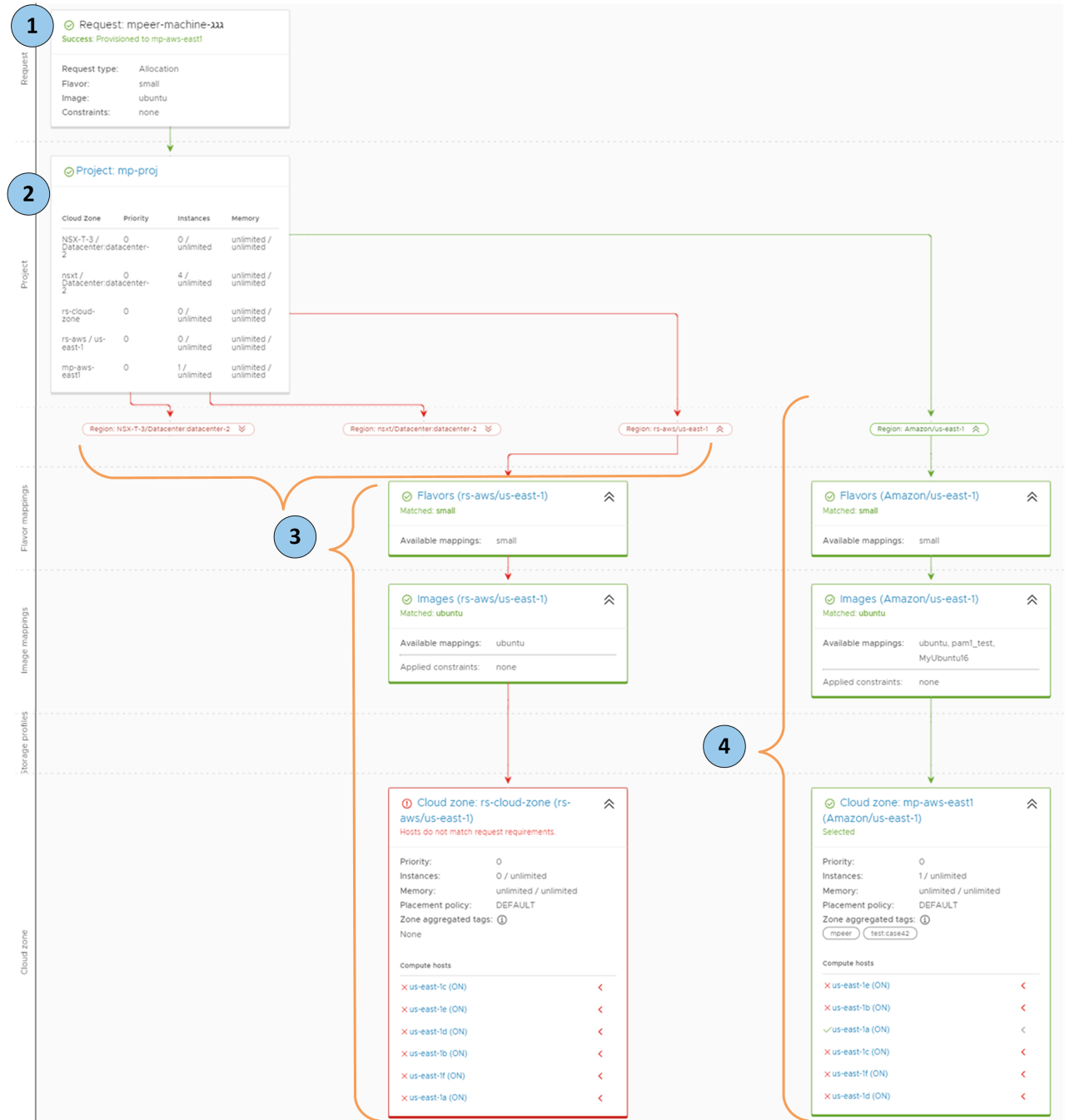
Como administrador de nuvem que está configurando projetos para várias equipes, é necessário compreender como os projetos determinam onde os componentes do modelo de nuvem serão implantados. Essa compreensão ajuda a criar projetos que oferecem suporte a desenvolvedores de modelo de nuvem e a solucionar falhas de implantações.

Quando você cria um modelo de nuvem, primeiro associe-o a um projeto. No momento da implantação, os requisitos de modelo de nuvem são avaliados em relação às zonas de nuvem do projeto para encontrar o melhor local de implantação.

O seguinte fluxo de trabalho ilustra o processo.

- 1 É enviada uma solicitação de implantação de modelo de nuvem.

- 2 O projeto avalia os requisitos de modelo e projeto, por exemplo, tags de tipo, imagem e restrição. Os requisitos são comparados às zonas de nuvem do projeto para localizar uma zona compatível com os requisitos.
- 3 Essas zonas não tinham os recursos para suportar a solicitação.
- 4 Essa zona de nuvem oferece suporte aos requisitos de solicitação e o modelo é implantado nessa região da conta da zona de nuvem.



Como projetar suas implantações do Cloud Assembly

6

Implantações começam com modelos de nuvem, antes chamados de blueprints, que são especificações que definir máquinas, aplicativos e serviços a serem criados em recursos de nuvem por meio do Cloud Assembly.

Como os modelos de nuvem funcionam

Modelos podem se destinar a fornecedores de nuvem específicos ou ser independentes da nuvem. As zonas de nuvem atribuídas ao seu projeto determinam qual abordagem deve ser tomada. Consulte seu administrador de nuvem para saber quais tipos de recursos compõem suas zonas de nuvem.

A criação de modelos do Cloud Assembly é um processo de infraestrutura como código. Você começa adicionando recursos na tela de design. Em seguida, preenche os detalhes usando o editor de código. O editor de código permite digitar o código diretamente ou inserir valores em um formulário.

Antes de criar um modelo de nuvem

É possível criar um modelo do Cloud Assembly a qualquer momento. Para implantá-lo, no entanto, primeiro é necessário [Capítulo 4 Como compilar a infraestrutura de recursos do Cloud Assembly](#) e [Capítulo 5 Como adicionar e gerenciar projetos do Cloud Assembly](#) que inclua essa infraestrutura.

Pronto para projetar?

Explore a navegação à esquerda ou acesse diretamente os tópicos na tabela a seguir.

| Primeiros passos | Saiba mais sobre designs e recursos de modelos de nuvem | | Mais exemplos |
|---|--|---|---|
| Primeiros passos com designs do Cloud Assembly | Entrada do usuário em solicitações do vRealize Automation | Sinalizadores de recursos do Cloud Assembly para solicitações | Exemplo de modelo do Cloud Assembly documentado |
| Criando associações e dependências entre recursos no Cloud Assembly | Nomenclatura personalizada para recursos implantados no Cloud Assembly | Expressões do Cloud Assembly | Exemplos de recursos do vSphere no Cloud Assembly |

| Primeiros passos | Saiba mais sobre designs e recursos de modelos de nuvem | | Mais exemplos |
|---|--|--|--|
| Controlando a versão dos seus modelos do Cloud Assembly | Reutilizando um grupo de propriedades no Cloud Assembly | Propriedades secretas do Cloud Assembly | Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation |
| Outras maneiras de criar modelos do Cloud Assembly | Acesso remoto a uma implantação do Cloud Assembly | Inicialização de máquinas no Cloud Assembly | Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation |
| Obtendo ajuda para complementação de código no Cloud Assembly | Endereços IP estáticos do vSphere no Cloud Assembly | Configurações do Terraform no Cloud Assembly | Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation |
| | Clusters de máquina e disco no Cloud Assembly | Posicionamento de discos SCSI com o Cloud Assembly | Exemplos de modelo de nuvem de configuração do Puppet no vCenter |
| | Tipos de recursos personalizados para modelos de nuvem do Cloud Assembly | Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade | |

Este capítulo inclui os seguintes tópicos:

- [Primeiros passos com designs do Cloud Assembly](#)
- [Obtendo ajuda para complementação de código no Cloud Assembly](#)
- [Criando associações e dependências entre recursos no Cloud Assembly](#)
- [Controlando a versão dos seus modelos do Cloud Assembly](#)
- [Entrada do usuário em solicitações do vRealize Automation](#)
- [Reutilizando um grupo de propriedades no Cloud Assembly](#)
- [Sinalizadores de recursos do Cloud Assembly para solicitações](#)
- [Expressões do Cloud Assembly](#)
- [Propriedades secretas do Cloud Assembly](#)
- [Acesso remoto a uma implantação do Cloud Assembly](#)
- [Posicionamento de discos SCSI com o Cloud Assembly](#)
- [Inicialização de máquinas no Cloud Assembly](#)
- [Clusters de máquina e disco no Cloud Assembly](#)
- [Nomenclatura personalizada para recursos implantados no Cloud Assembly](#)
- [Como adicionar o recurso SaltStack Config em designs do Cloud Assembly](#)
- [Configurações do Terraform no Cloud Assembly](#)

- Tipos de recursos personalizados para modelos de nuvem do Cloud Assembly
- Designs do Cloud Assembly que preparam para alterações de dia 2
- Outros exemplos de código do Cloud Assembly
- Esquema de propriedades de recursos do vRealize Automation
- Outras maneiras de criar modelos do Cloud Assembly
- Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade

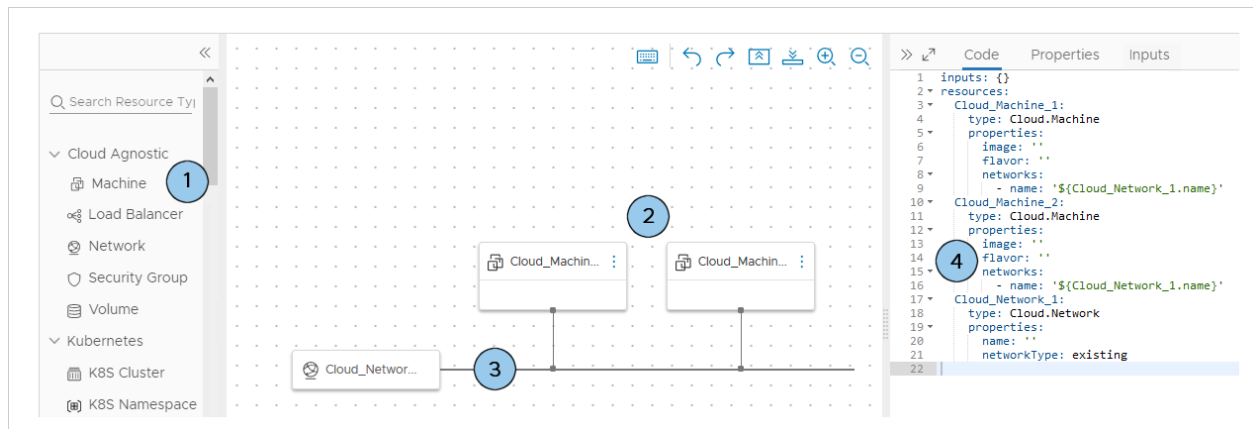
Primeiros passos com designs do Cloud Assembly

Use a página **Projetar** para criar especificações do modelo do Cloud Assembly para as máquinas e aplicativos que você deseja provisionar.

Como usar a página **Projetar**

Para criar um modelo de nuvem do zero, acesse **Projetar > Modelos de Nuvem**. Em seguida, clique em **Novo de > Tela em branco**.

- 1 Localize recursos.
- 2 Arraste os recursos até a tela.
- 3 Conecte recursos.
- 4 Configure os recursos editando o código do modelo de nuvem.



Selecionando e adicionando recursos à tela

Os recursos aparecem à esquerda da página **Projetar** para seleção e movimentação.

| | |
|---|---|
| Recursos independentes da nuvem | É possível implantar recursos independentes de nuvem para qualquer fornecedor de nuvem. No momento do provisionamento, a implantação usa recursos específicos da nuvem que são correspondidos. Por exemplo, se você espera que um modelo de nuvem seja implantado em zonas de nuvem da AWS e do vSphere, use componentes independentes de nuvem. |
| Recursos do fornecedor de nuvem | Recursos do fornecedor, como aqueles específicos para a Amazon Web Services, o Microsoft Azure, a Google Cloud Platform ou o VMware vSphere, só podem ser implantados em zonas de nuvem AWS, Azure, GCP ou vSphere correspondentes. É possível adicionar recursos independentes de nuvem a um modelo de nuvem que contenha recursos específicos de nuvem de um determinado fornecedor. Basta saber quais são as zonas de nuvem do projeto compatíveis em termos de fornecedor. |
| Recursos de gerenciamento de configuração | Os recursos de gerenciamento de configuração dependem dos seus aplicativos integrados. Por exemplo, um recurso do Puppet pode monitorar e reforçar a configuração dos outros recursos. |

Conectando recursos

Use os controles gráficos tela de design do Cloud Assembly para conectar recursos.

Os recursos devem ser compatíveis para uma conexão. Por exemplo:

- Conectar um balanceador de carga a um cluster de máquinas.
- Conectar uma máquina a uma rede.
- Conectar o armazenamento externo a uma máquina.

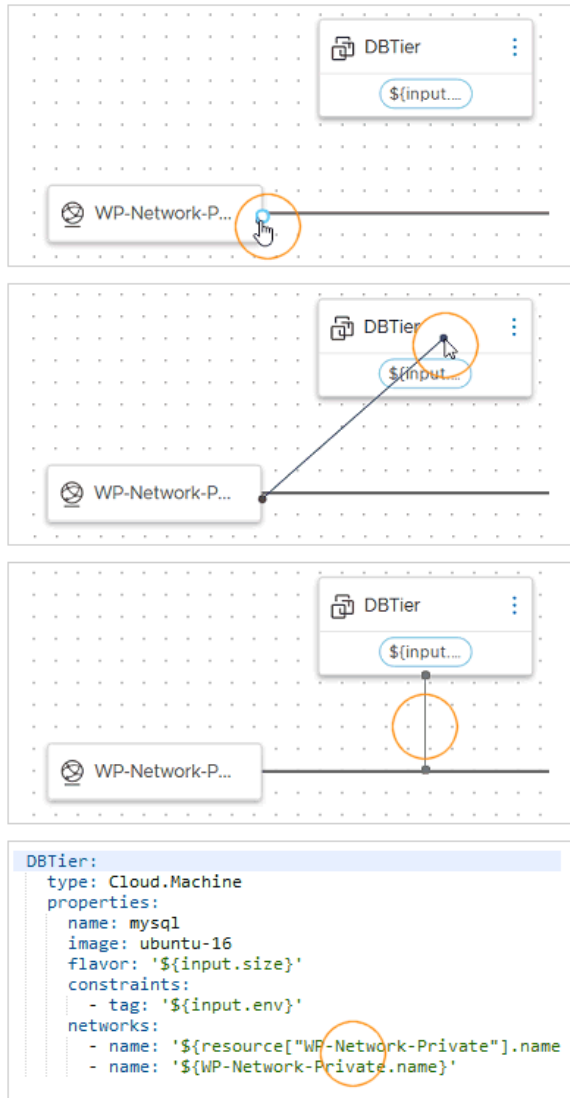
Importante Um conector com linha sólida requer que os dois recursos sejam implantados na mesma zona de nuvem. Se você adicionar restrições conflitantes aos recursos, a implantação poderá falhar.

Por exemplo, não é possível implantar recursos conectados em que tags de restrição forcem o posicionamento de um dos recursos em uma zona em us-west-1 e do outro recurso em uma zona em us-east-1.

Setas sólidas ou tracejadas indicam apenas uma dependência, e não uma conexão. Para obter mais informações sobre dependências, consulte [Criando associações e dependências entre recursos no Cloud Assembly](#).

Para conectar, passe o cursor sobre a borda de um recurso para revelar a bolha de conexão. Em seguida, clique e arraste a bolha até o recurso e a liberação de destino.

No editor de código, o código adicional para o recurso de origem aparece no código do recurso de destino.



Na figura, a máquina SQL e a rede privada estão conectadas e, portanto, devem ser implantadas na mesma zona de nuvem.

Editando o código do modelo de nuvem

O editor de código permite que você digite, recorte, copie e cole o código diretamente. Se não se sentir à vontade ao editar o código, você poderá clicar em um recurso que já esteja na tela de design, clicar na guia **Propriedades** do editor de código e inserir valores lá. Os valores de propriedades inseridos aparecerão no código como se você os tivesse digitado diretamente.

The screenshot displays the vRealize Automation Cloud Assembly interface. On the left, a code editor shows the following JSON configuration for a 'WebTier' resource:

```
WebTier:
  type: Cloud.Machine
  properties:
    name: wordpress
    flavor: '${input.size}'
    image: ubuntu
    count: '${input.count}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    storage:
      disks:
        - capacityGb: '${input.archiveDiskSize}'
          name: ArchiveDisk
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
    packages:
      - apache2
      - php
      - php-mysql
      - libapache2-mod-php
```

On the right, the 'Properties' tab is active, showing a form with the following fields and values:

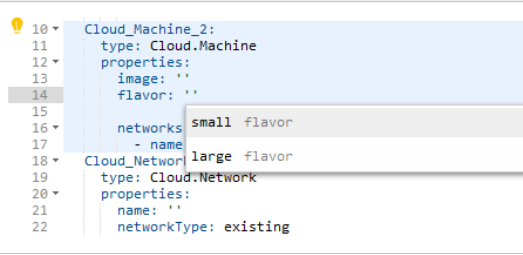
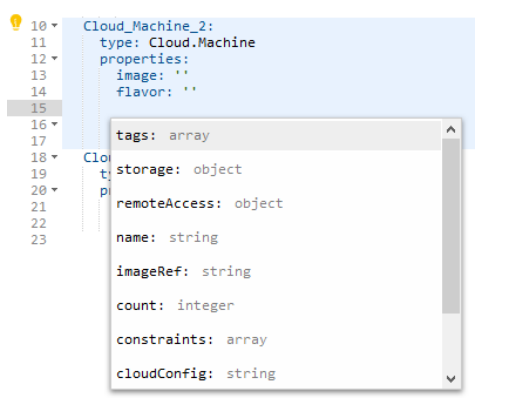
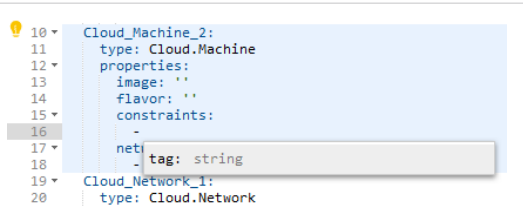
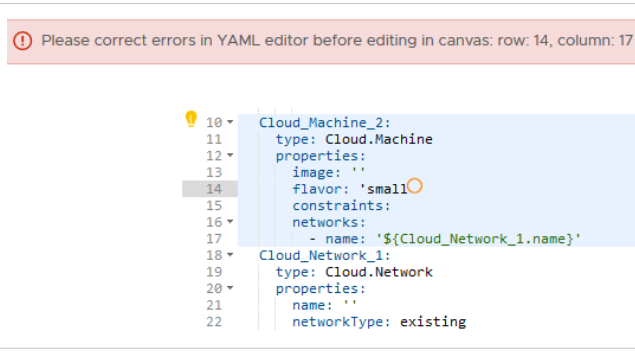
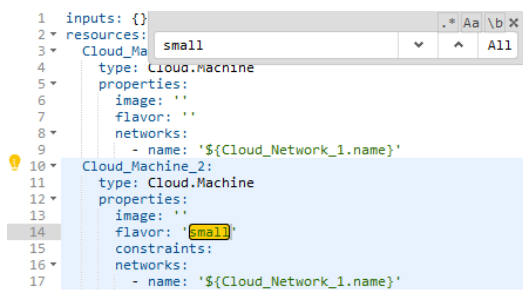
- Count:** "\${input.count}"
- Image Type:** ubuntu
- Flavor *:** \${input.size}
- Storage:** (empty)
- Constraints:** (empty)
- Tag:** (empty)
- Maximum Capacity of the disk in GB:** 1
- Size of boot disk in GB:** 1
- Networks:** (empty)

Observe que você pode copiar e colar o código de um modelo de nuvem para outro.

Obtendo ajuda para complementação de código no Cloud Assembly

Adicionar recursos do Cloud Assembly e conectá-los na tela, cria somente o código inicial. Para configurá-los totalmente, edite o código.

O editor de código permite digitar o código diretamente ou inserir valores de propriedade em um formulário. Para ajudar na criação do código direto, o editor do Cloud Assembly inclui recursos de preenchimento de sintaxe e verificação de erros.

| Dicas do editor | Exemplo |
|-------------------------|---|
| Valores disponíveis |  |
| Propriedades permitidas |  |
| Propriedades herdadas |  |
| Erros de sintaxe |  |
| Ctrl + F para Pesquisar |  |

| Dicas do editor | Exemplo |
|---|--|
| <p>Parâmetros opcionais</p> <div> <p>Insert optional parameters</p> <ul style="list-style-type: none"> + name + tags + storage + imageName </div> | <pre> 1 inputs: {} 2 resources: 3 Cloud_Machine_1: 4 type: Cloud.Machine 5 properties: 6 image: '' 7 flavor: '' 8 networks: 9 - name: '\${Cloud_Network_1.name}' 10 Cloud_Machine_2: 11 type: Cloud.Machine 12 properties: 13 image: '' 14 flavor: 'small' 15 constraints: 16 networks: 17 - name: '\${Cloud_Network_1.name}' </pre> |
| <p>Ajuda do esquema</p> | <p>Para todas as propriedades personalizadas, você também pode consultar o Esquema de tipos de recurso do vRealize Automation no VMware {code}.</p> <div> <div> <p>cloudConfig</p> <p>Type string</p> <p>When provisioning an instance, machine cloud-init startup instructions from user data fields. Sample cloud config instructions:</p> <pre> #cloud-config repo_update: true repo_upgrade: all packages: - httpd - db-server runcmd: - [sh, -c, "amazon-linux-extras insta - systemctl start httpd - sudo systemctl enable httpd </pre> </div> <div> <p>DBTier:</p> <pre> type: Cloud.Machine properties: name: mysql image: ubuntu-16 flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - name: '\${resource["WP-Network-Private - name: '\${WP-Network-Private.name}' remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#/#/' -i - service mysql restart - mysql -e "GRANT ALL PRIVILEGES ON *. - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] bTier: type: Cloud.Machine </pre> </div> </div> |

Criando associações e dependências entre recursos no Cloud Assembly

Quando você implanta um modelo do Cloud Assembly, um recurso pode precisar que outro componente esteja disponível primeiro.

Importante Setas indicam apenas uma dependência, e não uma conexão. Para conectar recursos de forma que eles se comuniquem, consulte [Primeiros passos com designs do Cloud Assembly](#).

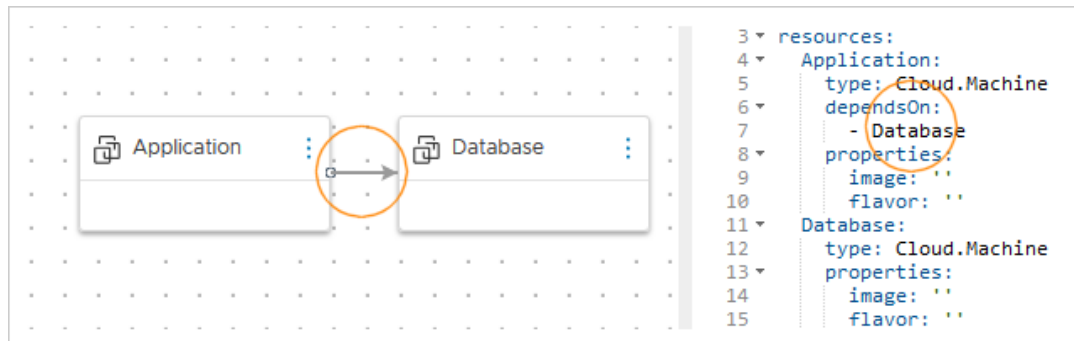
Dependências explícitas

Às vezes, um recurso precisa que outro seja implantado primeiro. Por exemplo, pode ser necessário que um servidor do database exista primeiro, antes que um servidor de aplicativos possa ser criado e configurado para acessá-lo.

Uma dependência explícita define a ordem de compilação no momento da implantação ou para ações de dimensionamento vertical/horizontal. É possível adicionar uma dependência explícita usando a tela de criação gráfica ou o editor de códigos.

- Opção tela de design — desenha uma conexão, iniciando no recurso dependente e terminando no recurso a ser implantado primeiro.
- Opção editor de códigos — adiciona uma propriedade `dependsOn` ao recurso dependente e identifica o recurso a ser implantado primeiro.

Uma dependência explícita cria uma seta sólida na tela.



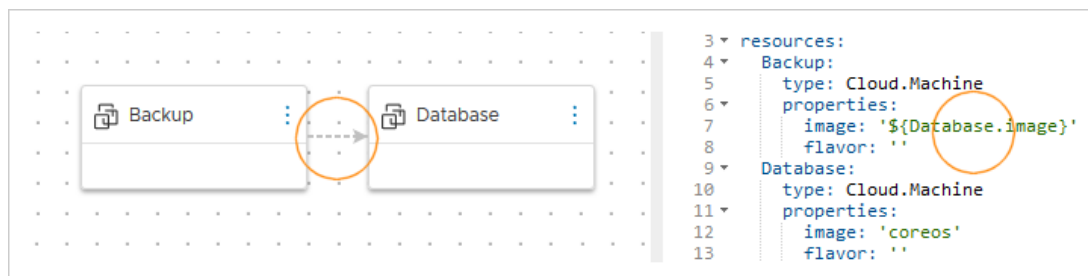
Associações de propriedades

Às vezes, uma propriedade de recurso precisa de um valor encontrado em uma propriedade de outro recurso. Por exemplo, um servidor de backup pode precisar da imagem do sistema operacional do servidor do database que está sendo copiado como backup, então o servidor do database deve existir primeiro.

Também chamada de dependência implícita, uma associação de propriedade controla a ordem de compilação, aguardando até que a propriedade necessária esteja disponível antes da implantação do recurso dependente. Você adiciona uma associação de propriedade usando o editor de código.

- Edite o recurso dependente, adicionando uma propriedade que identifica o recurso e a propriedade que devem existir primeiro.

Uma associação de propriedade cria uma seta tracejada na tela.



Controlando a versão dos seus modelos do Cloud Assembly

Como desenvolvedor de modelo de nuvem, você pode capturar com segurança um snapshot de um design de trabalho antes de arriscar outras alterações.

No momento da implantação, é possível selecionar qualquer uma das suas versões para implantar.

Capturando uma versão do modelo de nuvem

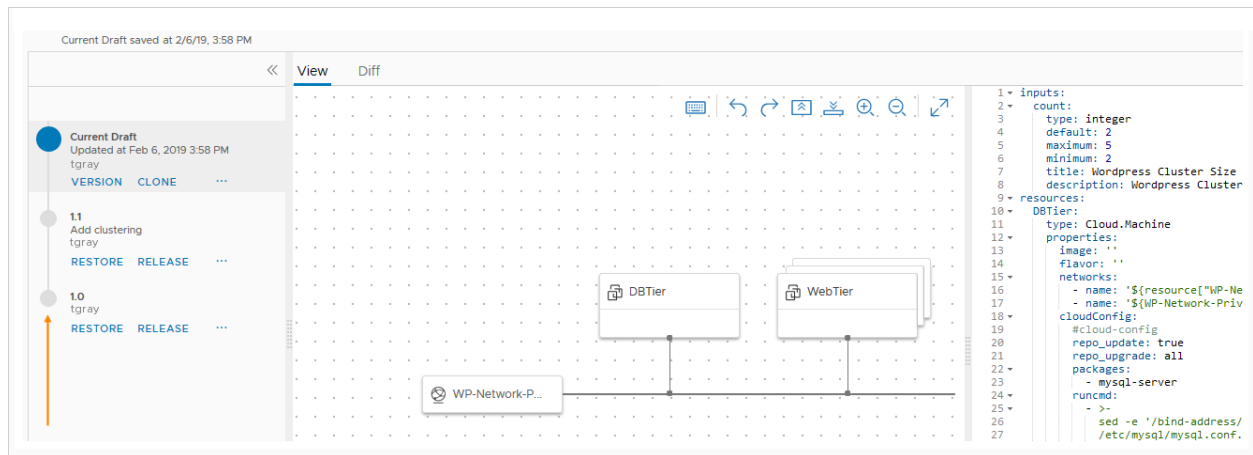
Na página de projeto, clique em **Versão** e forneça um nome.

O nome deve ser alfanumérico, sem espaços e somente pontos, hifens e sublinhados permitidos como caracteres especiais.

Restaurando uma versão mais antiga

Na página de projeto, clique em **Histórico da Versão**.

À esquerda, selecione uma versão mais antiga para inspecioná-la na tela e no editor de código. Quando encontrar a versão desejada, clique em **Restaurar**. A restauração substitui o rascunho atual sem remover quaisquer versões nomeadas.



Lançando uma versão no Service Broker

Na página de projeto, clique em **Histórico da Versão**.

À esquerda, selecione uma versão e lance-a.

Você não poderá lançar um Rascunho Atual até que o transforme em versão.

Reimportando a versão no Service Broker

Para habilitar a nova versão para os usuários do catálogo, reimporte-a.

No Service Broker, acesse **Conteúdo e Políticas > Fontes de Conteúdo**.

Na lista de origens, clique na origem do projeto que contém o modelo de nuvem com a versão recém-lançada.

Clique em **Salvar e Importar**.

Comparando versões de modelos de nuvem

Quando as alterações e as versões são acumuladas, pode ser desejável identificar as diferenças entre elas.

No Cloud Assembly, na exibição Histórico de Versões, selecione uma versão e clique em **Comparar**. Em seguida, no menu suspenso **Comparar com**, selecione outra versão para comparar.

Observe que é possível alternar entre revisar diferenças de código ou diferenças de topologia visual.

Figura 6-1. Diferenças de código

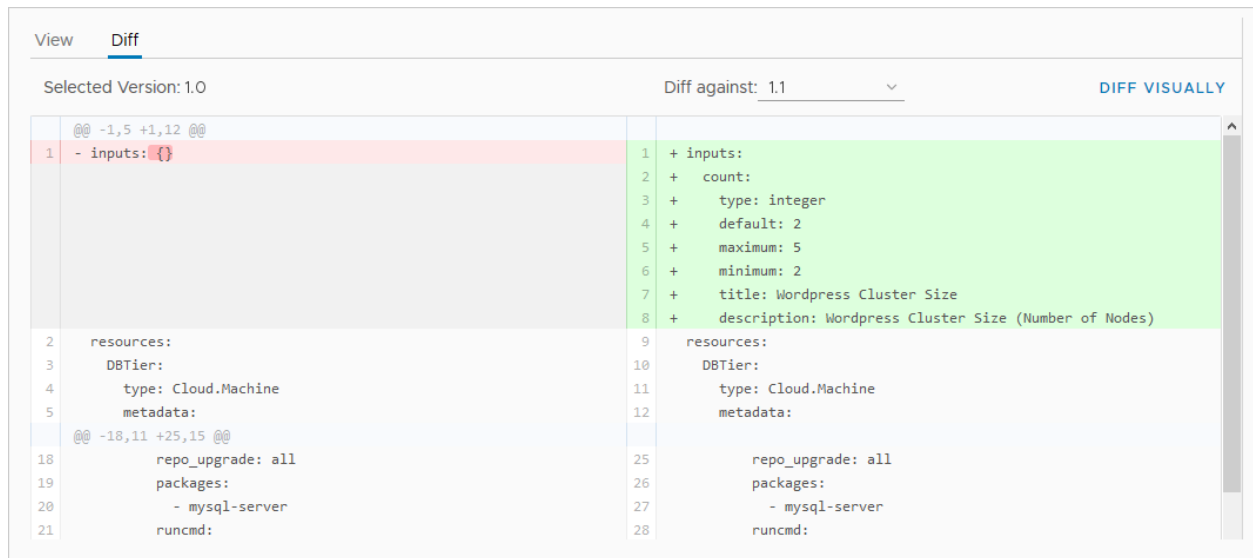
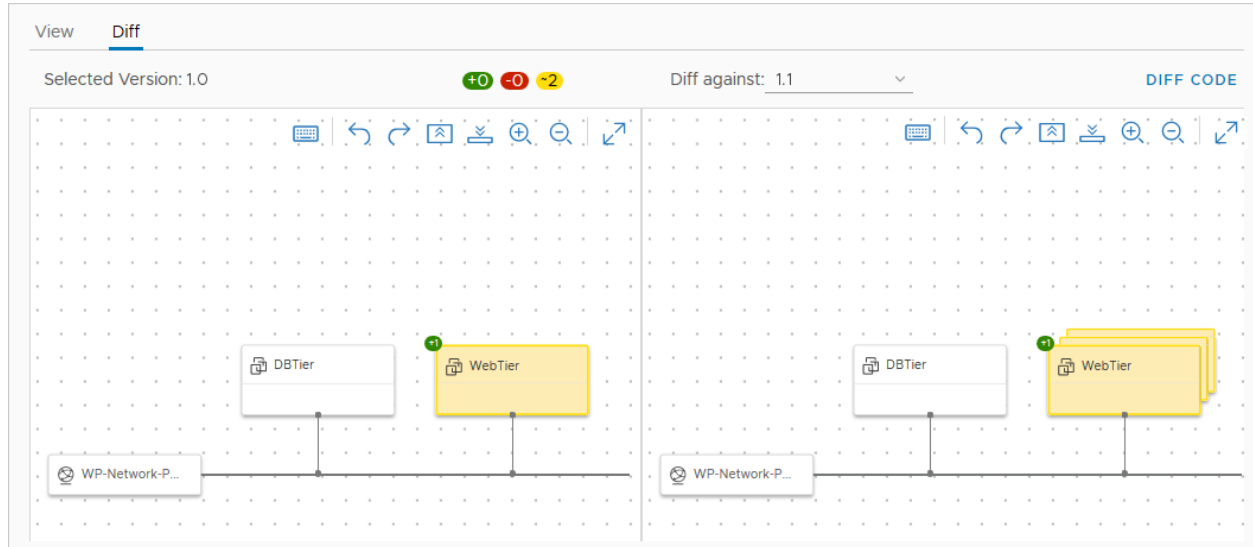


Figura 6-2. Diferenças na topologia visual



Clonando um modelo de nuvem

Embora não seja o mesmo que salvar uma versão, na página de projeto, **Ações > Clonar** faz uma cópia do modelo atual para desenvolvimento alternativo.

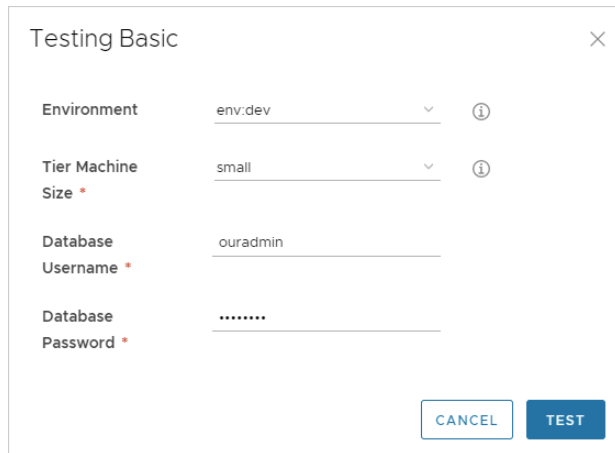
Entrada do usuário em solicitações do vRealize Automation

Como desenvolvedor de design de modelo de nuvem, você usa parâmetros de entrada para que os usuários possam fazer seleções personalizadas no momento da solicitação.

Como as entradas funcionam

Quando os usuários fornecem entradas, não é mais necessário salvar várias cópias dos modelos que são apenas um pouco diferentes. Além disso, as entradas podem preparar um modelo para operações de dia 2. Consulte [Como usar entradas de modelo de nuvem para atualizações de dia 2 do vRealize Automation](#).

As seguintes entradas mostram como criar um modelo de nuvem para um servidor de banco de dados MySQL, em que os usuários podem implantar esse modelo em diferentes ambientes de recursos de nuvem e aplicar diferentes recursos e credenciais todas as vezes.



The image shows a 'Testing Basic' dialog box with a close button (X) in the top right corner. It contains four input fields: 'Environment' with a dropdown menu showing 'env:dev' and an information icon; 'Tier Machine Size' with a dropdown menu showing 'small' and an information icon; 'Database Username' with a text input field containing 'ouradmin'; and 'Database Password' with a masked text input field showing '.....'. At the bottom right, there are two buttons: 'CANCEL' and 'TEST'.

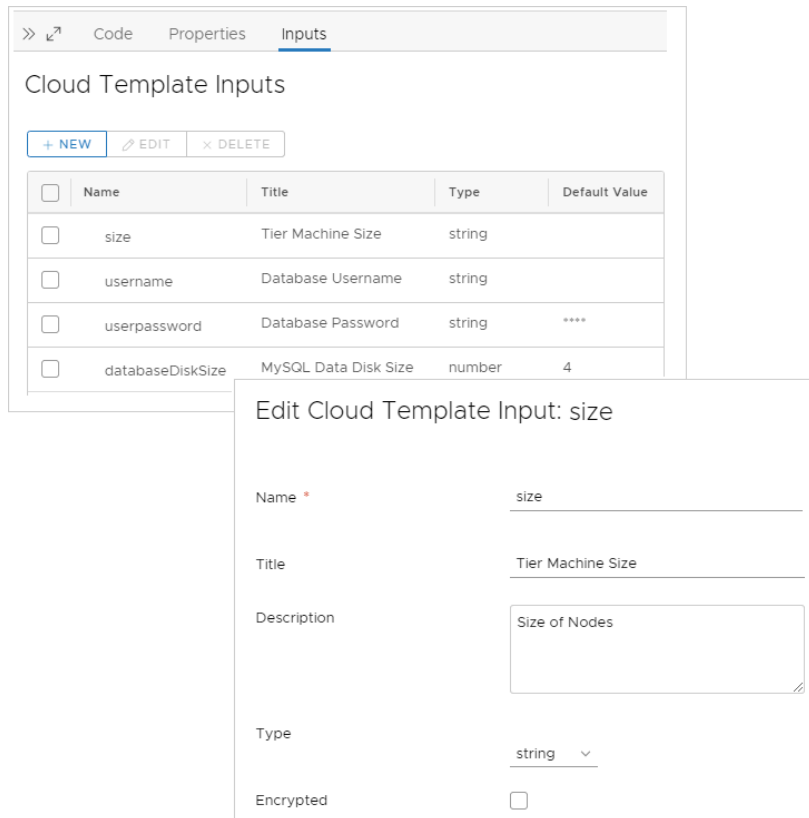
Adicionando parâmetros de entrada

Adicione uma seção `inputs` ao seu código de modelo, onde são definidos valores selecionáveis.

No exemplo a seguir, o tamanho da máquina, o sistema operacional e o número de servidores agrupados em cluster são selecionáveis.

```
inputs:
  wp-size:
    type: string
    enum:
      - small
      - medium
    description: Size of Nodes
    title: Node Size
  wp-image:
    type: string
    enum:
      - coreos
      - ubuntu
    title: Select Image/OS
  wp-count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: Wordpress Cluster Size
    description: Wordpress Cluster Size (Number of nodes)
```

Se você não se sentir à vontade ao editar o código, poderá clicar na guia **Entradas** do editor de código e inserir as configurações lá. O exemplo a seguir mostra algumas entradas para o banco de dados MySQL mencionado anteriormente.



Fazendo referência a parâmetros de entrada

Em seguida, na seção `resources`, referencie um parâmetro de entrada usando a sintaxe `${input.propriedade-nome}`.

Se um nome de propriedade incluir um espaço, delimite-o com colchetes e aspas duplas em vez de usar a notação de ponto: `${input["nome da propriedade"]}`

Importante No código do modelo de nuvem, não é possível usar a palavra `input`, exceto para indicar um parâmetro de entrada.

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

Entradas opcionais

As entradas são normalmente obrigatórias e marcadas com um asterisco. Para tornar uma entrada opcional, defina um valor padrão vazio, conforme mostrado.

```
owner:
  type: string
  minLength: 0
  maxLength: 30
  title: Owner Name
  description: Account Owner
  default: ''
```

Lista de propriedades de entrada

| Propriedade | Descrição |
|-------------|---|
| const | Usado com oneOf. O valor real associado ao título amigável. |
| default | Valor pré-preenchido para a entrada. O padrão deve ser do tipo correto. Não digite uma palavra como padrão para um número inteiro. |
| description | Texto de ajuda do usuário para a entrada. |
| encrypted | Se você deseja criptografar a entrada que o usuário digita, verdadeiro ou falso. As senhas normalmente são criptografadas. Também é possível criar propriedades criptografadas que são reutilizáveis em vários modelos de nuvem. Consulte Propriedades secretas do Cloud Assembly . |

| Propriedade | Descrição |
|-------------|---|
| enum | <p>Um menu suspenso de valores permitidos.</p> <p>Use o exemplo a seguir como um guia de formatação.</p> <pre>enum: - value 1 - value 2</pre> |
| format | <p>Define o formato esperado para a entrada. Por exemplo, (25/04/19) suporta data e hora.</p> <p>Permite o uso do selecionador de data em formulários personalizados do Service Broker.</p> |
| items | Declara itens em uma matriz. Oferece suporte a número, inteiro, cadeia de caracteres, boolean ou objeto. |
| maxItems | Número máximo de itens selecionáveis em uma matriz. |
| maxLength | <p>Número máximo de caracteres permitido para uma cadeia de caracteres.</p> <p>Por exemplo, para limitar um campo a 25 caracteres, digite <code>maxLength: 25</code>.</p> |
| maximum | Maior valor permitido para um número ou inteiro. |
| minItems | Número mínimo de itens selecionáveis em uma matriz. |
| minLength | Número mínimo de caracteres permitido para uma cadeia de caracteres. |
| minimum | Menor valor permitido para um número ou inteiro. |
| oneOf | <p>Permite que o formulário de entrada do usuário exiba um nome amigável (título) para um valor menos amigável (const). Se definir um valor padrão, defina const, não o título.</p> <p>Válido para uso com tipos de cadeia de caracteres, inteiro e número.</p> |
| pattern | <p>Caracteres permitidos para entradas de cadeia de caracteres, na sintaxe de expressão regular.</p> <p>Por exemplo, <code>'[a-z]+'</code> ou <code>'[a-z0-9A-Z@#]+\$'</code>.</p> |
| properties | Declara a chave:bloco de propriedades de valor para objetos |
| readOnly | Usado para fornecer apenas um rótulo de formulário. |
| title | Usado com oneOf. O nome amigável para um valor const. O título aparece no formulário de entrada do usuário no momento da implantação. |

| Propriedade | Descrição |
|-------------|---|
| type | <p>Tipo de dados de número, inteiro, cadeia de caracteres, boolean ou objeto.</p> <hr/> <p>Importante Um tipo booleano adiciona uma caixa de seleção em branco ao formulário de solicitação. Deixar a caixa desmarcada não torna a entrada Falso.</p> <p>Para definir a entrada como Falso, os usuários devem marcar e limpar a caixa.</p> <hr/> |
| writeOnly | <p>Oculto os pressionamentos de teclas atrás de asteriscos no formulário. Não pode ser usado com enum. Aparece como um campo de senha em formulários personalizados do Service Broker.</p> <hr/> |

Exemplos adicionais

Cadeia de caracteres com enumeração

```
image:
  type: string
  title: Operating System
  description: The operating system version to use.
  enum:
    - ubuntu 16.04
    - ubuntu 18.04
  default: ubuntu 16.04

shell:
  type: string
  title: Default shell
  description: The default shell that will be configured for the created user.
  enum:
    - /bin/bash
    - /bin/sh
```

Inteiro com mínimo e máximo

```
count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1
```

Matriz de objetos

```
tags:
  type: array
  title: Tags
  description: Tags that you want applied to the machines.
  items:
```

```

type: object
properties:
  key:
    type: string
    title: Key
  value:
    type: string
    title: Value

```

Cadeia de caracteres com nomes amigáveis

```

platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws

```

Cadeia de caracteres com validação de padrão

```

username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$

```

Cadeia de caracteres como senha

```

password:
  type: string
  title: Password
  description: The initial password that will be required to logon to the machine.
  Configured to reset on first login.
  encrypted: true
  writeOnly: true

```

Cadeia de caracteres como área de texto

```

ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256

```


Boolean

```
public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false
```

Seletor de calendário de data e hora

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

Ações do vRealize Orchestrator como entradas

Em um modelo do Cloud Assembly, as ações do vRealize Orchestrator podem ser incluídas como entradas de modelo de nuvem.

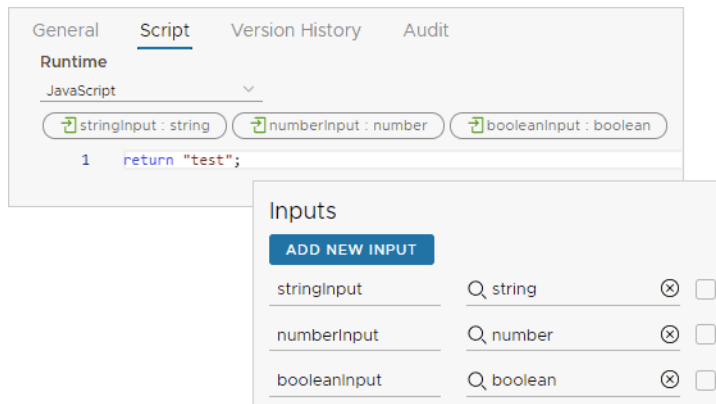
Adicionando uma ação do vRealize Orchestrator a entradas de modelo de nuvem

Para usar ações do vRealize Orchestrator como entradas de modelo de nuvem, siga estas diretrizes.

- 1 Na instância do vRealize Orchestrator incorporada ao vRealize Automation, crie uma ação que faça o que você deseja.

A ação do vRealize Orchestrator só deve incluir os tipos primitivos de cadeia de caracteres, inteiro, número e booleano. Não há suporte para tipos do vRealize Orchestrator.

Neste exemplo simples, a ação do vRealize Orchestrator coleta três entradas e retorna uma cadeia de caracteres embutida em código.



- 2 No Cloud Assembly, crie ou edite um modelo de nuvem.
- 3 No editor de código, clique na guia **Entradas** e em **Nova Entrada de Modelo de Nuvem**.

- 4 Para adicionar as entradas de ação do vRealize Orchestrator, clique no tipo e clique em **Constante**.

Adicione separadamente cada entrada de ação do vRealize Orchestrator como uma nova entrada de modelo de nuvem.

The screenshot shows the 'New Cloud Template Input' form. The 'Name' field is 'numberInput' and the 'Display Name' is 'Number for VRO'. The 'Type' dropdown is set to 'NUMBER'. The 'Default value source' is set to 'Constant'. The 'Default value' field is empty. Orange arrows point to the 'NUMBER' type button and the 'Constant' radio button.

- 5 Depois de adicionar as entradas de ação, crie outra entrada de modelo de nuvem, clique no tipo, clique em **Origem externa** e depois clique em **Selecionar**.

The screenshot shows the 'New Cloud Template Input' form. The 'Name' field is 'vroAction' and the 'Display Name' is 'VRO Action'. The 'Type' dropdown is set to 'STRING'. The 'Default value source' is set to 'External source'. The 'Action' field is 'Add an existing action' with a 'SELECT' button below it. Orange arrows point to the 'STRING' type button, the 'External source' radio button, and the 'SELECT' button.

- 6 Em **Ação**, procure e selecione a ação do vRealize Orchestrator que você criou e clique em **Salvar**.

Ao implantar o modelo de nuvem, as configurações da ação do vRealize Orchestrator aparecem no formulário de entrada para o usuário solicitante.

Padrões configuráveis

Para preencher o formulário de entrada com valores padrão, siga um destes procedimentos ao adicionar a ação do vRealize Orchestrator como a origem externa.

- Forneça manualmente o valor de propriedade padrão.

Desmarque a opção **Associar** e insira o valor.

Add an existing action

Action *

Action Parameters

Input ☐ Bind

- Use outro valor de propriedade das entradas que já estão no modelo de nuvem. Selecione a opção **Associar** e escolha uma propriedade na lista suspensa.

Add an existing action

Action *

Action Parameters

Input ☒ Bind

Canvas fields

Hard String

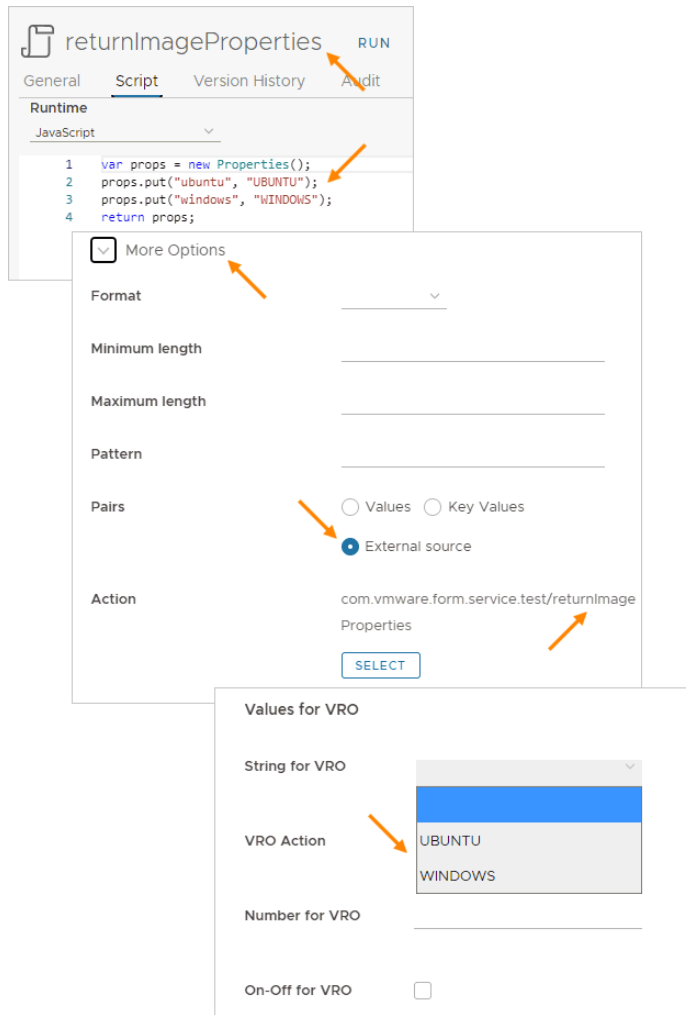
Input String

Adicionando seleções de entrada enumeradas do vRealize Orchestrator

Para criar uma lista de seleção do vRealize Orchestrator baseada em um formulário de entrada, faça o seguinte ao adicionar às entradas de modelo de nuvem.

- 1 No vRealize Orchestrator, crie uma ação que mapeie os valores desejados para a lista.
- 2 No Cloud Assembly, ao adicionar a entrada de modelo de nuvem, expanda **Mais Opções**.
- 3 Para **Pares**, clique em **Origem externa**, clique em **Selecionar** e adicione a ação do vRealize Orchestrator que você criou.

Observação Se você também criar um valor padrão ao adicionar a propriedade, esse padrão deverá corresponder exatamente a um dos valores enumerados da ação do vRealize Orchestrator.



Reutilizando um grupo de propriedades no Cloud Assembly

Quando você tiver propriedades do Cloud Assembly que sempre aparecem juntas, poderá montá-las em um grupo de propriedades.

Você pode adicionar rapidamente um grupo de propriedades a designs diferentes do Cloud Assembly, o que economiza o tempo ao adicionar as mesmas propriedades uma a uma. Além disso, você tem um único local para manter ou modificar o conjunto de propriedades, o que garante a sua aplicação consistente.

Somente usuários com a função de Administrador do Cloud Assembly podem criar, atualizar ou excluir um grupo de propriedades. O administrador pode compartilhar um grupo de propriedades com uma organização inteira ou limitar seu uso apenas dentro de um projeto.

Cuidado Um grupo de propriedades pode ser incluído em muitos modelos de nuvem, incluindo aqueles já lançados no catálogo. Alterações em um grupo de propriedades podem afetar outros usuários.

Há dois tipos de grupos de propriedades.

- **Grupos de propriedades de entrada no Cloud Assembly**

Os grupos de propriedades de entrada coletam e aplicam um conjunto de propriedades consistente no momento da solicitação do usuário. Os grupos de propriedades de entrada podem incluir entradas para o usuário adicionar ou selecionar, ou podem incluir valores de somente leitura que são necessários para o design.

As propriedades para o usuário editar ou selecionar podem ser lidas ou criptografadas. As propriedades somente leitura aparecem no formulário de solicitação, mas não podem ser editadas. Se você quiser que os valores de somente leitura permaneçam ocultos, use um grupo de propriedades constantes.

- **Grupos de propriedades constantes no Cloud Assembly**

Os grupos de propriedades constantes aplicam silenciosamente as propriedades conhecidas. Com efeito, os grupos de propriedades constantes são metadados invisíveis. Eles fornecem valores aos seus designs do Cloud Assembly de uma forma que impede que um usuário solicitante leia esses valores ou até mesmo saiba que ele está presente. Exemplos podem incluir chaves de licença ou credenciais de conta de domínio.

Os dois tipos de grupo de propriedades são manipulados de forma muito diferente pelo Cloud Assembly. Ao criar um grupo de propriedades, você deverá primeiro selecionar se quer criar entradas ou constantes. Você não pode criar um grupo de propriedades mescladas nem converter um conjunto existente de propriedades e seu grupo de propriedades de um tipo para o outro.

Grupos de propriedades de entrada no Cloud Assembly

Grupos de propriedade de entrada do Cloud Assembly normalmente incluem configurações relacionadas para o usuário inserir ou selecionar. Eles também podem incluir valores somente leitura necessários para o design do modelo de nuvem.

Criando o grupo de propriedades de entrada

- 1 Acesse **Design > Grupos de Propriedades** e clique em **Novo Grupo de Propriedades**.
- 2 Selecione **Valores de Entrada**.
- 3 Nomeie e descreva o novo grupo de propriedades.

| | |
|------------------|--|
| Nome | Os nomes de grupos de propriedades devem ser exclusivos em uma determinada organização. Apenas letras, números e sublinhados são permitidos. |
| Nome de Exibição | Adicione um título para todo o grupo de propriedades, que aparece no formulário de solicitação. |
| Descrição | Explique para que serve esse conjunto de propriedades. |

| | |
|---------|---|
| Escopo | Decida se um administrador pode compartilhar o grupo de propriedades com toda a organização. Caso contrário, apenas um projeto pode acessar o grupo de propriedades. Embora você sempre possa adicionar ou modificar propriedades no grupo, o escopo será permanente e não poderá ser alterado posteriormente. |
| Projeto | Quando o escopo é somente projeto, esse projeto pode acessar o grupo de propriedades. |

4 Para adicionar uma propriedade ao grupo, clique em **Nova Propriedade**.

O painel para adicionar uma nova propriedade é muito semelhante à guia Entradas do editor de códigos da página de design do Cloud Assembly.

| | |
|------------------|--|
| Nome | Nome do formulário livre para a propriedade individual. Apenas letras, números e sublinhados são permitidos. |
| Nome de Exibição | Adicione um nome de propriedade individual a ser exibido no formulário de solicitação. |
| Tipo | Cadeia de caracteres, Inteiro, Número, Boolean (T/F), Objeto ou Matriz. |
| Valor Padrão | Entrada de valor predefinido que aparece no formulário de solicitação. "Para todos os tipos, exceto Boolean, a entrada do usuário é opcional por padrão." Para garantir que todas as entradas sejam relevantes, siga um destes procedimentos: <ul style="list-style-type: none"> ■ Defina um valor padrão. ■ Exija a entrada do usuário adicionando a seguinte propriedade de modelo de nuvem ao código concluído. <pre>populateRequiredOnNonDefaultProperties: true</pre> |
| Criptografado | Quando selecionado, oculta o valor ao inseri-lo no formulário de solicitação e na implantação subsequente. As propriedades criptografadas não podem ter um valor padrão. |
| Somente leitura | Um valor não editável, mas visível, no formulário de solicitação. Exige um padrão. |
| Mais Opções | Opções que variam de acordo com o tipo de propriedade. Expanda a lista suspensa, adicione quaisquer configurações adicionais e clique em Criar . |

No exemplo a seguir, a propriedade que está sendo adicionada representa a imagem do sistema operacional e o usuário solicitante pode selecionar entre duas.

Observação Os sistemas operacionais mostrados na figura de exemplo já devem fazer parte da infraestrutura configurada do Cloud Assembly.

New Property

Name * image

Display Name Machine Image

Description

Type

STRING **INTEGER** **NUMBER** **BOOLEAN** **OBJECT** **ARRAY**

Default value coreos

Encrypted ☐

Read-only ☐ ⓘ

∨ **More Options**

Format ∨

Minimum length

Maximum length

Pattern

Pairs ☒ Values ☐ Key Values

Enum

Value

coreos -

ubuntu - +

- 5 Adicione mais propriedades ao grupo e clique em **Salvar** ao terminar.

Properties

2 items

Add at least one property in order to create a property group

+ NEW PROPERTY x DELETE

| <input type="checkbox"/> | Name | Display Name | Type | Default Value |
|--------------------------|--------|----------------|--------|---------------|
| <input type="checkbox"/> | image | Machine Image | string | coreos |
| <input type="checkbox"/> | flavor | Machine Flavor | string | small |

Adicionando o grupo de propriedades às entradas do modelo de nuvem

Mesmo para uma lista longa de entradas de propriedades, você só precisa adicionar o grupo de propriedades para torná-las parte do formulário de solicitação.

- 1 Na página de projeto do modelo de nuvem, acima da área de edição à direita, clique na guia **Entradas**.
- 2 Clique em **Nova Entrada de Modelo de Nuvem**.
- 3 Nomeie e descreva o grupo de propriedades.

| | |
|---------------------------------|--|
| Nome | Insira algo semelhante ao nome do grupo de propriedades criado anteriormente. |
| Nome de Exibição | Insira o mesmo título criado anteriormente para todo o grupo de propriedades, que aparece no formulário de solicitação. |
| Tipo | Selecione Objeto . |
| Tipo de Objeto | Selecione Grupo de Propriedades . |
| Lista de grupos de propriedades | Selecione o grupo de propriedades que você deseja. São exibidos somente os grupos de propriedades que são criados e disponibilizados para o seu projeto. Observe que grupos de propriedades constantes não são exibidos. |

New Cloud Template Input [X]

Name *

Display Name

Description

Type

STRING INTEGER NUMBER BOOLEAN **OBJECT** ARRAY

Select Object Type ☐ Properties ☒ Property Groups

Select from the existing property groups

Q

| Name | Description |
|--|-------------|
| <input checked="" type="radio"/> machine | |

- 4 Clique em **Criar**.

O processo cria um código de entradas de modelo de nuvem semelhante ao exemplo a seguir.

```
inputs:
  pgmachine:
    type: object
    title: Machine Properties
    $ref: /ref/property-groups/machine
  pgrequester:
    type: object
    title: Requester Details
    $ref: /ref/property-groups/requesterDetails
```

Você também pode inserir o código diretamente na página de design do Cloud Assembly e aproveitar a solicitação automática à medida que digita `$ref: /ref/p...` no editor de códigos.

Vinculando recursos de modelo de nuvem ao grupo de propriedades

Para usar os valores de entrada do grupo de propriedades, adicione vinculações sob o recurso.

Dependendo dos tipos de valores que estão em um grupo de propriedades, você pode querer fazer referência a eles individualmente. Você pode inseri-los separadamente, por nome do grupo de propriedades e nome da propriedade.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: '${input.pgmachine.image}'
      flavor: '${input.pgmachine.flavor}'
```

Você também pode adicionar rapidamente um conjunto inteiro de valores a um recurso referenciando um grupo inteiro de propriedades.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      requester: '${input.pgrequester}'
```

Código concluído

Quando você terminar de inserir as entradas e os recursos, o código finalizado parecerá semelhante ao exemplo a seguir.

```

>> Code Properties Inputs
1 formatVersion: 1
2 inputs:
3   pgmachine:
4     type: object
5     title: Machine Properties
6     $ref: /ref/property-groups/machine
7   pgrequester:
8     type: object
9     title: Requester Details
10    $ref: /ref/property-groups/requesterDetails
11  count:
12    type: integer
13    title: 'Machine Count'
14  resources:
15    Cloud_Machine_1:
16      type: Cloud.Machine
17      properties:
18        image: '${input.pgmachine.image}'
19        flavor: '${input.pgmachine.flavor}'
20        count: '${input.count}'
21        requester: '${input.pgrequester}'
22

```

Mediante solicitação de implantação, seus grupos de propriedades aparecem para que o usuário solicitante seja concluído.

Deployment Inputs

Machine Properties

Machine Image
Machine Flavor

Requester Details

Email
Mobile
Internal account? ☐
PIN
Account Type
Machine Count *

Grupos de propriedades no editor de formulário personalizado do Service Broker

Os grupos de propriedades de entrada aparecem na interface do formulário personalizado do Service Broker e estão disponíveis para personalização lá. Não há considerações especiais exclusivas para os grupos de propriedades ao personalizá-los. Os usuários do Service Broker nem mesmo precisam saber que a origem das entradas é um grupo de propriedades em vez de propriedades criadas separadamente.

The screenshot shows a form editor interface for a Service Broker. At the top, there is a 'General' tab and an 'ADD TAB' button. The form is set against a grid background. Two groups of properties are highlighted with dashed orange boxes:

- Machine Properties Group:** This group contains three properties:
 - Project:** A text input field with a dropdown arrow on the right.
 - Deployment Name:** A text input field.
 - Machine Count:** A text input field.
- Requester Details Group:** This group contains five properties:
 - Machine Image:** A text input field with a dropdown arrow on the right.
 - Machine Flavor:** A text input field with a dropdown arrow on the right.
 - Requester Details:** A section header for the following properties.
 - Email:** A text input field.
 - Mobile:** A text input field.
 - Internal account?:** A checkbox.
 - PIN:** A text input field.
 - Account Type:** A text input field.

Consulte [Personalizar um ícone e um formulário de solicitação do Service Broker](#) para obter mais informações.

Ações do vRealize Orchestrator em um grupo de propriedades de entrada

Em um grupo de propriedade de entrada do Cloud Assembly, você pode adicionar uma interação dinâmica com o vRealize Orchestrator.

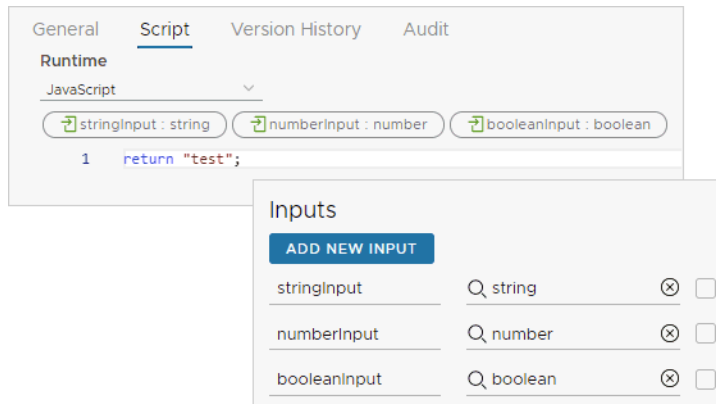
Adicionando uma ação do vRealize Orchestrator a um grupo de propriedades de entrada

Para adicionar interação dinâmica com o vRealize Orchestrator a um grupo de propriedades de entrada, siga estas diretrizes.

- 1 Na instância do vRealize Orchestrator incorporada ao vRealize Automation, crie uma ação que faça o que você deseja.

A ação do vRealize Orchestrator só deve incluir os tipos primitivos de cadeia de caracteres, inteiro, número e booleano. Não há suporte para tipos do vRealize Orchestrator.

Neste exemplo simples, a ação do vRealize Orchestrator coleta três entradas e retorna uma cadeia de caracteres embutida em código.



- 2 No do Cloud Assembly, inicie o processo de criação ou edição de um grupo de propriedades de entrada. Consulte [Grupos de propriedades de entrada no Cloud Assembly](#) se necessário.
- 3 Para adicionar as entradas de ação do vRealize Orchestrator a um grupo de propriedades, adicione novas propriedades, clique no tipo e clique em **Constante**.

Adicione separadamente cada entrada de ação do vRealize Orchestrator.

New Property

Name *

Display Name

Description

Type

STRING INTEGER **NUMBER** BOOLEAN OBJECT ARRAY

Default value source ☒ Constant ☐ External source

Default value

- Depois de adicionar as entradas, adicione uma nova propriedade, clique no tipo, clique em **Origem externa** e depois em **Selecionar**.

New Property

Name *

Display Name

Description

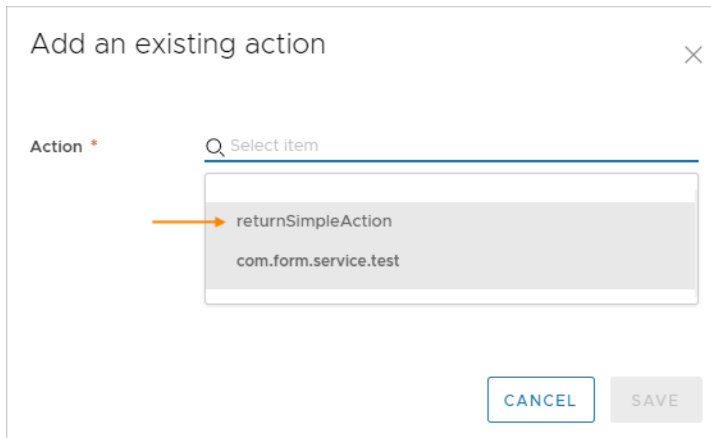
Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value source ☐ Constant ☒ External source

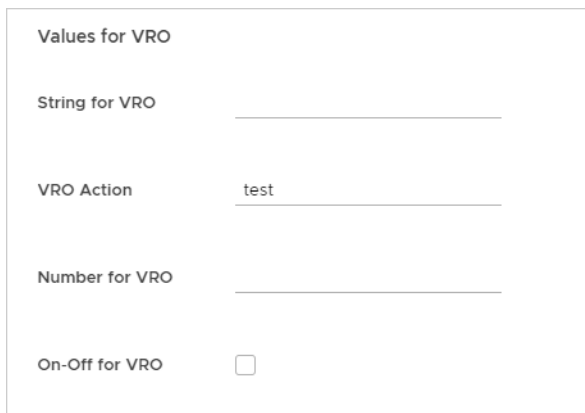
Action

- Em **Ação**, procure e selecione a ação do vRealize Orchestrator que você criou e clique em **Salvar**.



- 6 Salve o grupo de propriedades e adicione-o ao seu modelo de nuvem. Consulte [Grupos de propriedades de entrada no Cloud Assembly](#) se necessário.

Ao implantar o modelo de nuvem, o grupo de propriedades da ação do vRealize Orchestrator aparece no formulário de entrada do usuário solicitante.

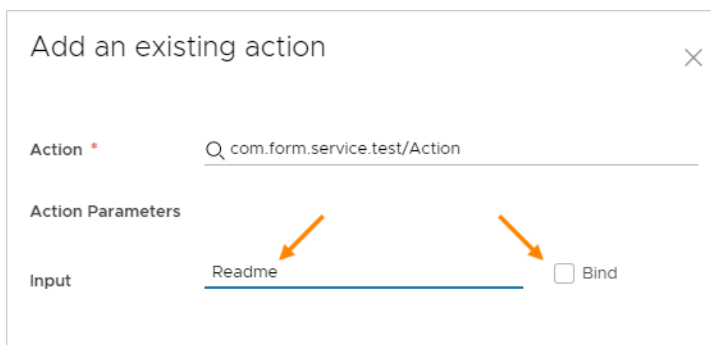


Padrões configuráveis

Para preencher o formulário de entrada com valores padrão, siga um destes procedimentos ao adicionar a ação do vRealize Orchestrator como a origem externa.

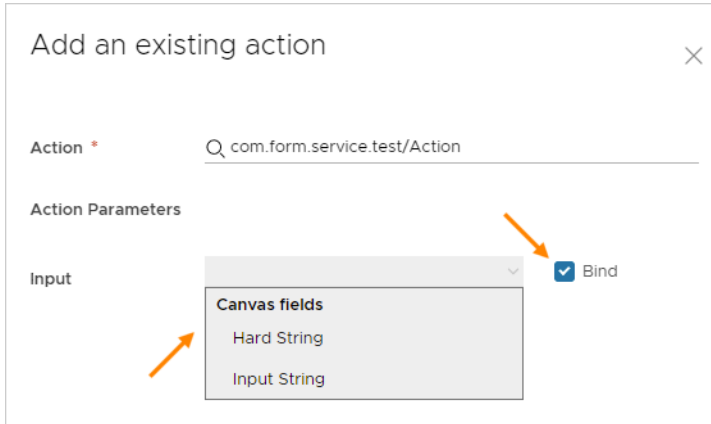
- Forneça manualmente o valor de propriedade padrão.

Desmarque a opção **Associar** e insira o valor.



- Use outro valor de propriedade do mesmo grupo de propriedades.

Selecione a opção **Associar** e escolha uma propriedade na lista suspensa.

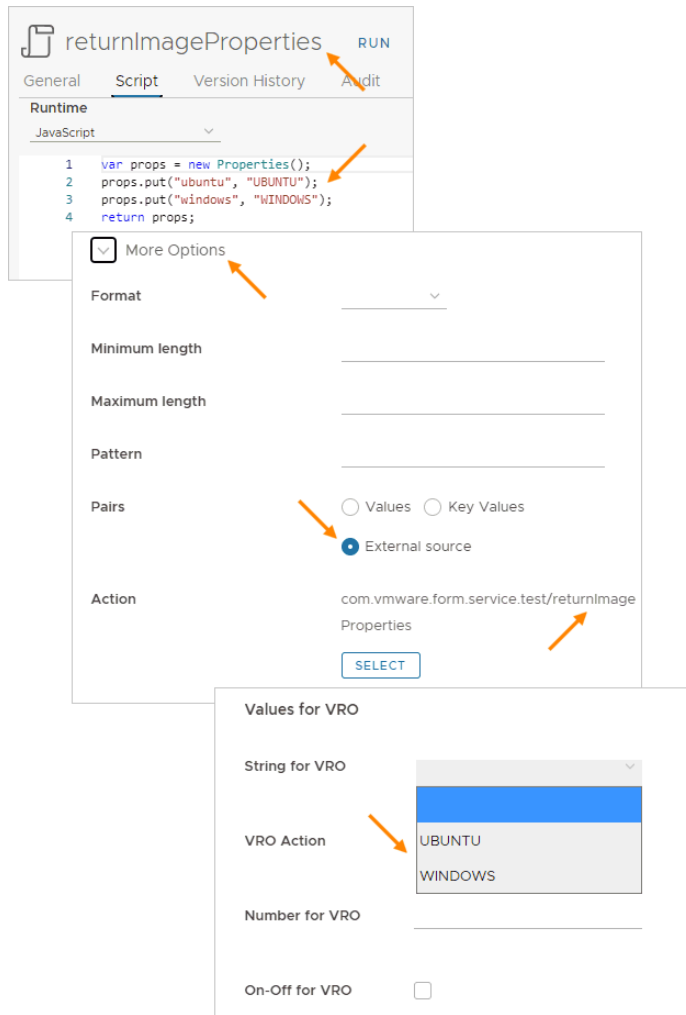


Adicionando seleções de entrada enumeradas do vRealize Orchestrator

Para criar uma lista de seleção do vRealize Orchestrator baseada em um formulário de entrada, faça o seguinte ao adicionar a um grupo de propriedades.

- 1 No vRealize Orchestrator, crie uma ação que mapeie os valores desejados para a lista.
- 2 No Cloud Assembly, ao adicionar uma propriedade ao grupo, expanda **Mais Opções**.
- 3 Para **Pares**, clique em **Origem externa**, clique em **Selecionar** e adicione a ação do vRealize Orchestrator que você criou.

Observação Se você também criar um valor padrão ao adicionar a propriedade, esse padrão deverá corresponder exatamente a um dos valores enumerados da ação do vRealize Orchestrator.



Grupos de propriedades constantes no Cloud Assembly

As constantes do Cloud Assembly permitem que você aplique silenciosamente pares de chave-valor conhecidos aos seus designs.

Como funcionam as constantes

A chave aparece no código do modelo de nuvem, e o valor se torna parte de implantações baseadas nesse modelo de nuvem. Constantes exigem a vinculação do `propgroup` sob o recurso.

A vinculação do `propgroup` é usada apenas com grupos de propriedades constantes, não grupos de propriedades de entrada.

Propriedades secretas

Se você espera adicionar uma propriedade secreta a um grupo de propriedades, crie-a antes de prosseguir. Consulte [Propriedades secretas do Cloud Assembly](#).

Criando o grupo de propriedades constantes

- 1 Acesse **Design > Grupos de Propriedades** e clique em **Novo Grupo de Propriedades**.

2 Selecione **Valores Constantes**.

3 Nomeie e descreva o novo grupo de propriedades.

| | |
|------------------|--|
| Nome | Os nomes de grupos de propriedades devem ser exclusivos em uma determinada organização. Apenas letras, números e sublinhados são permitidos. |
| Nome de Exibição | Deixe em branco. Nenhum título aparece no formulário de solicitação. |
| Descrição | Explique para que serve esse conjunto de constantes. |
| Escopo | <p>Decida se um administrador pode compartilhar o grupo de propriedades com toda a organização. Caso contrário, apenas um projeto pode acessar o grupo de propriedades.</p> <p>Embora você sempre possa adicionar ou modificar propriedades no grupo, o escopo será permanente e não poderá ser alterado posteriormente.</p> <p>Segredos: se você espera adicionar uma propriedade secreta ao grupo de propriedades, deve usar o escopo de projeto único. Propriedades secretas são salvas apenas no nível do projeto.</p> |
| Projeto | Quando o escopo é somente projeto, esse projeto pode acessar o grupo de propriedades. |

4 Para adicionar uma propriedade constante ao grupo, clique em **Nova Propriedade**.

5 Insira um nome que atua como a chave e uma descrição.

6 Selecione um tipo de propriedade.

7 Insira o valor da constante desejado e clique em **Criar**.

- Tipos de cadeia de caracteres, inteiro e número usam entrada direta.
- Para um valor de cadeia de caracteres secreto, selecione na lista de propriedades secretas do projeto.
- O tipo booleano usa uma caixa de seleção para indicar "true".
- Para o tipo de objeto ou matriz, substitua `null` pelo valor desejado.

New Property

Name *

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Select Type ☒ Constant value ☐ Secret

Constant value

New Property [X]

Name *

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Select Type ☐ Constant value ☒ Secret

Q Search

| | Name | Description |
|----------------------------------|------------------|-------------|
| <input checked="" type="radio"/> | AccountNumber | |
| <input type="radio"/> | password | |
| <input type="radio"/> | RemoteAccessKey1 | |

7 secrets

8 Adicione mais constantes ao grupo e clique em **Salvar** ao terminar.

Properties 3 items

Add at least one property in order to create a property group

[+ NEW PROPERTY](#) [X DELETE](#)

| <input type="checkbox"/> | Name | Display Name | Type | Constant Value |
|--------------------------|--------------------|--------------|---------|----------------|
| <input type="checkbox"/> | payerFederal | | boolean | true |
| <input type="checkbox"/> | payerCostCenter | | integer | 7890 |
| <input type="checkbox"/> | payerAccountNumber | | string | 123456 |

Vinculando recursos de modelo de nuvem ao grupo de propriedades

Para usar silenciosamente valores constantes em um recurso, adicione vinculações do `proppgroup` sob o recurso.

Você pode adicionar rapidamente um conjunto de constantes inteiro a um recurso, referenciando o próprio grupo de propriedades.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerInfo: '${proppgroup.payerDetails}'
```

Como alternativa, você pode adicionar constantes individuais do grupo de propriedades às partes selecionadas do seu design.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerAccount: '${propgroup.payerDetails.payerAccountNumber}'
      payerCost: '${propgroup.payerDetails.payerCostCenter}'
      payerFed: '${propgroup.payerDetails.payerFederal}'
```

Saiba mais sobre grupos de propriedades do Cloud Assembly

Um grupo de propriedades do Cloud Assembly pode ser incluído em muitos modelos de nuvem, o que afeta como você precisa gerenciar grupos de propriedades.

Modificando um grupo de propriedades

As alterações em um grupo de propriedades do Cloud Assembly afetam cada modelo de nuvem que o utiliza. Além disso, quando a versão alterada do modelo de nuvem é lançada, essas alterações agora afetam os usuários do catálogo do Service Broker.

A lista de grupos de propriedades e as páginas de edição de grupos de propriedades mostram o número de modelos de nuvem que incluem o grupo de propriedades. Para ver qual modelo de nuvem será afetado por uma alteração, clique no número.

The screenshot displays the 'Property Groups' management interface. At the top, there's a header 'Property Groups' with a '61 items' badge and a filter icon. Below the header are buttons for '+ NEW PROPERTY GROUP' and 'x DELETE', along with a search bar labeled 'Filter...'. A table lists the property groups:

| | Name | Type | Properties | Cloud Templates | Last Updated |
|-----------------------|----------|----------|------------|-----------------|--------------------------|
| <input type="radio"/> | machine | Input | 2 | 2 ← | Apr 29, 2021, 4:26:18 PM |
| <input type="radio"/> | mh_const | Constant | 5 | 1 | Apr 27, 2021, 5:29:33 PM |

An orange arrow points from the '2' in the 'Cloud Templates' column of the 'machine' group to a modal window titled 'Cloud Templates'. This modal shows the 'Properties' section with a '2 items' badge and a message: 'Add at least one property in order to create a property group'. It includes buttons for '+ NEW PROPERTY' and 'x DELETE'. Below is a table of properties:

| <input type="checkbox"/> | Name | Display Name | Type | Default Value |
|--------------------------|--------|----------------|--------|---------------|
| <input type="checkbox"/> | image | Machine Image | string | coreos |
| <input type="checkbox"/> | flavor | Machine Flavor | string | small |

Antes de modificar um grupo de propriedades, certifique-se de que a alteração seja aceitável para todos que estão criando ou atualizando implantações com base nos modelos de nuvem listados.

Excluindo um grupo de propriedades

A exclusão de um grupo de propriedades causa erros em todos os modelos de nuvem que o utilizam.

Não é possível excluir um grupo de propriedades até que ele seja removido manualmente de todos os modelos de nuvem nos quais está incluído. Para remover um grupo de propriedades de um modelo de nuvem, abra esse modelo de nuvem na tela de design.

- Grupos de propriedades de entrada

Na guia Entradas, selecione e remova o grupo de propriedades. Como alternativa, use o editor de código para excluir o grupo de propriedades associado na seção `inputs` do código.

- Grupos de propriedades constantes

Use o editor de código para excluir uma ou mais entradas `propgroup` associadas na seção `resources` do código.

Observação Não será possível excluir um grupo de propriedades se ele estiver incluído em um modelo de nuvem com controle de versão. Modelos de nuvem com controle de versão são somente leitura.

Sinalizadores de recursos do Cloud Assembly para solicitações

O Cloud Assembly inclui várias configurações de modelo de nuvem que ajustam como um recurso é tratado no momento da solicitação.

As configurações de sinalizador de recurso não fazem parte do esquema de propriedades do objeto de recurso. Para um determinado recurso, você adiciona as configurações de sinalizador fora da seção de propriedades, conforme mostrado.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    preventDelete: true
    properties:
      image: coreos
      flavor: small
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 1
```

| Sinalizador de recurso | Descrição |
|------------------------|---|
| allocatePerInstance | <p>Quando definido como "true", a alocação de recursos pode ser personalizada para cada máquina em um cluster. Se você estiver usando a extensibilidade, "true" fará com que o tópico de evento de extensibilidade <code>compute.allocation.pre</code> seja executado várias vezes ao implantar mais de uma máquina de nuvem.</p> <p>O padrão é "false", que aloca recursos igualmente no cluster, resultando na mesma configuração para cada máquina. Além disso, ações de dia 2 podem não ser possíveis separadamente para recursos individuais.</p> <p>A alocação por instância permite que <code>count.index</code> aplique corretamente a configuração para máquinas individuais. Para exemplos de código, consulte Clusters de máquina e disco no Cloud Assembly.</p> |
| createBeforeDelete | <p>Algumas ações de atualização exigem que o recurso existente seja removido e um novo seja criado. Por padrão, a remoção é a primeira, que pode levar a condições em que o recurso antigo desapareceu, mas o novo não foi criado com êxito por algum motivo.</p> <p>Defina esse sinalizador como true se você precisar certificar-se de que o novo recurso foi criado com êxito antes de excluir o anterior.</p> |
| createTimeout | <p>O tempo limite padrão do Cloud Assembly para as solicitações de alocação de recursos, criação e planejamento é de 2 horas (2h). Além disso, um administrador de projeto pode definir um tempo limite padrão personalizado para essas solicitações, aplicável durante todo o projeto.</p> <p>Esse sinalizador permite que você substitua quaisquer padrões e defina o tempo limite individual para uma operação de recurso específica. Consulte também <code>updateTime</code> e <code>deleteTimeout</code>.</p> |
| deleteTimeout | <p>O tempo limite padrão do Cloud Assembly para solicitações de exclusão é de 2 horas (2h). Além disso, um administrador de projeto pode definir um tempo limite padrão diferente para solicitações de exclusão, aplicável durante todo o projeto.</p> <p>Esse sinalizador permite que você substitua quaisquer padrões e defina o tempo limite individual para uma operação de exclusão de recurso específica. Consulte também <code>updateTimeout</code> e <code>createTimeout</code>.</p> |
| dependsOn | <p>Esse sinalizador identifica uma dependência explícita entre os recursos, em que um recurso deve existir antes de criar o próximo. Para obter mais informações, consulte Criando associações e dependências entre recursos no Cloud Assembly.</p> |

| Sinalizador de recurso | Descrição |
|---|---|
| <code>dependsOnPreviousInstances</code> | <p>Quando definido como "true", cria recursos de cluster sequencialmente. O padrão é "false", o que cria simultaneamente todos os recursos em um cluster.</p> <p>Por exemplo, a criação sequencial é útil para clusters de banco de dados em que nós primários e secundários devem ser criados, mas a criação do nó secundário precisa de definições de configuração que conectam o nó a um nó primário existente.</p> |
| <code>forceRecreate</code> | <p>Nem todas as ações de atualização exigem que o recurso existente seja removido e um novo seja criado. Se você quiser uma atualização para remover o recurso antigo e criar um novo, independentemente de a atualização ter feito isso por padrão, defina esse sinalizador como true.</p> |
| <code>ignoreChanges</code> | <p>Os usuários de um recurso podem reconfigurá-lo, alterando o recurso do seu estado implantado.</p> <p>Se você deseja realizar uma atualização de implantação, mas não sobrescrever o recurso alterado com a configuração do modelo de nuvem, defina esse sinalizador como "true".</p> |
| <code>ignorePropertiesOnUpdate</code> | <p>Os usuários de um recurso podem personalizar determinadas propriedades, e essas propriedades podem ser redefinidas para o estado original do modelo de nuvem durante uma ação de atualização.</p> <p>Para impedir que todas as propriedades sejam redefinidas por uma ação de atualização, defina esse sinalizador como true.</p> |
| <code>preventDelete</code> | <p>Se você precisar proteger um recurso criado contra exclusão acidental durante as atualizações, defina este sinalizador como verdadeiro. No entanto, se um usuário excluir a implantação, o recurso será excluído.</p> |
| <code>recreatePropertiesOnUpdate</code> | <p>Os usuários de um recurso podem reconfigurar propriedades, alterando o recurso de seu estado implantado. Durante uma atualização, um recurso pode ou não ser recriado. Recursos que não são recriados podem permanecer com propriedades em estados alterados.</p> <p>Se você quiser que um recurso e suas propriedades sejam recriados, independentemente de a atualização ter feito isso por padrão, defina esse sinalizador como "true".</p> |
| <code>updateTimeout</code> | <p>O tempo limite padrão do Cloud Assembly para solicitações de atualização é de 2 horas (2h). Além disso, um administrador de projeto pode definir um tempo limite padrão diferente para solicitações de atualização, aplicável durante todo o projeto.</p> <p>Esse sinalizador permite que você substitua quaisquer padrões e defina o tempo limite individual para uma operação de atualização de recurso específica. Consulte também <code>deleteTimeout</code> e <code>createTimeout</code>.</p> |

Expressões do Cloud Assembly

Para maior flexibilidade, é possível adicionar expressões ao código do modelo de nuvem do Cloud Assembly.

Como funcionam expressões

As expressões do Cloud Assembly usam a construção `${expressão}`, conforme mostrado nos exemplos a seguir.

Observação As expressões do Cloud Assembly não são iguais a expressões regulares. Consulte a [Sintaxe de expressões do Cloud Assembly](#) do Cloud Assembly.

Os exemplos de código a seguir estão adaptados para mostrar apenas as linhas importantes. Todo o modelo de nuvem não editado é exibido no final.

Exemplos

No momento da implantação, permita que o usuário cole a chave criptografada necessária para acesso remoto:

```
inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine
    properties:
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
```

Para implantar no VMware Cloud on AWS, defina o nome da pasta para o nome necessário da *Carga de trabalho*:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```


No momento da implantação, marque a máquina com uma tag *env* toda em letras minúsculas que corresponda ao ambiente selecionado:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      constraints:
        - tag: '${"env:" + to_lower(input.environment)}'
```

Defina o número de máquinas no cluster de front-end como um (pequeno) ou dois (grande). Observe que o cluster grande é definido pelo processo de eliminação:

```
inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      count: '${input.envsize == "Small" ? 1 : 2}'
```

Anexe as máquinas à mesma rede *Padrão* ligando à propriedade encontrada no recurso de rede:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing
```

Criptografar credenciais de acesso enviadas à API:

```
resources:
  apitier:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        #cloud-config
      runcmd:
        - export apikey=${base64_encode(input.username:input.password)}
        - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
```

Descobrir o endereço da máquina da API:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        runcmd:
          - echo ${resource.apitier.networks[0].address}
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
```

Modelo de nuvem completo

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
  sshKey:
    type: string
    maxLength: 500
  envsize:
    type: string
    enum:
      - Small
      - Large
  resources:
    frontend:
      type: Cloud.Machine
      properties:
        folderName: '${input.environment == "VMC" ? "Workload" : ""}'
        image: ubuntu
```

```

    flavor: medium
    count: '${input.envsize == "Small" ? 1 : 2}'
    remoteAccess:
      authentication: publicPrivateKey
      sshKey: '${input.sshKey}'
    cloudConfig: |
      packages:
        - nginx
      runcmd:
        - echo ${resource.apitier.networks[0].address}
    constraints:
      - tag: '${"env:" + to_lower(input.environment)}'
    networks:
      - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: small
      cloudConfig: |
        #cloud-config
      runcmd:
        - export apikey=${base64_encode(input.username:input.password)}
        - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
    remoteAccess:
      authentication: publicPrivateKey
      sshKey: '${input.sshKey}'
    constraints:
      - tag: '${"env:" + to_lower(input.environment)}'
    networks:
      - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing
    constraints:
      - tag: '${"env:" + to_lower(input.environment)}'

```

Sintaxe de expressões do Cloud Assembly

A sintaxe da expressão expõe todos os recursos disponíveis de expressões em modelos do Cloud Assembly.

Observação As expressões do Cloud Assembly não são iguais a expressões regulares.

A sintaxe a seguir só é parcialmente representada nos exemplos mostrados em [Expressões do Cloud Assembly](#).

Literais

Há suporte para os seguintes literais:

- Boolean (verdadeiro ou falso)
- Inteiro
- Ponto flutuante
- Cadeia de caracteres

Barra invertida com aspas duplas, aspas simples e barra invertida em si:

" é deixada como \"

' é deixada como \'

\ é deixada como \\

As aspas só precisam ser deixadas dentro de uma cadeia de caracteres fechada com o mesmo tipo de aspas, como mostra o exemplo a seguir.

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Nulo

Variáveis de ambiente

Nomes de ambiente:

- orgId
- projectId
- projectName
- deploymentId
- deploymentName
- blueprintId
- blueprintVersion
- blueprintName
- requestedBy (usuário)
- requestedAt (hora)

Sintaxe:

```
env.ENV_NAME
```

Exemplo:

```
${env.blueprintId}
```

Variáveis de recurso

As variáveis de recurso permitem vincular a propriedades de recursos de outros recursos.

Sintaxe:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

Os nomes de recursos não podem conter traços ou pontos. Sublinhados são permitidos.

Exemplos:

- `${resource.db.id}`
- `${resource.db.networks[0].address}`
- `${resource.app.id}` (retornar a cadeia de caracteres para recursos não agrupados em cluster, onde a contagem não é especificada. Retorne a matriz para recursos agrupados em cluster.)
- `${resource.app[0].id}` (retornar a primeira entrada para recursos agrupados em cluster.)

Autovariáveis de recurso

Autovariáveis de recursos são permitidas apenas para recursos que oferecem suporte à fase de alocação. Autovariáveis de recursos apenas estão disponíveis (ou apenas têm um conjunto de valores) após a conclusão da fase de alocação.

Sintaxe:

```
self.property_name
```

Exemplo:

```
${self.address} (retornar o endereço atribuído durante a fase de alocação.)
```

Observe que, para um recurso denominado `resource_x`, `self.property_name` e `resource.resource_x.property_name` são idênticas e ambas são consideradas autoreferências.

Condições

Sintaxe:

- Os operadores de igualdade são `==` e `!=`.
- Os operadores relacionais são `<` `>` `<=` e `>=`.
- Os operadores lógicos são `&&` `||` e `!`.
- Os condicionais usam o padrão:

```
condition-expression ? true-expression : false-expression
```

Exemplos:

```
${input.count < 5 && input.size == 'small'}
```

```
${input.count < 2 ? "small":"large"}
```

Índice de contagem do cluster

Sintaxe:

```
count.index
```

Exemplos:

- Retorne o tipo de nó para recursos agrupados em cluster:

```
${count.index == 0 ? "primary":"secondary"}
```

- Defina o tamanho de cada disco durante a alocação:

```
inputs:
  disks:
    type: array
    minItems: 0
    maxItems: 12
    items:
      type: object
      properties:
        size:
          type: integer
          title: Size (GB)
          minSize: 1
          maxSize: 2048
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    allocatePerInstance: true
    properties:
      capacityGb: '${input.disks[count.index].size}'
      count: '${length(input.disks)}'
```

- Para mais exemplos, consulte [Clusters de máquina e disco no Cloud Assembly](#).

Operadores aritméticos

Sintaxe:

Os operadores são + - / * e %.

Exemplo:

```
${(input.count + 5) * 2}
```

Concatenação de cadeia de caracteres

Sintaxe:

```
${'ABC' + 'DEF'} avalia como ABCDEF.
```

Operadores [] e .

A expressão segue o ECMAScript ao unificar o tratamento de [] e . operadores.

Portanto, `expr.identifier` é equivalente a `expr["identifier"]`. O identificador é usado para construir um literal cujo valor é o identificador e, em seguida, o operador `[]` é usado com esse valor.

Exemplo:

```
${resource.app.networks[0].address}
```

Além disso, quando uma propriedade inclui um espaço, delimite-a com colchetes e aspas duplas em vez de usar a notação de pontos.

Incorreto:

```
input.operating system
```

Correto:

```
input["operating system"]
```

Construção do mapa

Sintaxe:

```
${{'key1':'value1', 'key2':input.key2}}
```

Construção da matriz

Sintaxe:

```
${['key1','key2']}
```

Exemplo:

```
${[1,2,3]}
```

Funções

Sintaxe:

```
${função(argumentos...)}
```

Exemplo:

```
${to_lower(resource.app.name)}
```

Tabela 6-1. Funções

| Função | Descrição |
|--|--|
| <code>abs(número)</code> | Valor de número absoluto |
| <code>avg(matriz)</code> | Retorna a média de todos os valores da matriz de números |
| <code>base64_decode(cadeia de caracteres)</code> | Retorna o valor de base64 decodificado |
| <code>base64_encode(cadeia de caracteres)</code> | Retorna o valor codificado de base64 |

Tabela 6-1. Funções (continuação)

| Função | Descrição |
|---------------------------------------|---|
| ceil(número) | Retorna o valor menor (mais próximo ao infinito negativo) que é maior ou igual ao argumento e é igual a um inteiro matemático |
| contains(matriz, valor) | Verifica se a matriz contém um valor |
| contains(cadeia de caracteres, valor) | Verifica se a cadeia de caracteres contém um valor |
| digest(valor, tipo) | Retorna resumo do valor usando o tipo suportado (md5, sha1, sha256, sha384, sha512) |
| ends_with(assunto, sufixo) | Verifica se a cadeia de caracteres do assunto termina com cadeia de caracteres de sufixo |
| filter_by(matriz, filtro) | Retornar apenas as entradas de matriz que passam a operação de filtro <pre>filter_by([1,2,3,4], x => x >= 2 && x <= 3) retorna [2, 3] filter_by({'key1':1, 'key2':2}, (k,v) => v != 1) retorna [{"key2": 2}]</pre> |
| floor(número) | Retorna o valor maior (mais próximo ao infinito positivo) que é menor ou igual ao argumento e é igual a um inteiro matemático |
| format(formato, valores...) | Retorna uma cadeia de caracteres formatada usando o formato e os valores do Formatador de Classe Java . |
| from_json(cadeia de caracteres) | Analisa a cadeia de caracteres json |
| join(matriz, delim.) | Associa a matriz de cadeias de caracteres a um delimitador e retornar uma cadeia de caracteres |
| json_path(valor, caminho) | Avalia o caminho contra o valor usando XPath para JSON . |
| keys(mapa) | Retorna chaves do mapa |
| length(matriz) | Retorna comprimento da matriz |
| length(cadeia de caracteres) | Retorna comprimento da cadeia de caracteres |
| map_by(matriz, operação) | Retornar cada entrada de matriz com uma operação aplicada a ela <pre>map_by([1,2], x => x * 10) retorna [10, 20] map_by([1,2], x => to_string(x)) retorna ["1", "2"] map_by({'key1':1, 'key2':2}, (k,v) => {k:v*10}) retorna [{"key1":10}, {"key2":20}]</pre> |

Tabela 6-1. Funções (continuação)

| Função | Descrição |
|--|--|
| map_to_object(matriz, keyname) | Retornar uma matriz de pares key:value do nome de chave especificado emparelhado com valores de outra matriz <pre>map_to_object(resource.Disk[*].id, "source")</pre> retorna uma matriz de pares key:value que tem um campo de chave chamado origem emparelhada com cadeias de caracteres de ID de disco Observe que <pre>map_by(resource.Disk[*].id, id => {'source':id})</pre> retorna o mesmo resultado |
| matches(cadeia de caracteres, regex) | Verifica se a cadeia de caracteres corresponde a uma expressão Regex |
| max(matriz) | Retorna o valor máximo da matriz de números |
| merge(mapa, mapa) | Retorna um mapa mesclado |
| min(matriz) | Retorna o valor mínimo da matriz de números |
| not_null(matriz) | Retorna a primeira entrada que não é nula |
| now() | Retorna a hora atual no formato ISO-8601 |
| intervalo(início, parada) | Retornar uma série de números em incrementos de 1 que começa com o número de início e termina antes do número de parada |
| replace(cadeia de caracteres, destino, substituição) | Substitui a cadeia de caracteres contendo cadeia de destino com cadeia de destino |
| reverse(matriz) | Reverte entradas da matriz |
| slice(matriz, início, fim) | Retorna a fatia da matriz do índice inicial para o índice final |
| split(cadeia de caracteres, delim.) | Divide a cadeia de caracteres com um delimitador e retornar matriz de cadeias de caracteres |
| starts_with(assunto, prefixo) | Verifica se a cadeia de caracteres do assunto começa com a cadeia de prefixo |
| substring(cadeia de caracteres, início, fim) | Retorna a subcadeia de caracteres do índice inicial até o índice final |
| sum(matriz) | Retorna a soma de todos os valores da matriz de números |
| to_json(valor) | Coloca em série o valor como cadeia de caracteres json |
| to_lower(cad.) | Converte a cadeia de caracteres em minúsculas |
| to_number(cadeia de caracteres) | Analisa a cadeia de caracteres como número |
| to_string(valor) | Retorna representação de cadeia de caracteres do valor |
| to_upper(cad.) | Converte a cadeia de caracteres em maiúsculas |
| trim(cadeia de caracteres) | Remove espaços à esquerda e à direita |

Tabela 6-1. Funções (continuação)

| Função | Descrição |
|----------------------------------|--|
| url_encode(cadeia de caracteres) | Codifica a cadeia de caracteres usando a especificação de codificação da URL |
| uuid() | Retorna UUID gerado aleatoriamente |
| values(mapa) | Retorna valores do mapa |

Solução de problemas

A linguagem YAML usa dois pontos e espaço (": ") como o separador entre chave e valor em pares de chave-valor. A sintaxe da expressão depende do YAML. Portanto, um espaço depois de dois pontos às vezes pode fazer com que uma expressão falhe.

Por exemplo, o espaço entre "win" : e "lin" na expressão a seguir causa uma falha.

```
${contains(input.image,"(Windows)") == true ? "win" : "lin"}
```

A expressão de trabalho omite o espaço.

```
${contains(input.image,"(Windows)") == true ? "win" : "lin"}
```

Se uma expressão continuar a falhar, tente colocar toda a expressão em marcas de verificação, conforme mostrado.

```
ezOS: '${contains(input.image,"(Windows)") == true ? "win" : "lin"}'
```

Propriedades secretas do Cloud Assembly

Uma propriedade secreta do Cloud Assembly é um valor reutilizável e criptografado que os usuários do projeto podem adicionar aos seus designs de modelo de nuvem.

As credenciais e as chaves de acesso seguro são exemplos típicos de propriedades secretas. Depois de criado e salvo, um valor de propriedade secreta nunca pode ser descriptografado ou lido.

Criando uma propriedade secreta

- 1 Faça login no Cloud Assembly com privilégios da função de administrador do projeto.
- 2 Acesse **Infraestrutura > Administração > Segredos** e clique em **Novo Segredo**.
- 3 Selecione o projeto.
- 4 Insira um nome de propriedade exclusivo para o segredo, sem espaços ou caracteres especiais.
O nome é o identificador visível do segredo.
- 5 Insira o valor secreto.
Ao digitar, o valor é ocultado por padrão, o que o protegerá se a tela for compartilhada.

Se necessário, você pode clicar no símbolo do olho para revelar e verificar um valor. Porém, depois de ser salvo, um valor secreto ficará criptografado no banco de dados e nunca poderá ser exposto novamente.

6 Opcionalmente, insira uma descrição mais longa da propriedade secreta.

7 Clique em **Criar**.

Adicionando uma propriedade secreta a um modelo de nuvem

Os usuários do projeto podem adicionar uma propriedade secreta como uma vinculação no código de modelo de nuvem.

Observe que começar a digitar os caracteres `'${secret.` revela uma lista de seleção de segredos que foram criados para o projeto.

```
type: Cloud.Machine
properties:
  name: ourvm
  image: mint20
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: '${secret.ourPublicKey}'
    username: root
```

Para adicionar uma propriedade secreta a uma configuração do Terraform, consulte [Usando uma propriedade secreta do Cloud Assembly em uma configuração do Terraform](#).

Acesso remoto a uma implantação do Cloud Assembly

Para acessar remotamente uma máquina que o Cloud Assembly implantou, adicione propriedades, antes da implantação, ao modelo de nuvem dessa máquina.

Para acesso remoto, é possível configurar uma das seguintes opções de autenticação.

Observação Nos casos em que as chaves precisam ser copiadas, também é possível criar uma seção `cloudConfig` no modelo de nuvem para copiar automaticamente as chaves no provisionamento. As especificações não estão documentadas aqui, mas [Inicialização de máquinas no Cloud Assembly](#) fornece informações gerais sobre o `cloudConfig`.

Gerar um par de chaves no momento do provisionamento

Se você não tiver seu próprio par de chaves pública e privada para autenticação de acesso remoto, o Cloud Assembly poderá gerar um par de chaves.

Use o código a seguir como uma diretriz.

- 1 No Cloud Assembly, antes do provisionamento, adicione propriedades de `remoteAccess` ao modelo de nuvem conforme mostrado no exemplo.

O username é opcional. Se você o omitir, o sistema gerará um ID aleatório como o nome de usuário.

Exemplo:

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: generatedPublicPrivateKey
    username: testuser
```

- 2 No Cloud Assembly, provisione a máquina a partir do modelo de nuvem e traga-a para um estado iniciado.

O processo de provisionamento gera as chaves.

- 3 Localize o nome da chave nas propriedades em **Recursos > Implantações > Topologia**.

- 4 Use a interface do provedor de nuvem, como o cliente vSphere, para acessar a linha de comando da máquina provisionada.

- 5 Conceda permissão de leitura para a chave privada.

```
chmod 600 key-name
```

- 6 Acesse a implantação do Cloud Assembly, selecione a máquina e clique em **Ações > Obter Chave Privada**.

- 7 Copie o arquivo de chave privada para a sua máquina local.

Um caminho de arquivo local típico é `/home/username/.ssh/key-name`.

- 8 Abra uma sessão SSH remota e conecte-se à máquina provisionada.

```
ssh -i key-name user-name@machine-ip
```

Fornecer o próprio par de chaves pública-privada

Muitas empresas criam e distribuem os próprios pares de chaves pública-privada para autenticação.

Use o código a seguir como uma diretriz.

- 1 No ambiente local, obtenha ou gere seu par de chaves pública-privada.
Por enquanto, basta gerar e salvar localmente as chaves.
- 2 No Cloud Assembly, antes do provisionamento, adicione propriedades de `remoteAccess` ao modelo de nuvem conforme mostrado no exemplo.

A `sshKey` inclui o alfanumérico longo encontrado no arquivo de chave pública *nome de chave.pub*.

O nome de usuário é opcional e é criado para ser usado no login. Se você o omitir, o sistema gerará um ID aleatório como o nome de usuário.

Exemplo:

```
type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9tslf
qGxvU66PX9IeZax5hZvNWFgJw6ag+Z1zndOLhVdVoW49f274/mIRiId7Uuw...
    username: testuser
```

- 3 No Cloud Assembly, provisione a máquina a partir do modelo de nuvem e traga-a para um estado iniciado.
- 4 Usando o cliente do fornecedor de nuvem, acesse a máquina provisionada.
- 5 Adicione o arquivo de chave pública à pasta inicial na máquina. Use a chave especificada em `remoteAccess.sshKey`.
- 6 Verifique se a contraparte do arquivo de chave privada está presente na máquina local.
A chave é normalmente `/home/username/.ssh/key-name` sem a extensão `.pub`.
- 7 Abra uma sessão SSH remota e conecte-se à máquina provisionada.

```
ssh -i key-name user-name@machine-ip
```

Fornecer um par de chaves AWS

Adicionando um nome de par de chaves do AWS ao modelo de nuvem, é possível acessar remotamente uma máquina que o Cloud Assembly implanta no AWS.

Lembre-se de que os pares de chaves AWS são específicos da região. Se provisionar cargas de trabalho em `us-east-1`, o par de chaves deverá existir na `us-east-1`.

Use o código a seguir como uma diretriz. Essa opção funciona apenas para zonas de nuvem AWS.

```
type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess:
    authentication: keyPairName
    keyPair: cas-test
constraints:
  - tag: 'cloud:aws'
```

Fornecer um nome de usuário e senha

Ao adicionar um nome de usuário e uma senha ao modelo de nuvem, é possível ter acesso remoto simples a uma máquina que o Cloud Assembly implanta.

Embora seja menos seguro, o login remoto com um nome de usuário e senha pode ser tudo o que a sua situação requer. Lembre-se de que alguns fornecedores de nuvem ou configurações podem não oferecer suporte a essa opção menos segura.

- 1 No Cloud Assembly, antes do provisionamento, adicione propriedades de `remoteAccess` ao modelo de nuvem conforme mostrado no exemplo.

Defina o nome de usuário e a senha para a conta com a qual você espera fazer login.

Exemplo:

```
type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: usernamePassword
    username: testuser
    password: admin123
```

- 2 No Cloud Assembly, provisione a máquina a partir do modelo de nuvem e traga-a para um estado iniciado.
- 3 Vá para a interface do seu fornecedor de nuvem e acesse a máquina provisionada.
- 4 Na máquina provisionada, crie ou habilite a conta.
- 5 Na máquina local, abra uma sessão remota para o endereço IP da máquina provisionada ou FQDN e faça login normalmente com o nome de usuário e a senha.

Posicionamento de discos SCSI com o Cloud Assembly

Para gerenciar um disco SCSI, você deve especificar e saber seu controlador SCSI e o número da unidade lógica (LUN). Para um objeto de disco vSphere, você pode usar o Cloud Assembly para atribuir ambos os valores no modelo de nuvem.

A capacidade de usar diferentes controladores SCSI é importante para o desempenho e necessária para alguns tipos de implantação, como o Oracle Real Application Clusters (RAC).

Controlador SCSI e propriedades do disco LUN

Para atribuir um controlador SCSI e LUN, adicione as seguintes propriedades do modelo de nuvem:

```
SCSIController
```

```
unitNumber
```

Você também tem a opção de omitir as propriedades e, nesse caso, a atribuição segue um padrão previsível. O Cloud Assembly não implanta mais discos SCSI em ordem aleatória, o que os tornou difíceis de gerenciar.

Os controladores e discos SCSI são numerados em ordem, com zero sendo o primeiro. Cada controlador SCSI pode oferecer suporte a discos SCSI de números de unidade de 0 a 15.

Opção 1: Definir o controlador SCSI e o número da unidade

Você pode especificar totalmente ambas as propriedades, conforme mostrado no exemplo a seguir. Nesse caso, a atribuição do controlador SCSI e o número da unidade correspondem aos valores inseridos.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
      unitNumber: 0
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
```

```

    unitNumber: 1
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_3
      unitNumber: 4

```

Opção 2: Definir apenas o controlador SCSI

Você pode especificar o controlador SCSI e omitir o número da unidade. Nesse caso, a atribuição do controlador SCSI corresponde ao valor inserido. O número da unidade é definido como o primeiro número da unidade disponível naquele controlador.

```

resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_0
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_0
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_1

```

Opção 3: Omitir ambas as propriedades

Você pode omitir o controlador SCSI e o número da unidade. Nesse caso, a atribuição é definida para o primeiro controlador SCSI disponível e o primeiro número de unidade disponível sob esse controlador.

```

resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1

```



```

totalMemoryMB: 1024
attachedDisks:
  - source: '${resource.Cloud_vSphere_Disk_1.id}'
  - source: '${resource.Cloud_vSphere_Disk_2.id}'
  - source: '${resource.Cloud_vSphere_Disk_3.id}'
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
Cloud_vSphere_Disk_2:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
Cloud_vSphere_Disk_3:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1

```

Não é uma opção: apenas LUN

Você não pode omitir o controlador SCSI e especificar apenas um número de unidade. Isso pode resultar em uma implantação em que vários controladores SCSI têm um disco desse número, mas, para fins de gerenciamento, você não saberá qual disco é qual.

Usando entradas para definir o controlador SCSI e LUN

Para tornar o projeto mais dinâmico, use entradas para que o usuário possa especificar qual controlador SCSI e número de unidade na ocasião da solicitação ou da atualização.

```

inputs:
  diskProperties:
    type: array
    minItems: 1
    maxItems: 10
    items:
      type: object
      properties:
        size:
          type: integer
        SCSIController:
          type: string
          title: SCSI Controller
          enum:
            - SCSI_Controller_0
            - SCSI_Controller_1
            - SCSI_Controller_2
            - SCSI_Controller_3
        unitNumber:
          type: integer
          title: Unit Number

resources:
  app:

```

```

type: Cloud.vSphere.Machine
allocatePerInstance: true
properties:
  flavor: small
  image: centos
  attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0, 4), 'source')}'
disk:
  type: Cloud.vSphere.Disk
  allocatePerInstance: true
  properties:
    capacityGb: '${input.diskProperties[count.index].size}'
    SCSIController: '${input.diskProperties[count.index].SCSIController}'
    unitNumber: '${input.diskProperties[count.index].unitNumber}'
    count: ${length(input.diskProperties)}

```

size 1

SCSI Controller SCSI_Controller_0

Unit Number 2

CANCEL APPLY

Inicialização de máquinas no Cloud Assembly

Você pode aplicar a inicialização da máquina no Cloud Assembly executando comandos diretamente ou, se estiver implantando em zonas de nuvem baseadas no vSphere, por meio de especificações de personalização.

Como funcionam comandos e especificações de personalização

- Comandos

Uma seção `cloudConfig` no seu código de modelo de nuvem contém os comandos que você deseja executar.

- Especificações de personalização

Uma propriedade no seu código de modelo de nuvem faz referência a uma especificação de personalização do vSphere por nome.

Comandos e especificações de personalização podem não se misturar

Ao implantar no vSphere, prossiga com cuidado se tentar combinar o `cloudConfig` e a inicialização da especificação de personalização. Eles não são formalmente compatíveis e podem produzir resultados inconsistentes ou indesejados quando usados juntos.

Para obter um exemplo de como os comandos e as especificações de personalização interagem, consulte [Endereços IP estáticos do vSphere no Cloud Assembly](#).

Especificações de personalização do vSphere em modelos do Cloud Assembly

Ao implantar em zonas de nuvem baseadas no vSphere no Cloud Assembly, especificações de personalização podem aplicar configurações de sistema operacional guest no momento da implantação.

Ativando a especificação de personalização

A especificação de personalização deve existir no vSphere, no destino no qual for implantada.

Edite diretamente o código do modelo de nuvem. O exemplo a seguir aponta para uma especificação de personalização `cloud-assembly-linux` para um host do WordPress no vSphere.

```
resources:
  WebTier:
    type: Cloud.vSphere.Machine
    properties:
      name: wordpress
      cpuCount: 2
      totalMemoryMB: 1024
      imageRef: 'Template: ubuntu-18.04'
      customizationSpec: 'cloud-assembly-linux'
      folderName: '/Datacenters/Datacenter/vm/deployments'
```

Usar especificações de personalização ou comandos cloudConfig

Se quiser que a experiência de provisionamento corresponda ao que está fazendo atualmente no vSphere, continuar usando as especificações de personalização poderá ser a melhor abordagem. No entanto, para expandir para o provisionamento de nuvem híbrida ou várias nuvens, uma abordagem mais neutra são os comandos de inicialização cloudConfig.

Para obter mais informações sobre as seções de cloudConfig em modelos de nuvem, consulte [Comandos de configuração em modelos do Cloud Assembly](#).

Comandos e especificações de personalização podem não se misturar

Ao implantar no vSphere, proceda com cuidado se tentar combinar o comando cloudConfig incorporado e a inicialização de especificação de personalização. Eles não são formalmente compatíveis e podem produzir resultados inconsistentes ou indesejados quando usados juntos.

Para obter um exemplo de como os comandos e as especificações de personalização interagem, consulte [Endereços IP estáticos do vSphere no Cloud Assembly](#).

Comandos de configuração em modelos do Cloud Assembly

É possível adicionar uma seção `cloudConfig` ao código de modelo do Cloud Assembly, na qual são adicionados comandos de inicialização de máquina, executados no momento da implantação.

formatos de comandos `cloudConfig`

- Linux — os comandos de inicialização seguem o padrão aberto [cloud-init](#).
- Windows — os comandos de inicialização usam [Cloudbase-init](#).

O Linux [cloud-init](#) e o Windows [Cloudbase-init](#) não compartilham a mesma sintaxe. Uma seção `cloudConfig` para um sistema operacional não funcionará em uma imagem de máquina do outro sistema operacional.

O que comandos `cloudConfig` podem fazer

Você usa comandos de inicialização para automatizar a aplicação de dados ou configurações no momento da criação da instância, o que pode personalizar usuários, permissões, instalações ou qualquer outra operação baseada em comando. Exemplos incluem:

- Configuração de um nome do host
- Geração e configuração de chaves privadas SSH
- Instalação de pacotes

Onde comandos `cloudConfig` podem ser adicionados

Você pode adicionar uma seção `cloudConfig` ao código do modelo de nuvem, mas também pode adicionar uma seção a uma imagem de máquina com antecedência ao configurar a infraestrutura. Dessa forma, todos os modelos de nuvem que fizerem referência à imagem de origem terão a mesma inicialização.

É possível ter um mapa de imagem e um modelo de nuvem em que ambos contêm comandos de inicialização. No momento da implantação, os comandos são mesclados e o Cloud Assembly executa os comandos consolidados.

Quando o mesmo comando é exibido em ambos os locais, mas inclui parâmetros diferentes, somente o comando de mapa de imagem é executado.

Consulte [Saiba mais sobre mapeamentos de imagem no vRealize Automation](#) para obter mais detalhes.

Comandos cloudConfig de exemplo

A seção de exemplo a seguir do cloudConfig é obtida do código de modelo de nuvem para o servidor MySQL baseado em Linux do [Criar um modelo de nuvem básico](#).

Observação Para garantir a interpretação correta de comandos, sempre inclua o caractere de pipe cloudConfig: |, conforme mostrado.

```
cloudConfig: |
  #cloud-config
  repo_update: true
  repo_upgrade: all
  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
    - php-mcrypt
    - mysql-client
  runcmd:
    - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
      https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
      mywordpresssite --strip-components 1
    - i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
      {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
      i=$((i+1)); done
    - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
      wordpress_blog;"
    - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
      mywordpresssite/wp-config.php
    - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
      'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
      -i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
      'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
      -e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
      'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
      -i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
      {DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - service apache2 reload
```

Se um script de inicialização na nuvem se comportar inesperadamente, verifique a saída do console capturado no `/var/log/cloud-init-output.log` ao solucionar o problema. Para obter mais informações sobre cloud-init, [consulte a documentação de cloud-init](#).

Comandos e especificações de personalização podem não se misturar

Ao implantar no vSphere, proceda com cuidado se tentar combinar o comando cloudConfig incorporado e a inicialização de especificação de personalização. Eles não são formalmente compatíveis e podem produzir resultados inconsistentes ou indesejados quando usados juntos.

Para obter um exemplo de como os comandos e as especificações de personalização interagem, consulte [Endereços IP estáticos do vSphere no Cloud Assembly](#).

vSphere modelos de inicialização no Cloud Assembly

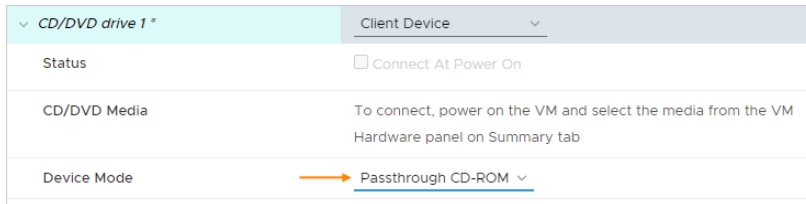
Quando o modelo Cloud Assembly implanta uma imagem com base em um modelo vSphere, o modelo vSphere deve ser configurado com antecedência para suportar o cloud-init.

Para configurar um modelo vSphere para suportar o cloud-init, siga os seguintes passos.

- 1 Na máquina virtual que se tornará o modelo, instale cloud-init.

Por exemplo, use `yum` para instalar cloud-init em CentOS ou `apt-get` para instalar no Ubuntu.

- 2 Defina o CD-ROM da máquina virtual para o modo de passagem.



- 3 Na linha de comando do sistema operacional convidado, execute o comando `cloud-init clean`.

Observação Quando o `cloud-init clean` finalizar, não modifique mais a máquina virtual.

- 4 Desligue a máquina virtual e converta-a em um modelo.

Endereços IP estáticos do vSphere no Cloud Assembly

Ao implantar no vSphere no Cloud Assembly, você pode atribuir um endereço IP estático, mas deve tomar cuidado para não introduzir conflitos entre os comandos de inicialização cloudConfig e especificações de personalização.

Designs de amostra

Os designs a seguir aplicam com segurança um endereço IP estático sem nenhum conflito entre os comandos de inicialização do modelo de nuvem e especificações de personalização. Todos contêm a configuração de rede `assignment: static`.

| Projetar | Amostra de código de modelo de nuvem |
|---|---|
| <p>Atribuir um endereço IP estático a uma máquina Linux que não possui código cloud-init</p> | <pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: linux-template networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre> |
| <p>Atribua um endereço IP estático a uma máquina Linux com código cloud-init que não contenha comandos de atribuição de rede. OBSERVAÇÃO: a especificação de personalização do vSphere será aplicada se você definir a propriedade customizeGuestOs como true ou omitir a propriedade customizeGuestOs.</p> | <p>Amostra do Ubuntu</p> <pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: true cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: root:Pa\$\$w0rd expire: false write_files: - path: /tmpFile.txt content: \${resource.wpnet.dns} runcmd: - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre> <p>Amostra do CentOS</p> <pre>resources: wpnet: type: Cloud.Network properties:</pre> |

Projetar**Amostra de código de modelo de nuvem**

```
    name: wpnet
    networkType: public
    constraints:
      - tag: sqa
DBTier:
  type: Cloud.vSphere.Machine
  properties:
    flavor: small
    image: centos-template
    customizeGuestOs: true
    cloudConfig: |
      #cloud-config
      write_files:
        - path: /test.txt
          content: |
            deploying in power off.
            then rebooting.
  networks:
    - name: '${wpnet.name}'
      assignment: static
      network: '${resource.wpnet.id}'
```


| Projetar | Amostra de código de modelo de nuvem |
|--|--|
| <p>Atribua um endereço IP estático a uma máquina Linux com código cloud-init que contenha comandos de atribuição de rede. A propriedade <code>customizeGuestOs</code> deve ser <code>false</code>.</p> | <p>Amostra do Ubuntu</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: false cloudConfig: #cloud-config write_files: - path: /etc/netplan/99-installer- config.yaml content: network: version: 2 renderer: networkd ethernet: ens160: addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre> <p>Amostra do CentOS</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: centos-template </pre> |

Projetar**Amostra de código de modelo de nuvem**

```

    customizeGuestOs: false
    cloudConfig: |
      #cloud-config
      ssh_pwauth: yes
      chpasswd:
        list: |
          root:VMware1!
        expire: false
      runcmd:
        - nmcli con add type
  ethernet con-name 'custom ens192'
  ifname ens192 ip4 ${self.networks[0].address}/
  ${resource.wpnet.prefixLength} gw4 $
  {resource.wpnet.gateway}
    - nmcli con mod 'custom ens192' ipv4.dns "$
  {join(resource.wpnet.dns, ' ')}"
    - nmcli con mod 'custom ens192' ipv4.dns-
  search "${join(resource.wpnet.dnsSearchDomains, ',')}
    - nmcli con down 'System ens192' ; nmcli
  con up 'custom ens192'
    - nmcli con del 'System ens192'
    - hostnamectl set-hostname --static `dig -x
  ${self.networks[0].address} +short | cut -d "." -f 1`
    - hostnamectl set-hostname --pretty $
  {self.resourceName}
    - touch /etc/cloud/cloud-init.disabled
  networks:
    - name: '${wpnet.name}'
      assignment: static
      network: '${resource.wpnet.id}'

```

Ao basear a implantação em uma imagem referenciada, atribua um endereço IP estático a uma máquina Linux com código cloud-init que contenha comandos de atribuição de rede. A propriedade `customizeGuestOs` deve ser `false`. Além disso, o modelo de nuvem não deve incluir a propriedade `ovfProperties`, que bloqueia a personalização.

```

resources:
  wpnet:
    type: Cloud.Network
    properties:
      name: wpnet
      networkType: public
      constraints:
        - tag: sqa
  DBTier:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small

imageRef: 'https://cloud-images.ubuntu.com/releases/
focal/release/ubuntu-20.04-server-cloudimg-amd64.ova'
customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:Pa$$w0rd
      ubuntu:Pa$$w0rd
    expire: false
  write_files:
    - path: /etc/netplan/99-netcfg-vrac.yaml
      content: |
        network:
          version: 2
          renderer: networkd

```

Projetar**Amostra de código de modelo de nuvem**

```

ethernets:
  ens192:
    dhcp4: no
    dhcp6: no
    addresses:
      - ${resource.DBTier.networks[0].address}/${
        {resource.wpnet.prefixLength}
        gateway4: $
        {resource.wpnet.gateway}
        nameservers:
          search: $
          {resource.wpnet.dnsSearchDomains}
          addresses: ${resource.wpnet.dns}
    runcmd:
      - netplan apply
      - hostnamectl set-hostname --pretty $
        {self.resourceName}
      - touch /etc/cloud/cloud-init.disabled
    networks:
      - name: '${wpnet.name}'
        assignment: static
        network: '${resource.wpnet.id}'

```

Designs que não funcionam ou podem produzir resultados indesejados

- O código cloud-init não contém comandos de atribuição de rede, e a propriedade `customizeGuestOs` é `false`.

Nem os comandos de inicialização, nem especificações de personalização estão presentes para definir as configurações de rede.

- O código cloud-init não contém comandos de atribuição de rede, e a propriedade `ovfProperties` está definida.

Comandos de inicialização não estão presentes, mas `ovfProperties` bloqueou a especificação da personalização.

- O código cloud-init contém comandos de atribuição de rede, e a propriedade `customizeGuestOs` está ausente ou definida como `true`.

A aplicação da especificação de personalização entra em conflito com os comandos de inicialização.

Outras soluções alternativas para cloud-init e especificações de personalização

Ao implantar no vSphere, você também pode personalizar uma imagem para solucionar conflitos de cloud-init e especificações de personalização. Consulte o seguinte repositório externo para obter mais informações.

- [Scripts de preparação de imagem do vSphere](#)

Implantação atrasada no Cloud Assembly

Uma máquina virtual pode precisar ser totalmente inicializada antes de prosseguir com a implantação do Cloud Assembly.

Por exemplo, implantar uma máquina que ainda está instalando pacotes e iniciando um servidor web pode levar a condições em que um usuário rápido tenta acessar o aplicativo antes que esteja disponível.

Esteja ciente das seguintes considerações ao usar este recurso.

- O recurso usa o módulo `phone_home` de [cloud-init](#) e está disponível durante a implantação de máquinas Linux.
- O phone home não está disponível para Windows devido às limitações de [Cloudbase-init](#).
- O phone home pode afetar a ordem de implantação como uma dependência explícita, mas tem mais flexibilidade em relação às opções de tempo e processamento.

Consulte [Criando associações e dependências entre recursos no Cloud Assembly](#).

- O phone home requer uma seção `cloudConfig` no modelo de nuvem.
- A sua criatividade é um fator. Comandos de inicialização podem incluir tempo de espera incorporado entre operações, que pode ser usado em conjunto com o phone home.
- O phone home baseado em modelo de nuvem não funcionará se o modelo de máquina já contiver as configurações do módulo `phone_home`.
- A máquina deve ter acesso de comunicação de saída de retorno ao Cloud Assembly.

Para introduzir um atraso de implantação no Cloud Assembly, adicione uma seção

`cloudConfigSettings` ao modelo de nuvem:

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

| Propriedade | Descrição |
|--------------------------------------|--|
| <code>phoneHomeShouldWait</code> | Se for esperar pela inicialização, <code>true</code> ou <code>false</code> . |
| <code>phoneHomeTimeoutSeconds</code> | Quando se decide se deseja prosseguir com a implantação, mesmo que a inicialização ainda esteja em execução. O padrão é 10 minutos. |
| <code>phoneHomeFailOnTimeout</code> | Se deseja continuar com a implantação após o tempo de intervalo esgotado, <code>true</code> ou <code>false</code> . Observe que, mesmo ao prosseguir, a implantação ainda poderá falhar por motivos distintos. |

Personalização de guests do Windows no Cloud Assembly

Para que o Cloud Assembly inicialize automaticamente uma máquina Windows na implantação, prepare uma imagem que ofereça suporte a Cloudbase-Init e, em seguida, um modelo de nuvem que contenha os comandos apropriados.

O processo de criação de imagem varia dependendo do fornecedor de nuvem. O exemplo mostrado aqui é para o vSphere.

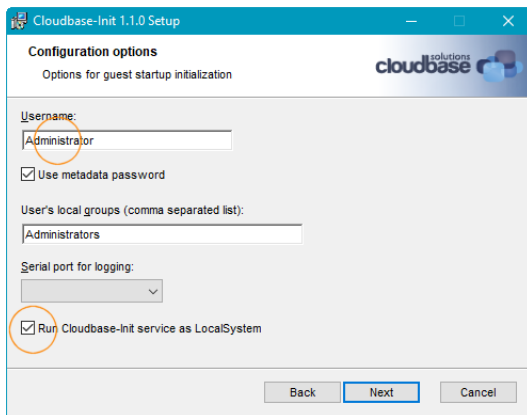
Imagem do Windows do Cloud Assembly para o vSphere

Para o Cloud Assembly inicializar uma máquina Windows implantada no vSphere, a imagem precisa ser baseada em um modelo do vSphere com o Cloudbase-Init instalado e configurado.

Criando a imagem

- 1 Use o vSphere para criar e ligar uma máquina virtual Windows.
- 2 Na máquina virtual, faça login no Windows.
- 3 Baixe Cloudbase-Init.
<https://cloudbase.it/cloudbase-init/#download>
- 4 Inicie o arquivo .msi de Cloudbase-Init.

Durante a instalação, insira **Administrador** como o nome de usuário e selecione a opção para executar como LocalSystem.



Outras seleções de configuração podem permanecer como valores padrão.

- 5 Permita que a instalação seja executada, mas não feche a página final Concluído do assistente de configuração.

Importante Não feche a página final do assistente de configuração.

- 6 Com a página Concluído do assistente de instalação ainda aberta, use o Windows para navegar até o caminho de instalação de Cloudbase-Init e abra o seguinte arquivo em um editor de texto.

```
conf\cloudbase-init-unattend.conf
```

- 7 Defina `metadata_services` como `OvfService` como mostrado. Adicione a configuração se ela ainda não existir.

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```

- 8 Salve e feche `cloudbase-init-unattend.conf`.

- 9 Na mesma pasta, abra o seguinte arquivo em um editor de texto.

```
conf\cloudbase-init.conf
```

- 10 Defina `first_logon_behaviour`, `metadata_services` e `plugins` conforme mostrado. Adicione as configurações se elas ainda não existirem.

```
first_logon_behaviour=always
. . .
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
. . .
plugins=cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.win
dows.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUs
erSSHPublicKeysPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
. . .
```

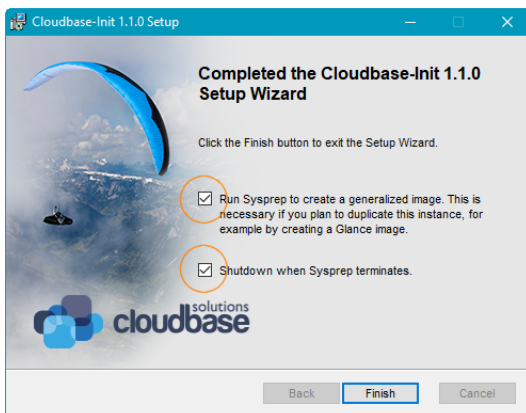
- 11 Salve e feche `cloudbase-init.conf`.

- 12 Na página Concluído do assistente de instalação, selecione as opções para executar Sysprep e desligar após Sysprep e clique em **Concluir**.

Observação A VMware tem visto casos em que a execução do Sysprep impede que as implantações da imagem funcionem.

Durante a implantação, o Cloud Assembly aplica uma especificação de personalização gerada dinamicamente, o que desconecta a interface de rede. O estado de Sysprep pendente na imagem pode fazer com que a especificação de personalização falhe e deixar a implantação desconectada.

Se você suspeitar que isso está acontecendo no seu ambiente, tente deixar as opções de Sysprep desativadas ao criar a imagem.



13 Depois que a máquina virtual for encerrada, use vSphere para transformá-la em um modelo.

Detalhes adicionais

A tabela a seguir expande as entradas de configuração feitas durante a instalação.

| Definição da configuração | Objetivo |
|--|---|
| Username, CreateUserPlugin e SetUserPasswordPlugin | Após Sysprep, a primeira inicialização usa CreateUserPlugin para criar a conta com o nome de usuário Administrador e uma senha em branco. SetUserPasswordPlugin permite que Cloudbase-Init altere a senha em branco para a senha de acesso remoto que será incluída no modelo de nuvem. |
| Comportamento do primeiro logon | Essa configuração solicita que o usuário altere a senha no primeiro logon. |
| Serviços de metadados | Ao listar apenas OvfService, Cloudbase-Init não tentará encontrar outros serviços de metadados que não sejam compatíveis com o vCenter. Isso resulta em arquivos de log mais limpos, pois os logs seriam preenchidos de outra forma com entradas sobre a falha ao encontrar os outros serviços. |
| Plug-ins | Ao listar apenas os plug-ins com recursos compatíveis com o OvfService, os logs são mais limpos. Cloudbase-Init executa plug-ins na ordem especificada. |
| Executar como LocalSystem | Essa configuração oferece suporte a qualquer comando de inicialização avançado que possa exigir que Cloudbase-Init seja executado em uma conta de administrador dedicada. |

Comandos do Cloudbase-Init para Windows no Cloud Assembly

Para executar a inicialização da máquina Windows no momento da implantação, adicione comandos do Cloudbase-Init ao código do modelo do Cloud Assembly.

O exemplo mostrado aqui é baseado no vSphere, mas outros fornecedores de nuvem devem ser semelhantes.

Pré-requisitos

- Crie a infraestrutura. No Cloud Assembly, adicione sua conta de nuvem do vSphere e uma zona de nuvem associada.
- Adicione mapeamentos de tipo e imagem e adicione perfis de rede e de armazenamento.

Na sua infraestrutura, um mapeamento de imagem deve apontar para um modelo do Windows que você criou para oferecer suporte ao Cloudbase-Init. Consulte [Imagem do Windows do Cloud Assembly para o vSphere](#).

Se o modelo não estiver listado, vá para Contas de Nuvem e sincronize imagens. Caso contrário, a sincronização automática será executada a cada 24 horas.

- Adicione um projeto, adicione usuários e certifique-se de que eles possam provisionar sua zona de nuvem.

Para obter mais informações sobre a criação de infraestrutura e projetos, consulte os exemplos no [Tutorial: configurando e testando a infraestrutura e as implantações de várias nuvens no Cloud Assembly](#).

Procedimento

- 1 No Cloud Assembly, acesse a guia **Projetar** e crie um novo modelo de nuvem.
- 2 Adicione uma seção `cloudConfig` com os comandos do Cloudbase-init desejados.

Os exemplos de comando a seguir criam um novo arquivo na unidade `C:` do Windows e definem o nome do host.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: cloudbase-init-win-2016
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: Administrator
        password: Password1234@$
      cloudConfig: |
        #cloud-config
        write_files:
          content: Cloudbase-Init test
          path: C:\test.txt
          set_hostname: testname
```

Para obter mais informações, consulte a [documentação do Cloudbase-init](#).

- 3 Adicione propriedades `remoteAccess` para que você configure a máquina para login inicial no Windows.

Conforme mencionado quando você criou o modelo, o serviço de metadados seleciona as credenciais de login e as expõe para `CreateUserPlugin` e `SetUserPasswordPlugin`. Observe que a senha deve atender aos requisitos de senha do Windows.

- 4 No Cloud Assembly, teste e implante o modelo de nuvem.
- 5 Após a implantação, use a Windows RDP e as credenciais no modelo para fazer login na nova máquina Windows e verificar a personalização.

No exemplo acima, você deve procurar o arquivo `C:\test.txt` e verificar as propriedades do sistema para o nome do host.

Clusters de máquina e disco no Cloud Assembly

Os designs de modelo do Cloud Assembly podem implantar um cluster de máquinas e anexar um cluster de discos.

Para implantar clusters de máquinas e discos, aproveite as vantagens do [Sinalizadores de recursos do Cloud Assembly para solicitações](#) de `allocatePerInstance`, de `count.index` e da [Sintaxe de expressões do Cloud Assembly](#) `map_to_object` nos seus modelos de nuvem.

Os exemplos de código de modelo de nuvem a seguir podem servir como diretrizes para designs que implantam clusters.

Duas máquinas que compartilham um cluster de discos

```
resources:
  app0:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0,2), "source")}'
  appl:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2,4), "source")}'
  disk:
    type: Cloud.Volume
    allocatePerInstance: true
    properties:
      count: 4
      capacityGb: 5
```

Número variável de máquinas com um disco cada

```
inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: '${input.count}'
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, count.index, count.index + 1), "source")}'
```

```

disk:
  type: Cloud.Volume
  allocatePerInstance: true
  properties:
    count: '${input.count}'
    capacityGb: 5

```

Número variável de máquinas com dois discos cada

```

inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: ${input.count}
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2*count.index,
2*(count.index + 1)), "source")}'
    disk:
      type: Cloud.Volume
      allocatePerInstance: true
      properties:
        count: ${2*input.count}
        capacityGb: 5

```

Defina tamanhos de discos no momento da solicitação

```

inputs:
  disksize:
    type: array
    minItems: 2
    maxItems: 2
    items:
      type: object
      properties:
        size:
          type: integer
resources:
  app:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      flavor: small
      image: ubuntu
      attachedDisks: ${map_to_object(slice(resource.disk[*].id, 0, 2), 'source')}
    disk:
      type: Cloud.Volume

```

```
allocatePerInstance: true
properties:
  count: 2
  capacityGb: ${input.disksize[count.index].size}
```

Nomenclatura personalizada para recursos implantados no Cloud Assembly

Como administrador de nuvem ou projeto, você tem uma convenção de nomenclatura prescrita para recursos no seu ambiente e deseja que o recurso implantado siga essas convenções sem a interação dos usuários. É possível criar um modelo de nomenclatura para todas as implantações de um projeto do Cloud Assembly.

Por exemplo, sua convenção de nomenclatura para hosts é prefixar um recurso como *projectname-sitecode-costcenter-whereDeployed-identifier*. Você configura o modelo de nomenclatura personalizado para as máquinas de cada projeto. Algumas das variáveis de modelo são retiradas do sistema conforme este ele é implementado, enquanto outras são baseadas nas propriedades personalizadas do projeto. O modelo de nomenclatura personalizado para o prefixo acima é semelhante ao exemplo a seguir.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

O identificador, fornecido no modelo como `${#####}`, mostra um identificador de seis dígitos. O identificador é um contador que garante exclusividade. O contador é global para a organização e incrementa em todos os projetos, não apenas no projeto atual. Quando você tem vários projetos, não espere uma sequência de 000123 a 000124 para implantações no projeto atual. Você pode esperar um incremento de 000123 a 000127.

Todos os nomes de recursos devem ser exclusivos. Para garantir a exclusividade, use a propriedade de número incremental. Os números incrementam para todas as implantações, incluindo aquelas cujos nomes são definidos pelo Cloud Assembly. À medida que seu sistema se tornar mais robusto e como o sistema aplica nomes personalizados a muitos tipos de recursos, a numeração poderá parecer aleatória, mas os valores ainda garantirão a exclusividade. Os números também incrementam quando você executa uma implantação de teste.

A lista a seguir é um exemplo de onde os nomes personalizados são aplicados. Ela não deve ser considerada uma lista definitiva.

Tabela 6-2. Exemplo de lista de recursos aos quais nomes personalizados são aplicados

| Grupo de Recursos | Tipos de Recursos |
|------------------------|--|
| Máquinas virtuais | <ul style="list-style-type: none"> ■ Cloud.Machine ■ Cloud.vSphere.Machine ■ Cloud.AWS.EC2.Instance ■ Cloud.GCP.Machine ■ Cloud.Azure.Machine |
| Balanceadores de carga | <ul style="list-style-type: none"> ■ Cloud.LoadBalancer ■ Cloud.NSX.LoadBalancer |
| Redes | <ul style="list-style-type: none"> ■ Cloud.Network ■ Cloud.vSphere.Network ■ Cloud.NSX.Network |
| Grupos de segurança | <ul style="list-style-type: none"> ■ Cloud.SecurityGroup |
| Discos | <ul style="list-style-type: none"> ■ Cloud.Volume ■ Cloud.vSphere.Disk ■ Cloud.AWS.Volume ■ Cloud.GCP.Disk ■ Cloud.Azure.Disk |
| NSX | <ul style="list-style-type: none"> ■ Cloud.NSX.Gateway ■ Cloud.NSX.NAT |
| Microsoft Azure | <ul style="list-style-type: none"> ■ Cloud.Azure.ResourceGroup |

Além dos exemplos fornecidos aqui, você também pode adicionar o nome do usuário, a imagem usada, outras opções internas e cadeias de caracteres simples. À medida que você cria o modelo, são fornecidas dicas relacionadas a possíveis opções.

Lembre-se de que alguns dos valores exibidos são apenas exemplos de caso de uso. Não será possível usá-los letra por letra no seu ambiente. Pense no local onde seriam feitas suas próprias substituições ou a extrapolação dos valores de exemplo a fim de atender às suas necessidades de gerenciamento da infraestrutura em nuvem e implantação.

Pré-requisitos

- Verifique se você conhece a convenção de nomenclatura que deseja usar para implantações de um projeto.
- Este procedimento pressupõe que você tenha ou possa criar um modelo de nuvem simples usado para testar seu nome de prefixo de host personalizado.

Procedimentos

- 1 Selecione **Infraestrutura > Projetos**.
- 2 Selecione um projeto existente ou crie um novo.

- 3 Na guia **Provisionamento**, localize a seção Propriedades personalizadas e crie as propriedades para o código do site e os valores do centro de custos.

É aqui que você substitui os valores vistos aqui por aqueles pertinentes ao seu ambiente.

Custom Properties

Specify the custom properties that should be added to all requests in this project. ⓘ

| Define custom properties | Name | Value |
|--------------------------|------------|-------------|
| | siteCode | BGL |
| | costCenter | IT-research |

Custom Naming

Specify the naming template to be used for machines provisioned in this project.

Template `${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}` ⓘ

- Crie uma propriedade personalizada com o nome **siteCode** e o valor **BGL**.
 - Adicione outra propriedade personalizada com o nome **costCenter** e o valor **IT-research**.
- 4 Localize a seção Nomenclatura Personalizada e adicione o modelo a seguir.

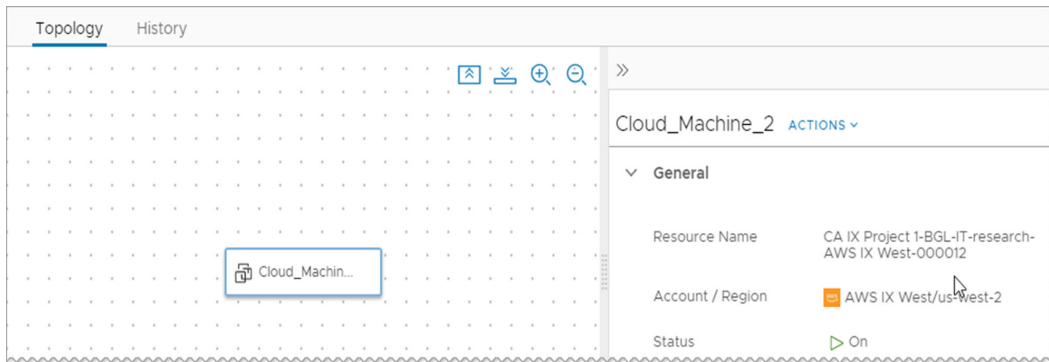
```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

É possível copiar na cadeia de caracteres, mas, se este for o seu primeiro modelo de nomenclatura, considere usar o texto de dica e selecionar rapidamente à medida que você cria o modelo.

- 5 Implante um modelo de nuvem associado ao projeto para verificar se o nome personalizado foi aplicado ao recurso.
- Clique na guia **Projetar** e, em seguida, clique em um modelo de nuvem associado ao projeto.
 - Implante o modelo de nuvem.

A página **Implantações** é aberta mostrando sua implantação em andamento.

- c Quando a implantação estiver concluída, clique no nome dela.
- d Na guia **Topologia**, observe que o nome personalizado é o nome do recurso no painel direito.



- 6 Se tiver implantado um modelo de nuvem de teste para verificar a convenção de nomenclatura, você poderá excluir a implantação.

Próximo passo

Crie modelos de nomenclatura personalizados para seus outros projetos.

Como adicionar o recurso SaltStack Config em designs do Cloud Assembly

Se você tiver integrado o SaltStack Config ao vRealize Automation, poderá aplicar o recurso SaltStack Config para instalar os subordinados em máquinas virtuais nas suas implantações. Depois que o subordinado for implantado, você poderá usar os poderosos recursos de gerenciamento de configuração, correção de desvios e gerenciamento de estado do SaltStack Config para gerenciar seus recursos.

Subordinados são agentes que executam o serviço sal-minion. O serviço assina trabalhos publicados por um mestre Salt, que é um servidor que executa o serviço salt-master. Quando um trabalho específico se aplica a um subordinado, este o executa.

Você pode usar o recurso SaltStack Config para implantar subordinados e aplicar arquivos de estado ao implantar máquinas Linux e Windows. Para adicionar ou atualizar subordinados e arquivos de estado em implantações existentes, você pode executar a ação de dia 2 **Aplicar Configuração do Salt**. Essa ação usa a propriedade `saltConfiguration`. Para obter mais informações sobre a ação de dia 2, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Se você usou a propriedade `saltConfiguration` para implantar os subordinados e arquivos de estado como uma ação de dia 0, considere atualizar seus modelos de nuvem para usar o recurso SaltStack Config. A propriedade `saltConfiguration` será suspensa em uma versão futura e será substituída pelo recurso SaltStack Config, juntamente com uma ação de dia 2 alternativa.

Observação A propriedade `saltConfiguration` e o recurso SaltStack Config têm suporte no mesmo modelo de nuvem, mas não para o mesmo recurso.

Por exemplo, você pode criar um modelo de nuvem com duas máquinas. A primeira máquina está conectada a um recurso SaltStack Config. A segunda máquina não está conectada a um recurso SaltStack Config e também não tem uma configuração Salt aplicada a ela. Depois de implantar o modelo de nuvem, você apenas pode realizar uma operação de Dia 2 na segunda máquina para aplicar uma configuração do Salt. A ação de Dia 2 na máquina com o recurso SaltStack Config será desativada

Antes de começar

- 1 Verifique se você instalou o SaltStack Config e configurou a integração. Consulte [Criar uma integração com o SaltStack Config no vRealize Automation](#).
- 2 No SaltStack Config, verifique se a resolução de nomes FQDN do subordinado para o mestre está funcionando.
 - a Para verificar o FQDN no mestre Salt no SaltStack Config, selecione **Subordinados > Todos os Subordinados**.
 - b Filtre a coluna **ID do subordinado** em busca do valor **saltmaster**.
 - c Clique em **saltmaster** para ver os detalhes.
 - d Verifique se o valor do FQDN está correto.
- 3 Se você estiver implantando subordinados em uma máquina Linux, verifique se as imagens no vSphere que você pretende implantar com um subordinado Salt têm recursos de SSH ativados. O SSH é usado para acessar a máquina remotamente e implantar o subordinado.
- 4 Se você estiver implantando subordinados em uma máquina Windows, consulte [Como implantar subordinados usando a API em um ambiente Windows](#).
- 5 Verifique se você pode atribuir endereços IP às máquinas implantadas.

O SaltStack Config requer que as máquinas tenham endereços IP. Use os endereços IP para o intervalo de CIDR de IPs públicos para o SDDC (centro de dados definido por software) no qual seu mestre Salt está localizado.
- 6 Verifique se o modelo de nuvem ao qual você está adicionando o subordinado é implantável antes de adicionar as propriedades de recursos SaltStack Config.
- 7 Verifique se você tem as seguintes funções de serviço:
 - a Administrador do Cloud Assembly
 - b Usuário do Cloud Assembly

c Administrador do Service Broker

Essas funções de serviço são necessárias para usar o recurso do SaltStack Config.

Adicionar o recurso SaltStack Config ao modelo de nuvem

Como desenvolvedor de modelo de nuvem, você pode adicionar propriedades ao YAML que instala o subordinado do SaltStack Config ao implantar o modelo.

As propriedades principais que você adiciona ao modelo incluem acesso remoto para a máquina que você deseja implantar e propriedades de configuração para o recurso SaltStack Config. O procedimento inclui apenas as propriedades selecionadas. O YAML inclui outras propriedades de recursos do SaltStack Config que não são usadas nesse exemplo. Para obter mais informações, revise o esquema.

Embora este exemplo mostre como adicionar o nome de usuário e a senha para as propriedades de acesso remoto, você pode configurar uma propriedade secreta e adicioná-la ao modelo. Para obter um exemplo, consulte [Propriedades secretas do Cloud Assembly](#).

Procedimentos

- 1 No Cloud Assembly, selecione **Design > Modelos de Nuvem**.
- 2 Abra um modelo existente.
- 3 Localize o recurso **SaltStack Config** e arraste-o até a tela.
- 4 Anexe o recurso **SaltStack Config** à máquina na qual o subordinado será instalado.
- 5 No painel de código, adicione propriedades ao recurso `Cloud_SaltStack_1`.

Não é necessário incluir todas as propriedades possíveis. Os valores utilizados neste exemplo são explicados na tabela.

```
Cloud_SaltStack_1:
  type: Cloud.SaltStack
  properties:
    masterId: saltstack_enterprise_installer
    hosts:
      - ${resource.Cloud_vSphere_Machine_1.id}
    saltEnvironment: sse
    stateFiles:
      - /doe.sls
    variables:
      user: joe
```

Descrição das propriedades `Cloud_SaltStack_1` usadas neste exemplo.

| Propriedade | Descrição |
|-----------------|--|
| masterId | No esquema de exemplo, o valor de <code>masterId</code> é <code>saltstack_enterprise_installer</code> . Você pode ter IDs de mestre definidos no SaltStack Config, em Administração > Chaves do Mestre . |
| hosts | O valor de <code>hosts</code> é o ID da máquina ou cluster de máquinas em que você deseja instalar o subordinado. Por padrão, o nome da máquina é transmitido como o ID do subordinado no SaltStack Config. É recomendável que você escolha nomes de máquina com 15 caracteres ou menos, especialmente se estiver implantando subordinados no Windows. O Windows não permite nomes de host que excedam 15 caracteres. Se quiser definir uma convenção de nomenclatura personalizada para as máquinas que deseja implantar, consulte Nomenclatura personalizada para recursos implantados no Cloud Assembly . |
| saltEnvironment | Neste exemplo, <code>sse</code> é uma localização para os arquivos de estado. Você pode ter seus arquivos de estado em outras localizações do servidor de arquivos no SaltStack Config, em Configuração > Servidor de Arquivos . |
| stateFiles | Neste exemplo, <code>doe.sls</code> é um arquivo de estado fornecido no diretório do servidor de arquivos especificado como <code>saltEnvironment</code> . |
| variables | As variáveis são os valores usados pelo arquivo de estado. Neste exemplo, <code>doe.sls</code> aceita um valor <code>user</code> . |

6 Adicione propriedades `remoteAccess` à máquina que hospeda o subordinado Salt.

O valor da chave `authentication` deve ser `usernamePassword` OU `generatedPublicPrivateKey`. Não há suporte para `publicPrivateKey`.

```
remoteAccess:
  authentication: usernamePassword
  username: adminUser
  password: adminPassword
```

7 Verifique se o YAML inclui propriedades semelhantes ao exemplo a seguir.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: adminUser
        password: adminPassword
```

```

Cloud_SaltStack_1:
  type: Cloud.SaltStack
  properties:
    masterId: saltstack_enterprise_installer
    hosts:
      - ${resource.Cloud_vSphere_Machine_1.id}
    saltEnvironment: sse
    stateFiles:
      - /doe.sls
    variables:
      user: joe

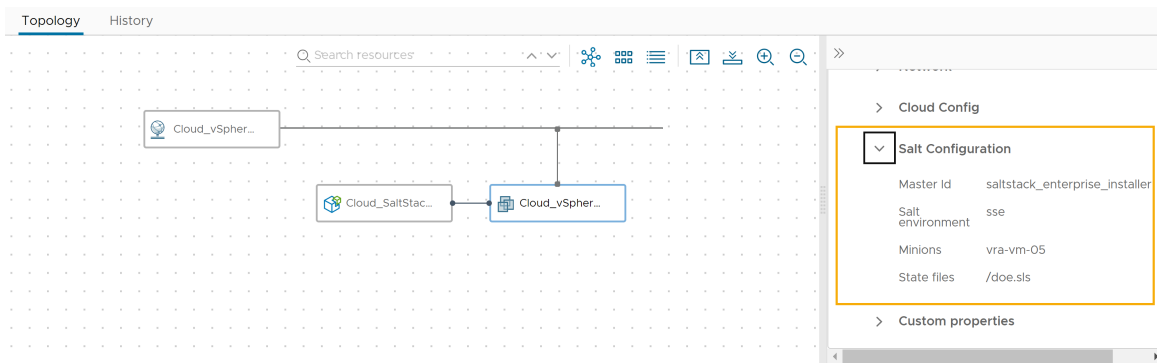
```

8 Teste e implante o modelo de nuvem.

Se a implantação do seu subordinado falhar, consulte [Solucionando problemas com implantações de subordinados](#).

9 Verifique as propriedades de Configuração do Salt da máquina implantada.

- Selecione **Implantações > Implantações** e abra os detalhes da implantação.
- Na guia **Topologia**, clique na máquina e expanda as propriedades no painel direito.



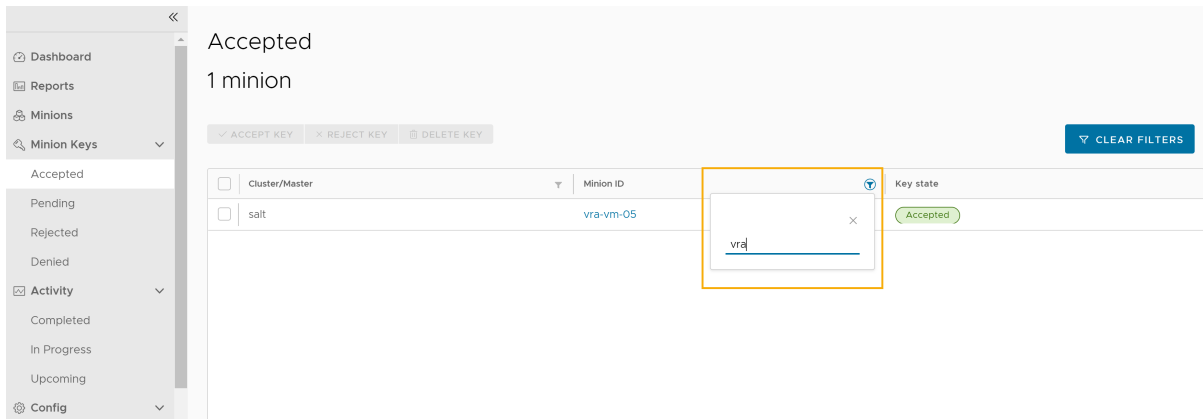
Verificar o subordinado no SaltStack Config

Depois de instalar o subordinado na máquina virtual, localize-o e execute quaisquer trabalhos ou comandos no recurso.

Procedimentos

- Para abrir o SaltStack Config, clique no menu Aplicativos no canto superior direito e clique em **Console de Serviços de Nuvem**.
- Clique no bloco de serviço **SaltStack Config**.
- No SaltStack Config, expanda **Chaves de Subordinados** e clique em **Aceito**.
- Na coluna **ID do Subordinado**, clique no ícone de filtro e digite o nome do subordinado.

O nome do subordinado é padronizado como o nome do host da máquina virtual. Neste exemplo, o ID do subordinado é vra-vm-05.



- 5 Para exibir os detalhes, clique no nome do subordinado.

Você pode executar trabalhos ou comandos no subordinado. Por exemplo, Uso de Disco de Exemplo. Esse trabalho retorna estatísticas de uso de disco para um subordinado.

vra-vm-05

Presence: Present

Key state: Accepted

Master: salt

Targets: [All Minions](#) , [Linux](#) , [Ubuntu](#)

IPv4: 10.196.194.192, 127.0.0.1

OS: Ubuntu16.04

Salt Version: 3002.7

[RUN JOB](#) [RUN COMMAND](#)

Grains Activity

| | |
|-----------------|--|
| biosreleasedate | 12/12/2018 |
| biosversion | 6.00 |
| > cpu_flags | -- |
| cpu_model | Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz |
| cpuarch | x86_64 |
| cwd | / |
| > disks | -- |

Solucionando problemas com implantações de subordinados

Leia sobre alguns erros comuns que os usuários enfrentam ao implantar subordinados Salt usando o recurso SaltStack Config ou a propriedade `saltConfiguration`.

Inicialização do host atrasada

Se serviços Windows ou Linux no host não estiverem prontos após a implantação do modelo de nuvem, você poderá receber um erro "Falha na execução do arquivo de estado e/ou implantação do subordinado" no Cloud Assembly.

Para resolver esse erro, faça upgrade do Master Plugin para a versão estável mais recente. Após o upgrade, você pode ativar uma definição de configuração no `/etc/salt/master.d/raas.conf` que dá tempo para que os serviços do Windows e Linux se tornem ativos antes de implantar o subordinado Salt.

Antes de fazer upgrade para a versão mais recente do Master Plugin, conclua essas etapas para atrasar a inicialização do host:

- 1 Verifique a guia **Histórico** na página de detalhes da implantação.
- 2 Se a mensagem de erro indicar "Falha na execução do arquivo de estado e/ou implantação do subordinado", copie o ID do trabalho (JID) e abra o SaltStack Config.
- 3 No SaltStack Config, selecione **Atividade > Concluída** para abrir trabalhos concluídos.
- 4 Na coluna **JID**, clique no ícone de filtro e digite o JID.
- 5 Clique no JID para revisar a página de resultados do trabalho.
- 6 Clique na guia **Bruta** para ver a saída bruta do trabalho.

Windows

Se a última linha na saída bruta do trabalho contiver "Falha ao se conectar ao host: tempo limite esgotado", você deverá adicionar esta definição de configuração a `/etc/salt/master.d/raas.conf` para atrasar a inicialização em 180 segundos:

```
sseapi_win_minion_deploy_delay: 180
```

Linux

Se a última linha da saída bruta para o trabalho contiver "O host remoto não pode ser acessado usando as credenciais fornecidas", você deverá adicionar esta definição de configuração a `/etc/salt/master.d/raas.conf` para atrasar a inicialização em 90 segundos:

```
sseapi_linux_minion_deploy_delay: 90
```

- 7 Reinicie o serviço do mestre Salt:

```
systemctl restart salt-master
```

- 8 Implante seu modelo de nuvem.

Se a implantação não foi bem-sucedida, você poderá aumentar o parâmetro de atraso e reimplantar o modelo.

O que fazer em seguida

Para usar os recursos do SaltStack Config para gerenciar seus recursos, consulte a [Documentação do SaltStack Config](#).

Configurações do Terraform no Cloud Assembly

Você pode incorporar as configurações do Terraform como um recurso nos seus modelos de nuvem do Cloud Assembly.

Preparando um ambiente de tempo de execução do Terraform do Cloud Assembly

Projetos que incluem configurações do Terraform exigem acesso a um ambiente de execução do Terraform que você integra com o produto Cloud Assembly no local.

Como adicionar um tempo de execução do Terraform

O ambiente de tempo de execução consiste em um cluster Kubernetes que executa comandos da CLI do Terraform para executar as operações solicitadas. Além disso, o tempo de execução coleta logs e retorna os resultados de comandos da CLI do Terraform.


O produto vRealize Automation no local exige que os usuários configurem seu próprio cluster Kubernetes de tempo de execução do Terraform. Só há suporte para um tempo de execução do Terraform por organização. Todas as implantações do Terraform para essa organização usam o mesmo tempo de execução.

- 1 Verifique se você tem um cluster Kubernetes para executar a CLI do Terraform.
 - Todos os usuários podem fornecer um arquivo Kubeconfig para executar a CLI do Terraform em um cluster Kubernetes não gerenciado.
 - Os usuários de licenças Enterprise têm a opção de executar a CLI do Terraform em um cluster Kubernetes gerenciado pelo vRealize Automation.

No Cloud Assembly, acesse **Infraestrutura > Recursos > Kubernetes** e verifique se você tem um cluster Kubernetes. Consulte [Como trabalhar com o Kubernetes no Cloud Assembly](#) se você precisar adicionar um.
- 2 Se o cluster Kubernetes foi adicionado ou modificado recentemente, aguarde sua coleta de dados ser concluída.

A coleta de dados recupera a lista de namespaces e outras informações e pode levar até 5 minutos, dependendo do provedor.
- 3 Após a conclusão da coleta de dados, acesse **Infraestrutura > Conexões > Integrações > Adicionar Integração** e selecione o cartão **Tempo de Execução do Terraform**.
- 4 Insira configurações.

Figura 6-3. Exemplo de integração de tempo de execução do Terraform



New Integration

Name *

Description

Terraform Runtime Integration

Runtime type *

☒ Managed kubernetes cluster
☐ External kubeconfig

Kubernetes cluster * ⓘ

Kubernetes namespace * ⓘ

Runtime Container Settings

Image ⓘ

CPU request (Millicores)

CPU limit (Millicores)

Memory request (MB)

Memory limit (MB)

| Configuração | Descrição |
|---|--|
| Nome | Dê à integração de tempo de execução um nome exclusivo. |
| Descrição | Explique sua finalidade. |
| Integração do tempo de execução do Terraform: | |
| Tipo de tempo de execução (apenas Enterprise) | Os usuários de licença Enterprise podem selecionar se desejam executar a CLI do Terraform em um cluster Kubernetes gerenciado pelo vRealize Automation ou um cluster Kubernetes não gerenciado. |
| Kubernetes kubeconfig (todos os usuários) | <p>Para um cluster Kubernetes não gerenciado, cole todo o conteúdo do arquivo kubeconfig do cluster externo.</p> <p>Para usar um tempo de execução externo do Kubernetes com um servidor proxy, consulte Como adicionar suporte a proxy.</p> <p>Essa opção está disponível para todos os usuários.</p> |

| Configuração | Descrição |
|--|---|
| Cluster Kubernetes (somente Enterprise) | Para o Kubernetes gerenciado pelo vRealize Automation, selecione o cluster no qual executar a CLI do Terraform. O cluster e seu arquivo kubeconfig devem estar acessíveis. Você pode validar o acesso a kubeconfig com um GET em <code>/cmx/api/resources/k8s/clusters/{clusterId}/kube-config</code> . Essa opção está disponível apenas para licenças Enterprise. |
| Namespace do Kubernetes | Selecione o namespace a ser usado no cluster para a criação de pods que executam a CLI do Terraform. |
| Configurações do contêiner de tempo de execução: | |
| Imagem | Insira o caminho para a imagem de contêiner da versão do Terraform que você deseja executar. Observação O botão VALIDATE não verifica a imagem do contêiner. |
| Solicitação de CPU | Insira a quantidade de CPU para os contêineres em execução. O padrão é para 250 millicores. |
| Limite de CPU | Insira a CPU máxima permitida para os contêineres em execução. O padrão é para 250 millicores. |
| Solicitação de memória | Insira a quantidade de memória para os contêineres em execução. O padrão é 512 MB. |
| Limite de memória | Insira a memória máxima permitida para os contêineres em execução. O padrão é 512 MB. |

5 Clique em **VALIDATE** e ajuste as configurações conforme necessário.

6 Clique em **Adicionar**.

As configurações são armazenadas em cache. Depois de adicionar a integração, você pode modificar as configurações, como o cluster ou o namespace, mas pode levar até 5 minutos para que uma alteração seja detectada e para que a CLI do Terraform seja executada sob as novas configurações.

Solucionando problemas com o tempo de execução do Terraform

Alguns problemas de implantação de configuração do Terraform podem estar relacionados à integração do tempo de execução.

| Problema | Causa | Resolução |
|---|---|---|
| A validação falha com um erro informando que o namespace é inválido. | Você modificou o cluster, mas deixou o namespace anterior na interface do usuário. | Sempre selecione um namespace novamente depois de modificar a seleção do cluster. |
| A lista suspensa de namespaces está vazia ou não lista namespaces recém-adicionados. | A coleta de dados para o cluster não foi concluída. A coleta de dados leva até 5 minutos depois de inserir ou modificar o cluster e até 10 minutos ao inserir ou modificar o namespace. | Para um novo cluster com namespaces existentes, aguarde até 5 minutos para que a coleta de dados seja concluída. Para um novo namespace em um cluster existente, aguarde até 10 minutos para que a coleta de dados seja concluída. Se o problema persistir, remova o cluster e, em seguida, adicione-o novamente em Infraestrutura > Recursos > Kubernetes . |
| Os contêineres da CLI do Terraform estão criados em um cluster anterior, em um namespace anterior ou em configurações de tempo de execução anteriores, mesmo depois que a conta de integração foi atualizada. | O cliente de API do Kubernetes usado pelo vRealize Automation foi armazenado em cache por 5 minutos. | As alterações podem precisar de até 5 minutos para entrar em vigor. |
| A validação ou uma operação de implantação do Terraform falha com um erro informando que o kubeconfig não está disponível. | Às vezes, esses erros ocorrem porque o cluster não está acessível a partir do vRealize Automation. Em outros casos, as credenciais do usuário, os tokens ou os certificados são inválidos. | O erro de kubeconfig pode ocorrer por várias razões e pode exigir um compromisso com o suporte técnico para solução de problemas. |

Como adicionar suporte a proxy

Para que o cluster de tempo de execução externo do Kubernetes se conecte por meio de um servidor proxy, siga estas etapas.

- 1 Faça login no servidor do seu cluster Kubernetes externo.
- 2 Crie uma pasta vazia.
- 3 Na nova pasta, adicione as seguintes linhas a um novo arquivo denominado Dockerfile.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final
ENV https_proxy=protocol://username:password@proxy_host:proxy_port
ENV http_proxy=protocol://username:password@proxy_host:proxy_port
ENV no_proxy=.local,.localdomain,localhost
```

- 4 Modifique os valores de espaço reservado para que as variáveis de ambiente `https_proxy` e `http_proxy` incluam as configurações do servidor proxy que você usa para acessar a Internet.

O *protocolo* será http ou https de acordo com o que o servidor proxy usa, que pode não corresponder ao nome da variável de ambiente `https_proxy` ou `http_proxy`.

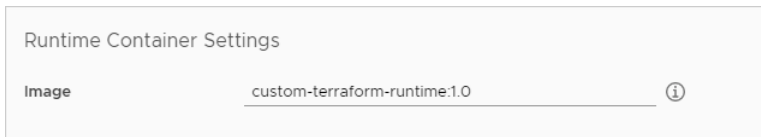
- 5 Salve e feche o Dockerfile.

- Na pasta vazia, execute o seguinte comando. Dependendo dos seus privilégios de conta, poderá ser necessário executar o comando no modo sudo.

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

O comando cria uma imagem local Docker custom-terraform-runtime:1.0.

- Em Cloud Assembly, em **Infraestrutura > Conexões > Integrações**, vá para a sua integração do tempo de execução do Terraform.
- Crie ou edite as configurações do contêiner de tempo de execução para usar a imagem custom-terraform-runtime:1.0:



Tempo de execução do Cloud Assembly Terraform sem acesso à Internet

Os usuários do Cloud Assembly que precisam projetar e executar integrações do Terraform enquanto estão desconectados da Internet podem configurar seu ambiente de execução seguindo este exemplo.

Observação Para obter uma origem para a criação da imagem, a configuração envolve uma breve conexão à Internet. Talvez seja necessário realizar essas etapas fora do site desconectado, se uma conexão temporária não for possível.

Esse processo pressupõe que você tenha [seu próprio Registro Docker](#) e possa acessar seus repositórios sem uma conexão com a Internet.

Criar a imagem de contêiner personalizada

- Crie uma imagem de contêiner personalizada que inclua os binários do plug-in do provedor do Terraform.

O Dockerfile a seguir mostra um exemplo de criação de uma imagem personalizada com o provedor do Terraform GCP.

O download da imagem de base `projects.registry.vmware.com/vra/terraform:latest` no Dockerfile requer acesso à Internet para o registro VMware Harbor em `projects.registry.vmware.com`.

Configurações de firewall ou de proxy podem fazer com que a criação da imagem falhe. Pode ser necessário ativar o acesso a `releases.hashicorp.com` para baixar os binários do plug-in de provedor do Terraform. No entanto, você pode usar seu registro privado para fornecer os binários do plug-in como uma opção.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final

# Create provider plug-in directory
ARG plugins=/tmp/terraform.d/plugin-cache/linux_amd64
```

```
RUN mkdir -m 777 -p $plugins

# Download and unzip all required provider plug-ins from hashicorp to provider directory
RUN cd $plugins \
    && wget -q https://releases.hashicorp.com/terraform-provider-google/3.58.0/terraform-provider-google_3.58.0_linux_amd64.zip \
    && unzip *.zip \
    && rm *.zip

# For "terraform init" configure terraform CLI to use provider plug-in directory and not
download from internet
ENV TF_CLI_ARGS_init="-plugin-dir=$plugins -get-plugins=false"
```

- 2 Crie, marque e envie a imagem do contêiner personalizado ao seu próprio repositório Docker no seu site desconectado.
- 3 No Cloud Assembly no seu site desconectado, em **Infraestrutura > Conexões > Integrações**, vá para a sua integração do tempo de execução do Terraform.
- 4 Crie ou edite as configurações do contêiner de tempo de execução para adicionar seu repositório à imagem de contêiner personalizada. O exemplo de nome de imagem de contêiner personalizada criado é `registry.ourcompany.com/project1/image1:latest`.

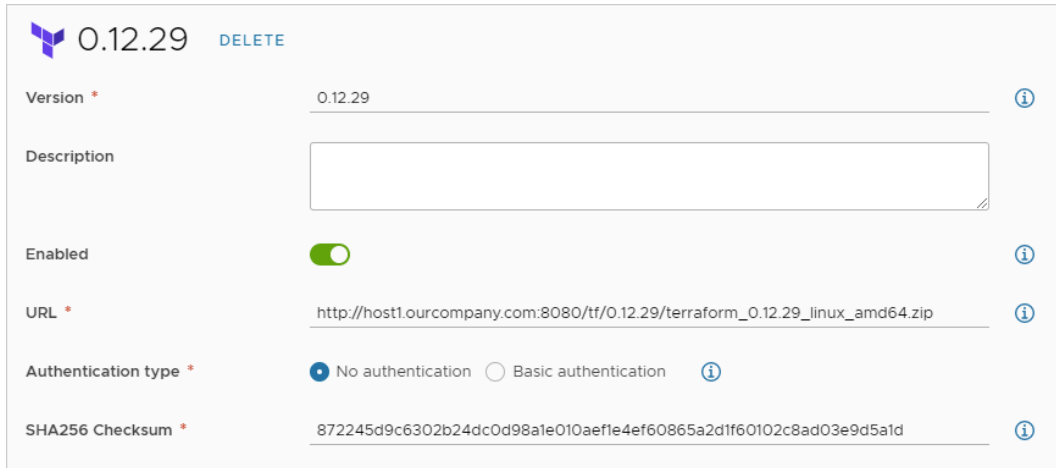
Runtime Container Settings

| | | |
|-------|--|---|
| Image | registry.ourcompany.com/project1/image1:latest | ⓘ |
|-------|--|---|

Hospedar a CLI do Terraform localmente

- 1 Baixe os binários da CLI do Terraform.
- 2 Carregue os binários da CLI do Terraform no seu servidor Web local ou FTP.
- 3 No Cloud Assembly, acesse **Infraestrutura > Configurar > Versões do Terraform**.
- 4 Crie ou edite a versão do Terraform para que ela inclua a URL para os binários da CLI do Terraform hospedados no seu servidor local.
- 5 Se o seu servidor Web ou FTP local exigir autenticação por login, selecione **Autenticação Básica** e insira credenciais de nome de usuário e senha que podem acessar o servidor.

Para alterar o tipo de autenticação, você deve ter a função de administrador de nuvem no Cloud Assembly.



0.12.29 [DELETE](#)

Version * 0.12.29 ⓘ

Description

Enabled ☒ ⓘ

URL * http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip ⓘ

Authentication type * ☒ No authentication ☐ Basic authentication ⓘ

SHA256 Checksum * 872245d9c6302b24dc0d98a1e010aef1e4ef60865a2d1f60102c8ad03e9d5a1d ⓘ

Projetar e implantar configurações do Terraform

Com o tempo de execução em vigor, você pode adicionar arquivos de configuração do Terraform ao Git, projetar modelos de nuvem para eles e implantar.

Para começar, consulte [Preparando para configurações do Terraform no Cloud Assembly](#).

Solução de problemas

Ao implantar, abra a implantação no Cloud Assembly. Na guia Histórico, procure eventos do Terraform e clique em **Mostrar Logs** à direita. Quando seu provedor do Terraform local está funcionando, as seguintes mensagens aparecem no log.

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```

Para um registro mais robusto, você pode editar manualmente o código do modelo de nuvem para adicionar `TF_LOG: DEBUG` conforme mostrado no exemplo a seguir.

```
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      providers:
        - name: google
          # List of available cloud zones: gcp/us-west1
          cloudZone: gcp/us-west1
    environment:
      # Configure terraform CLI debug log settings
      TF_LOG: DEBUG
    terraformVersion: 0.12.29
    configurationSource:
      repositoryId: fc569ef7-f013-4489-9673-6909a2791071
      commitId: 3e00279a843a6711f7857929144164ef399c7421
      sourceDirectory: gcp-simple
```

Criando sua própria imagem de base

Embora a VMware atualize ocasionalmente a imagem de base no `projects.registry.vmware.com/vra/terraform:latest`, essa imagem pode estar desatualizada e conter vulnerabilidades.

Para criar sua própria imagem de base, use o seguinte Dockerfile.

```
FROM alpine:latest as final
RUN apk add --no-cache git wget curl openssh
```

Preparando para configurações do Terraform no Cloud Assembly

Antes de adicionar uma configuração do Terraform a um modelo de Cloud Assembly, configure e integre o repositório de controle de versão.

- 1 [Pré-requisitos](#)
- 2 [Armazenar arquivos de configuração do Terraform em um repositório de controle de versão](#)
- 3 [Ativar mapeamento de zona de nuvem](#)
- 4 [Integre seu repositório com o Cloud Assembly](#)

Pré-requisitos

Para o produto vRealize Automation no local para executar operações do Terraform, você precisa da integração com o tempo de execução do Terraform. Consulte [Preparando um ambiente de tempo de execução do Terraform do Cloud Assembly](#).

Armazenar arquivos de configuração do Terraform em um repositório de controle de versão

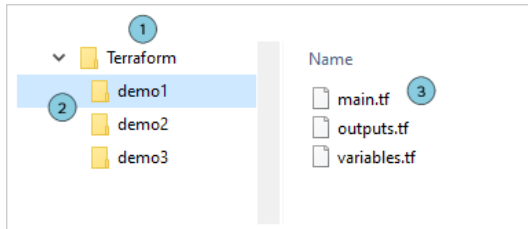
O Cloud Assembly oferece suporte aos seguintes repositórios de controle de versão para configurações do Terraform.

- Nuvem do GitHub, GitHub Enterprise no local
- Nuvem do GitLab, GitLab Enterprise no local
- Bitbucket no local

No seu repositório de controle de versão, crie um diretório padrão com uma camada de subdiretórios, cada um com arquivos de configuração do Terraform. Crie um subdiretório por configuração do Terraform.

- 1 Diretório padrão
- 2 Camada única de subdiretório
- 3 Arquivos de configuração do Terraform pronta para implantação

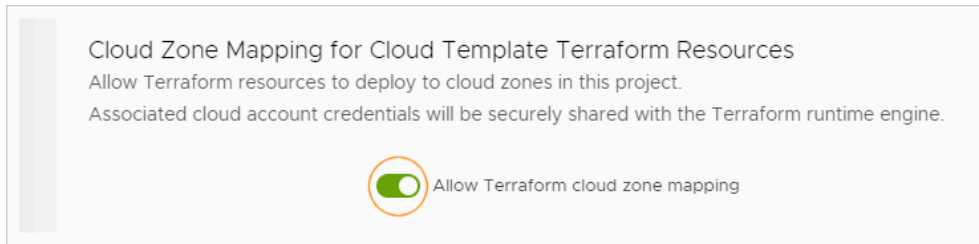
Não inclua um arquivo de estado do Terraform com arquivos de configuração. Se `terraform.tfstate` estiver presente, ocorrerão erros durante a implantação.



Ativar mapeamento de zona de nuvem

Se você espera implantar em uma conta de nuvem, o mecanismo de tempo de execução do Terraform precisa dessas credenciais da zona de nuvem.

Na guia **Provisionamento** do projeto, ative **Permitir mapeamento de zona de nuvem do Terraform**.



Mesmo que as credenciais sejam transmitidas com segurança, para segurança adicional, você deverá deixar a opção desativada se os usuários do projeto não precisarem implantar em uma conta de nuvem.

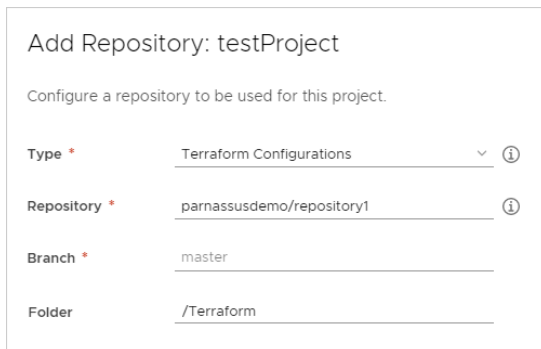
Integre seu repositório com o Cloud Assembly

No Cloud Assembly, acesse **Infraestrutura > Conexões > Integrações**.

Adicione uma integração ao tipo de oferta de repositório em que você armazenou as configurações do Terraform: GitHub, GitLab ou Bitbucket.

Quando você adicionar o projeto à integração, selecione o tipo de **Configurações do Terraform** e identifique o repositório e a ramificação.

A **Pasta** é o diretório padrão da estrutura anterior.



Projetando para configurações do Terraform no Cloud Assembly

Com os arquivos de configuração do repositório e do Terraform implantados, você pode criar um modelo do Cloud Assembly para eles.

- 1 [Pré-requisitos](#)
- 2 [Ativar versões de tempo de execução do Terraform](#)
- 3 [Adicionar recursos do Terraform ao design](#)
- 4 [Implantar o modelo de nuvem](#)

Pré-requisitos

Configure e integre seu repositório de controle de versão. Consulte [Preparando para configurações do Terraform no Cloud Assembly](#).

Ativar versões de tempo de execução do Terraform

Você pode definir as versões de tempo de execução do Terraform disponíveis para os usuários ao implantar as configurações do Terraform. Observe que as configurações do Terraform também podem incluir restrições de versão com codificação interna.

Para criar a lista de versões permitidas, acesse **Infraestrutura > Configurar > Versões do Terraform**.

Adicionar recursos do Terraform ao design

Crie seu modelo de nuvem que inclui as configurações do Terraform.

- 1 No Cloud Assembly, acesse **Projetar > Modelos de Nuvem** e clique em **Novo a partir de > Terraform**.

O assistente de configuração do Terraform é exibido.

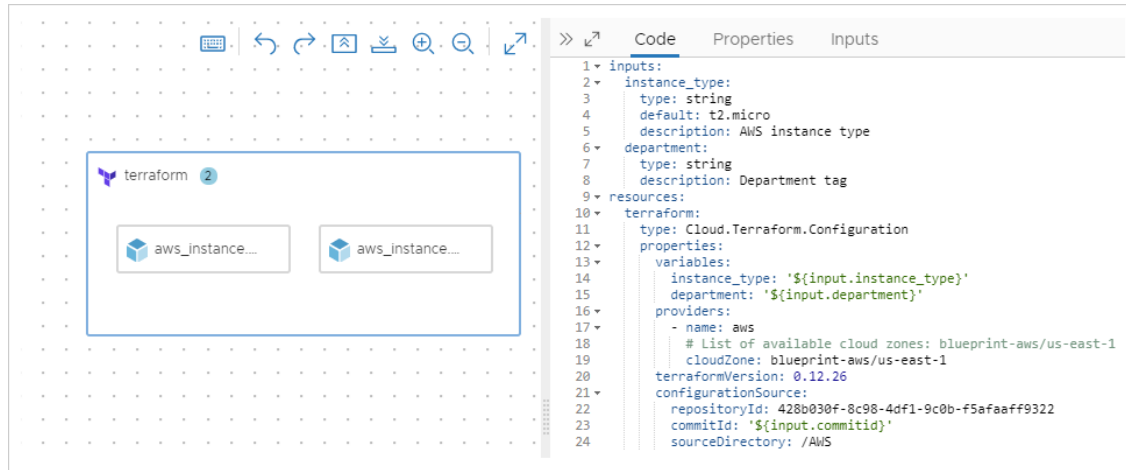
- 2 Siga os prompts.

| Página do assistente | Configuração | Valor |
|------------------------|--------------|---|
| Novo modelo de nuvem | Nome | Dê ao design um nome de identificação. |
| | Descrição | Explique para que serve o design. |
| | Projeto | Selecione o design que inclui a integração do repositório onde a configuração do Terraform está armazenada. |
| Origem de configuração | Repositório | Selecione o repositório integrado no qual você armazenou a configuração do Terraform. |

| Página do assistente | Configuração | Valor |
|------------------------|---------------------|---|
| | Confirmar | <p>Selecione uma confirmação do repositório ou deixe a entrada em branco para usar a configuração do Terraform do cabeçalho do repositório.</p> <p>Limitação do Bitbucket – O número de confirmações selecionáveis pode estar truncado em decorrência da configuração do servidor do repositório do bitbucket.</p> |
| | Diretório de origem | Selecione um subdiretório na estrutura do repositório que você criou. Os subdiretórios de exemplo mostrados na configuração anterior eram demo1, demo2 e demo3. |
| Finalizar configuração | Repositório | Verifique a seleção correta do repositório. |
| | Diretório de origem | Verifique a seleção correta do diretório. |
| | Versão do Terraform | Selecione a versão de tempo de execução do Terraform a ser executada ao implantar a configuração do Terraform. |
| | Provedores | <p>Se a configuração do Terraform incluir bloco de provedor, verifique o provedor e a zona de nuvem em que esse modelo de nuvem será implantado.</p> <p>Não ter um provedor não é problema. Depois de concluir o assistente, basta editar o provedor e a zona de nuvem nas propriedades do modelo para adicionar ou alterar o destino de implantação.</p> |
| | Variáveis | Selecione valores confidenciais para criptografia, como senhas. |
| | Saídas | Verifique as saídas da configuração do Terraform, que são convertidas em expressões que o seu código de design pode fazer referência adicional. |

3 Clique em **Criar**.

O recurso do Terraform aparece na tela do modelo de nuvem, com o código Cloud Assembly que reflete a configuração do Terraform para implantação.



Se desejar, você poderá adicionar outros recursos do Cloud Assembly ao modelo de nuvem para combinar o código do Terraform e que não são do Terraform em um design híbrido.

Observação A atualização das configurações do Terraform no repositório não sincroniza as alterações no seu modelo de nuvem. A sincronização automática pode introduzir riscos de segurança, como variáveis sigilosas adicionadas recentemente.

Para capturar as alterações de configuração do Terraform, execute novamente o assistente, escolha a nova confirmação e identifique as novas variáveis sigilosas.

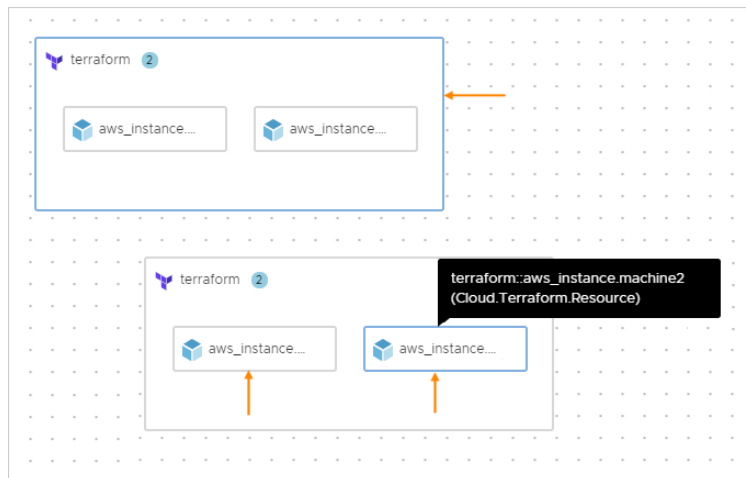
Implantar o modelo de nuvem

Quando você implanta o modelo de nuvem, a guia **Histórico** de implantações permite que você expanda um evento, como uma fase de alocar ou criar, para inspecionar um log de mensagens da CLI do Terraform.

Aprovações — Além das fases esperadas do Terraform, como PLAN, ALLOCATE ou CREATE, o Cloud Assembly introduz o controle por meio de uma fase de aprovação. Consulte [Como configurar políticas de aprovação do Service Broker](#) para obter mais informações sobre solicitações de aprovação.

| Timestamp | Status | Resource type | Resource name | Details |
|---|--------------------------|--------------------------------|---------------|--|
| Aug 3, 202... | PLAN_FINISHED | Cloud.Terraform.Configurati... | terraform | Creating 2 Terraform resources, updating 0 Terraform resources, deleting 0 Terraform resources |
| Aug 3, 202... | PLAN_IN_PROGRESS | Cloud.Terraform.Configurati... | terraform | Hide Logs |
| <pre> 2:24:23 PM * provider.random: version = "~> 2.3" 2:24:23 PM 2:24:23 PM Terraform has been successfully initialized! 2:24:28 PM Refreshing Terraform state in-memory prior to plan... 2:24:28 PM The refreshed state will be used to calculate this plan, but will not be 2:24:28 PM persisted to local or remote state storage. </pre> | | | | |
| Aug 3, 202... | INITIALIZATION_FINISH... | | | |
| Aug 3, 202... | INITIALIZATION_IN_PRO... | | | |

Após a implantação, você verá um recurso externo que representa o componente geral do Terraform, com os recursos filhos dentro, para os componentes separados que o Terraform criou. O recurso pai do Terraform controla o ciclo de vida dos recursos filhos.



Usando uma propriedade secreta do Cloud Assembly em uma configuração do Terraform

É possível aplicar valores secretos e criptografados às configurações do Terraform que você adiciona aos designs de modelo de nuvem do Cloud Assembly.

- 1 No seu repositório git, adicione um arquivo de origem de configuração do Terraform que faz referência às propriedades secretas como variáveis.

Neste exemplo de fonte de configuração do Terraform, as chaves de API e de aplicativo são as variáveis secretas.

```

variable "datadog_api_key" {
  description = "Datadog API Key"
}

```

```

variable "datadog_app_key" {
  description = "Datadog App Key"
}
provider "datadog" {
  api_key = "${var.datadog_api_key}"
  app_key = "${var.datadog_app_key}"
}

# Create a new monitor
resource "datadog_monitor" "default" {
  # ...
}

# Create a new timeboard
resource "datadog_timeboard" "default" {
  # ...
}

```

- 2 No Cloud Assembly, vá para **Infraestrutura > Administração > Segredos** e insira seus valores de propriedade secreta.

Adicione nomes secretos e valores correspondentes. Para os nomes, é mais fácil simplesmente inserir o mesmo nome que o nome da variável da origem do Terraform.

Se necessário, consulte [Propriedades secretas do Cloud Assembly](#) para obter mais detalhes.

| Secrets | | | |
|------------------------------|-----------------|-----------|-------|
| + NEW SECRET | | | |
| | Name | Project | Value |
| ⋮ | datadog_api_key | Terraform | ***** |
| ⋮ | datadog_app_key | Terraform | ***** |

- 3 No Cloud Assembly, importe a configuração do Terraform para uso em um modelo de nuvem.

Acesse **Design > Modelos de Nuvem** e clique em **Novo a Partir de > Terraform**.

Observação Mesmo que as variáveis apareçam para seleção na última página do assistente, você não precisa definir as variáveis secretas como confidenciais. As variáveis secretas do Cloud Assembly já serão criptografadas e não precisarão da criptografia aplicada pelo assistente.

Se necessário, consulte [Projetando para configurações do Terraform no Cloud Assembly](#) para obter mais detalhes.

O modelo de nuvem de exemplo deve ser semelhante ao seguinte código:

```

inputs:
  datadog_api_key:
    type: string
    description: Datadog API Key
  datadog_app_key:

```

```

type: string
description: Datadog App Key
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      variables:
        datadog_api_key: '${input.datadog_api_key}'
        datadog_app_key: '${input.datadog_app_key}'
      providers: []
      terraformVersion: 0.12.29
      configurationSource:
        repositoryId: 0fbf8f5e-54e1-4da3-9508-2b701gf25f51
        commitId: ed12424b249aa50439kr1c268942a4616bd751b6
        sourceDirectory: datadog

```

- 4 No editor de códigos, para os valores secretos, altere manualmente `input` para `secret` conforme mostrado.

```

terraform:
  type: Cloud.Terraform.Configuration
  properties:
    variables:
      datadog_api_key: '${secret.datadog_api_key}'
      datadog_app_key: '${secret.datadog_app_key}'

```

- 5 Na seção `inputs`: do código, remova as entradas que foram substituídas pelas vinculações para propriedades secretas.

Saiba mais sobre as configurações do Terraform no vRealize Automation

Esteja ciente de determinadas limitações e resolução de problemas quando incorporar configurações do Terraform como um recurso no vRealize Automation.

Limitações para configurações do Terraform

- Ao validar um projeto com as configurações do Terraform, o botão TEST verifica a sintaxe Cloud Assembly, mas não a sintaxe do código Terraform nativo.
Além disso, o botão TEST não valida IDs de confirmação associados a configurações do Terraform.
- Para um modelo de nuvem que inclui configurações do Terraform, clonar o modelo para um projeto diferente requer a seguinte solução alternativa.
 - a No novo projeto, na guia **Integrações**, copie o `repositoryId` para a sua integração.
 - b Abra o modelo de clone. No editor de código, substitua `repositoryId` pelo valor que você copiou.

- No repositório de controle de versão, não inclua um arquivo de estado do Terraform com arquivos de configuração. Se `terraform.tfstate` estiver presente, ocorrerão erros durante a implantação.

Ações de dia 2 com suporte para o recurso Terraform principal

Para o recurso Terraform principal, você pode visualizar ou atualizar o arquivo de estado do Terraform. Para obter mais informações sobre as ações de arquivo de estado, consulte a lista abrangente de ações em [Quais ações posso executar nas implantações do Cloud Assembly](#).

Ações de dia 2 com suporte para recursos herdeiros

Depois de implantar as configurações do Terraform, pode levar até 20 minutos para que uma ação de dia 2 fique disponível em recursos herdeiros.

Para recursos herdeiros em uma configuração do Terraform, apenas o seguinte subconjunto de ações de dia 2 tem suporte. Para obter detalhes sobre as ações, procure-as na lista abrangente de ações em [Quais ações posso executar nas implantações do Cloud Assembly](#).

| Provedor | Tipo de recurso do Terraform | Ações de dia 2 com suporte |
|----------|------------------------------|----------------------------|
| AWS | aws_instance | Ligar |
| | | Desligar |
| | | Reinicializar |
| | | Redefinir |
| Azure | azurerm_virtual_machine | Ligar |
| | | Desligar |
| | | Reiniciar |
| | | Suspender |
| vSphere | vsphere_virtual_machine | Ligar |
| | | Desligar |
| | | Reinicializar |
| | | Redefinir |
| | | Desligar |
| | | Suspender |
| | | Criar snapshot |
| | | Excluir instantâneo |
| GCP | google_compute_instance | Reverter Snapshot |
| | | Ligar |

| Provedor | Tipo de recurso do Terraform | Ações de dia 2 com suporte |
|----------|------------------------------|----------------------------|
| | | Desligar |
| | | Criar snapshot |
| | | Excluir instantâneo |

Solução de problemas de disponibilidade de ações de dia 2

Ações de dia 2 prontas para uso (OOTB) que estão ausentes ou desativadas podem exigir solução de problemas.

| Problema | Causa | Resolução |
|--|--|---|
| Um recurso do Terraform não tem uma ação esperada de dia 2 OOTB no menu Ações. | A ação pode não ser compatível com o provedor e o tipo de recurso, conforme mencionado na lista anterior. Como alternativa, a ação pode precisar de até 20 minutos para aparecer devido à temporização da descoberta de recursos e do cache de recursos. | Verifique o provedor e o tipo de recurso no projeto. Aguarde até 20 minutos para que a coleta de dados seja concluída. |
| Um recurso do Terraform não tem uma ação esperada de dia 2 mesmo após os 20 minutos para a coleta de dados. | Um problema de detecção de recursos está impedindo que a ação seja exibida. Uma maneira de isso acontecer é quando o recurso é criado acidentalmente em uma zona de nuvem fora do projeto. Por exemplo, seu projeto inclui apenas uma conta de nuvem e uma zona de nuvem us-east-1 cloud, mas a configuração do Terraform inclui um bloco de provedor para us-west-1, e você não o alterou no tempo de design. Outra possibilidade é que a coleta de dados não esteja funcionando. | Verifique as zonas de nuvem do projeto em relação às zonas de nuvem no design. Acesse Infraestrutura > Conexões > Contas de nuvem e verifique o status da coleta de dados e a data da última coleta bem-sucedida para a conta de nuvem. |
| Mesmo que não haja problemas óbvios com o estado do recurso e a coleta de dados, uma ação de dia 2 está desativada (cinza). | Ocorrem problemas de tempo e falha de coleta de dados de forma ocasional. | O problema se resolverá sozinho dentro de 20 minutos. |
| A ação de dia 2 incorreta está desativada, uma que deve ser ativada com base no estado do recurso. Por exemplo, Desligar está ativado e Ligar está desativado, mesmo que o recurso tenha sido desligado usando a interface do provedor. | O tempo de coleta de dados pode causar incompatibilidade temporária. Se você alterar o estado de energia fora do vRealize Automation, levará tempo para refletir corretamente a alteração. | Aguarde até 20 minutos. |

Como usar provedores Terraform personalizados no vRealize Automation

Se você quiser usar um provedor Terraform personalizado, siga estas etapas.

No seu repositório de controle de versão do Git, no diretório Terraform que contém main.tf, adicione a seguinte estrutura de subdiretório e seu arquivo ZIP do provedor Terraform personalizado.

```
terraform.d/plugins/<HOSTNAME>/<NAMESPACE>/<TYPE>/terraform-provider-
<TYPE_VERSION_TARGET>.zip
```

Por exemplo, se baixou o [azurerm versão 3.12.0](#), você cria a seguinte estrutura.

```
terraform.d/plugins/registry.terraform.io/hashicorp/azurerm/terraform-provider-
azurerm_3.12.0_linux_amd64.zip
```

Tipos de recursos personalizados para modelos de nuvem do Cloud Assembly

Quando você cria um modelo de nuvem no Cloud Assembly, a paleta de tipos de recursos inclui tipos de recursos para a conta de nuvem e os endpoints compatíveis. Você pode ter casos de uso em que deseja criar modelos de nuvem com base em uma lista expandida de tipos de recursos. Você pode criar tipos de recursos personalizados, adicioná-los à tela de criação e criar modelos de nuvem que atendam às suas necessidades de design e de implantação.

Nome do recurso personalizado e tipo de recurso

O nome do recurso personalizado identifica seu recurso personalizado dentro da paleta de tipo de recurso do modelo de nuvem.

O tipo de um recurso personalizado deve começar com **Custom.** e cada tipo de recurso devem ser exclusivos. Por exemplo, você pode definir `Custom.ADUser` como um tipo de recurso para um recurso personalizado que adiciona usuários do Active Directory. Embora a inclusão de **Custom.** não é validado na caixa de texto. A cadeia de caracteres será adicionada automaticamente se você a remover.

Recursos personalizados de ação de extensibilidade

Com tipos de recursos personalizados, você pode usar ações de extensibilidade em modelos de nuvem para criar aplicativos complexos. Por exemplo, você pode usar a integração nativa das ações de extensibilidade com a Amazon Web Services e o Microsoft Azure para fácil integração com os respectivos serviços. Você pode criar recursos personalizados de ação de extensibilidade clicando na opção **Baseado em** no editor de recursos personalizados e selecionando **Esquema definido pelo usuário do ABX**.

Ações de ciclo de vida para recursos personalizados de ação de extensibilidade

Ao usar uma ação de extensibilidade para seu recurso personalizado, você pode definir as seguintes ações de ciclo de vida:

- **Criar:** essa ação de extensibilidade é chamada quando uma implantação é iniciada.

- **Ler:** essa ação de extensibilidade é usada para recuperar o estado mais recente do recurso implantado.
- **Atualizar:** essa ação de extensibilidade é chamada quando uma propriedade de modelo de nuvem é atualizada. Essa ação é disparada somente quando uma propriedade não está marcada com `recreateOnUpdate`.
- **Destruir:** essa ação de extensibilidade é chamada quando uma implantação é excluída.

Essas ações de ciclo de vida podem ser selecionadas manualmente em suas ações de extensibilidade existentes ou geradas automaticamente selecionando **Gerar Ações**. Ao selecionar **Gerar Ações**, você deve especificar o projeto no qual a nova ação de extensibilidade será gerada.

Observação Você pode editar as ações de extensibilidade associadas às suas ações de ciclo de vida clicando na opção **Abrir** ao lado da ação específica.

Recursos personalizados do vRealize Orchestrator

Cada recurso personalizado do vRealize Orchestrator baseia-se em um tipo de inventário de SDK e é criado por um fluxo de trabalho do vRealize Orchestrator, que tem uma saída que é uma instância do seu tipo de SDK desejado. Não há suporte para tipos primitivos, como `Properties`, `Date`, `string` e `number`, para a criação de tipos de recursos personalizados.

Observação Os tipos de objeto SDK podem ser diferenciados de outros tipos de propriedade pelos dois pontos (":") usados para separar o nome de plug-in e o nome do tipo. Por exemplo, `AD:UserGroup` é um tipo de objeto SDK usado para gerenciar grupos de usuários do Active Directory.

Você pode usar os fluxos de trabalho internos no vRealize Orchestrator ou pode criar seus próprios fluxos de trabalho. Usar o vRealize Orchestrator para criar fluxos de trabalho de qualquer coisa como serviço/XaaS significa que você pode criar um modelo de nuvem que adiciona um usuário do Active Directory a máquinas no momento da implantação ou adicionar um balanceador de carga F5 personalizado a uma implantação. Você pode criar recursos personalizados do vRealize Orchestrator clicando na opção **Baseado em** no editor de recursos personalizados e selecionando **Inventário do vRO**.

Tipo externo de recurso personalizado do vRealize Orchestrator

A propriedade de tipo externo define o tipo do seu recurso personalizado do vRealize Orchestrator. Quando você seleciona um fluxo de trabalho de criação como o tipo de recurso personalizado no Cloud Assembly, a lista suspensa de tipos externos é exibida abaixo dele. A lista suspensa inclui propriedades de tipo externo, que são selecionadas entre os parâmetros de saída do fluxo de trabalho do vRealize Orchestrator. As propriedades de saída do fluxo de trabalho selecionadas incluídas no menu suspenso devem ser tipos de objeto SDK que não são da matriz, como `VC:VirtualMachine` OU `AD:UserGroup`.

Observação Ao criar fluxos de trabalho personalizados que usam o plug-in de tipo dinâmico, verifique se as suas variáveis são criadas usando o método `DynamicTypesManager.getObject()`.

Ao definir seus tipos de recursos personalizados, você também define o escopo da disponibilidade do tipo externo selecionado. O tipo externo selecionado pode:

- Ser compartilhado entre projetos.
- Estar disponível apenas para o projeto selecionado.

Você só pode ter um tipo de recurso personalizado com um valor de tipo externo específico por escopo definido. Por exemplo, se você criar um recurso personalizado no seu projeto, que usa `VC:VirtualMachine` como um tipo externo, não será possível criar outro recurso personalizado para o mesmo projeto que usa o mesmo tipo externo. Você também não pode criar dois recursos personalizados compartilhados que usam o mesmo tipo externo.

Validação de ação de ciclo de vida do vRealize Orchestrator

Quando você adiciona fluxos de trabalho Criar, Excluir e Atualizar como ações de ciclo de vida ao seu recurso personalizado, o Cloud Assembly valida se os fluxos de trabalho selecionados têm definições de propriedade de entrada e saída corretas.

- O fluxo de trabalho Criar deve ter um parâmetro de saída que seja um tipo de objeto SDK, como `SSH:Host` OU `SQL:Database`. Se o fluxo de trabalho selecionado não passar na validação, você não poderá adicionar fluxos de trabalho Atualizar ou Excluir ou salvar as alterações no recurso personalizado.
- O fluxo de trabalho Excluir deve ter um parâmetro de entrada que seja um tipo de objeto SDK que corresponda ao tipo externo do recurso personalizado.
- O fluxo de trabalho Atualizar deve ter um parâmetro de entrada e de saída que seja um tipo de objeto SDK que corresponda ao tipo externo do recurso personalizado.

Esquema de propriedades de recursos personalizados

É possível editar e visualizar o esquema de propriedades de recursos personalizados selecionando a guia **Propriedades**. O esquema inclui o nome, o tipo de dados, o tipo de propriedade e, se disponível, a descrição de uma determinada propriedade. O esquema também define se uma propriedade específica é necessária ou opcional no modelo de nuvem.

Observação Para o esquema de propriedade dos recursos personalizados de ação de extensibilidade, todas as propriedades são necessárias no modelo de nuvem.

Quando você adiciona fluxos de trabalho do vRealize Orchestrator ao recurso personalizado, seus parâmetros de entrada e de saída são adicionados como propriedades. Para os recursos personalizados de ação de extensibilidade, você deve criar manualmente o esquema de propriedade dos recursos personalizados de ação de extensibilidade na guia **Propriedades**. Nessa guia, você também pode modificar e formatar as propriedades dos seus recursos personalizados baseados em ações de extensibilidade do vRealize Orchestrator. Por exemplo, você pode alterar o nome de exibição de uma determinada propriedade ou adicionar restrições.

Observação Ao adicionar restrições à seção de itens de campos de matriz ou à seção de propriedades de campos de objetos no esquema de propriedades, verifique se você validou essas restrições, pois restrições aplicadas incorretamente podem causar problemas com o recurso personalizado. Por exemplo, ao adicionar uma restrição máxima a uma matriz de números, você deve verificar se essa restrição não quebra o valor padrão da propriedade.

Você pode editar o esquema de propriedades para recursos personalizados navegando até a guia **Propriedades** e usando a guia **Código** ou **Formulário**.

- **Código:** edite o esquema de propriedade usando o conteúdo YAML.
- **Formulário:** ao clicar em **Nova Propriedade**, você cria uma nova propriedade configurando o nome, o nome para exibição, a descrição, o tipo de propriedade e o valor padrão. Você também pode ocultar propriedades não obrigatórias e não calculadas do esquema, clicando em **Remover propriedade**.

Formulários de Solicitação Personalizados de Operação de Dia 2

Você pode simplificar o formulário de solicitação das operações de dia 2 incluído em seu recurso personalizado adicionando e modificando diferentes tipos de propriedades de recursos.

Por exemplo, é possível vincular o valor de um parâmetro de entrada no formulário de solicitação a uma fonte externa, como uma ação do vRealize Orchestrator que recupera um nome de implantação ou um nome do projeto. Você também pode vincular o valor de um parâmetro de entrada específico ao valor calculado de duas outras caixas de texto incluídas no mesmo formulário de solicitação.

Observação Essa funcionalidade está disponível para recursos personalizados e ações de recursos. Você pode personalizar o valor das propriedades de entrada do seu formulário de solicitação na guia **Valores** da página **Parâmetros de Solicitação** do editor de ação de recurso ou recurso personalizado.

Validação do formulário de solicitação de operação de Dia 2

Você pode validar o formulário de solicitação das suas operações de dia 2 adicionando uma validação externa. Usando uma validação externa, você impede que o usuário possa enviar o formulário de solicitação até que os parâmetros de validação sejam satisfeitos. Você pode adicionar validação externa na guia **Validações** da página **Parâmetros de Solicitação** do editor de ação de recurso ou recurso personalizado. Depois de selecionar a guia, você poderá arrastar um elemento **Validação de Orquestrador** até a tela e adicionar uma ação do vRealize Orchestrator que deseja usar para validação.

Por exemplo, você pode criar um recurso personalizado que inclui uma operação de dia 2 para alterar uma senha do usuário. Para esse caso de uso, é possível adicionar uma ação do vRealize Orchestrator com o `newPassword` e parâmetros de entrada do `confirmPassword` que usam o tipo `SecureString`.

Observação Este é um script de amostra para validar uma senha de usuário. Para seu próprio caso de uso, você pode decidir para usar um script diferente.

```
if (newPassword != confirmPassword) {
    return 'passwords are different';
}
if (newPassword.length < 7) {
    return 'password must be at least 10 symbols';
}
return null;
```

Como criar um modelo do Cloud Assembly que adiciona usuários ao Active Directory

Além dos recursos de modelo de nuvem do Cloud Assembly que você usa ao criar modelos de nuvem, também é possível criar seus próprios recursos personalizados.

Os recursos personalizados são objetos de ação do vRealize Orchestrator ou de extensibilidade que você gerencia por meio do vRealize Automation com as ações de ciclo de vida definidas no recurso personalizado. O serviço de modelo de nuvem chama automaticamente os fluxos de trabalho apropriados do vRealize Orchestrator ou as ações de extensibilidade quando a operação associada a uma ação de ciclo de vida específica é disparada. Você também pode estender a funcionalidade do tipo de recurso selecionando fluxos de trabalho ou ações de extensibilidade do vRealize Orchestrator que podem ser usados como operações de dia 2.

Esse caso de uso usa fluxos de trabalho incorporados fornecidos na biblioteca do vRealize Orchestrator. Ele inclui cadeias de caracteres ou valores prescritivos para demonstrar como realizar o processo. Você pode modificá-los para se adequação ao seu ambiente.

Para fins de referência, este caso de uso usa um projeto chamado **DevOpsTesting**. Você pode substituir esse projeto de amostra por qualquer projeto no seu ambiente.

Pré-requisitos

- Verifique se você configurou uma integração do vRealize Orchestrator. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).
- Verifique se os fluxos de trabalho que você está usando para as ações de criar, atualizar, destruir e dia 2 existem no vRealize Orchestrator e são executados com sucesso a partir de lá.
- No vRealize Orchestrator, localize o tipo de recurso usado pelos fluxos de trabalho. Os fluxos de trabalho incluídos neste recurso personalizado devem usar o mesmo tipo de recurso. Nesse caso de uso, o tipo de recurso é `AD:User`. Para obter mais informações sobre validação de tipos de recursos, consulte [Tipos de recursos personalizados para modelos de nuvem do Cloud Assembly](#).
- Usando os fluxos de trabalho integrados do Active Directory na sua integração do vRealize Orchestrator, configure um servidor do Active Directory.
- Verifique se você sabe como configurar e implantar um modelo de nuvem de máquina.

Procedimentos

- 1 Crie um recurso personalizado do Active Directory para adicionar um usuário a um grupo.

Essa etapa adiciona o recurso personalizado à tela de design de modelo de nuvem como um tipo de recurso.

- a No Cloud Assembly, selecione **Projetar > Recursos Personalizados** e clique em **Novo Recurso Personalizado**.
- b Forneça os seguintes valores.

Lembre-se de que, exceto para nomes de fluxo de trabalho, esses são valores de amostra.

| Configuração | Valor de amostra |
|-----------------|---|
| Nome | Usuário do AD Este é o nome do recurso que aparece na paleta de tipos de recursos do modelo de nuvem. |
| Tipo de Recurso | Custom.ADUser O tipo de recurso deve começar com Custom. e cada tipo de recurso devem ser exclusivos. Embora a inclusão de Custom. não é validado na caixa de texto. A cadeia de caracteres será adicionada automaticamente se você a remover. Esse tipo de recurso é adicionado à paleta de tipos de recursos para que você possa usá-lo no modelo de nuvem. |

- c Para habilitar esse tipo de recurso na lista de tipos de recurso de modelo de nuvem, verifique se a opção **Ativar** está ativa.
- d Selecione a configuração de **Escopo** que disponibiliza o tipo de recurso para qualquer projeto.
- e Em **Baseado em**, verifique se **Inventário do vRO** está selecionado como provedor de ação de ciclo de vida.

- f Selecione os fluxos de trabalho que definem o recurso e as ações de dia 2.

Observação Os fluxos de trabalho de dia 2 selecionados devem ter um parâmetro de entrada que seja do mesmo tipo que o tipo externo. A entrada de tipo externo não é exibida no formulário personalizado de dia 2 solicitado pelo usuário, pois é automaticamente vinculada ao recurso personalizado.

| Configuração | Valor de amostra |
|-----------------------------------|--|
| Ações de ciclo de vida - Criar | <p>Selecione o fluxo de trabalho Criar um usuário com uma senha em uma unidade organizacional.</p> <p>Se você tiver várias integrações do vRealize Orchestrator, selecione o fluxo de trabalho na instância de integração usada para executar esses recursos personalizados.</p> <p>Após a seleção do fluxo de trabalho, o menu suspenso de tipos externos ficará disponível e será automaticamente definido como <code>AD:User</code>.</p> <hr/> <p>Observação Um tipo de fonte externa poderá ser usado apenas uma vez se compartilhado e uma vez por projeto. Neste caso de uso, você está fornecendo o mesmo recurso personalizado para todos os projetos. Isso significa que você não pode usar <code>AD:User</code> para quaisquer outros tipos de recursos para todos os projetos. Se você tiver outros fluxos de trabalho que exijam o tipo <code>AD:User</code>, será necessário criar recursos personalizados individuais para cada projeto.</p> |
| Ações de ciclo de vida - Destruir | <p>Selecione o fluxo de trabalho Destruir um usuário.</p> |
| Ações adicionais | <p>Selecione o fluxo de trabalho Alterar a senha de um usuário.</p> <p>Na janela Adicionar Ação, insira um nome para a ação, como <code>password_change</code>, e clique em Adicionar.</p> <p>Para modificar o formulário de solicitação de ação ao qual o usuário responde quando solicita a ação, clique no ícone na coluna Parâmetros de Solicitação.</p> <hr/> <p>Observação Para fluxos de trabalho de ação adicionais, verifique se o fluxo de trabalho tem um parâmetro de entrada que seja do mesmo tipo que o tipo externo.</p> |

Neste exemplo, não há uma aplicação apropriada de um fluxo de trabalho de atualização. Um exemplo comum de um fluxo de trabalho de atualização, que faz alterações no recurso personalizado provisionado, é dimensionar ou expandir uma implantação.

- g Revise os valores de chave e tipo de esquema na guia **Propriedades** para compreender as entradas de fluxo de trabalho e poder configurar as entradas no modelo de nuvem.

O esquema lista os valores de entrada obrigatórios e opcionais definidos no fluxo de trabalho. Os valores de entrada necessários estão incluídos no YAML do modelo de nuvem.

Em Criar um fluxo de trabalho de usuário, `accountName`, `displayName` e `ouContainer` são valores de entrada necessários. As outras propriedades do esquema não são necessárias. Você também pode usar o esquema para determinar onde deseja criar associações a outros valores de campo, fluxos de trabalho ou ações. Associações não estão incluídas neste caso de uso.

- h Para concluir a criação do recurso personalizado, clique em **Criar**.

- 2 Crie um modelo de nuvem que adicione o usuário a uma máquina quando você o implantar.
 - a Selecione **Projetar > Modelos de Nuvem** e clique em **Novo a partir de > Tela em branco**.
 - b Especifique o nome **Máquina com um usuário do AD** para o modelo de nuvem.
 - c Selecione o projeto **DevOpsTesting** e clique em **Criar**.
 - d Adicione e configure uma máquina vSphere.
 - e Na lista de recursos personalizados à esquerda da página de design de modelo de nuvem, arraste o tipo de recurso **Usuário do AD** até a tela.

Observação Você pode selecionar o recurso personalizado rolando para baixo e selecionando-o no painel esquerdo ou procurando-o na caixa de texto **Pesquisar Tipos de Recurso**. Se o recurso personalizado não for exibido, clique no botão Atualizar ao lado da caixa de texto **Pesquisar Tipos de Recurso**.

- f À direita, edite o código YAML para adicionar os valores de entrada obrigatórios e a senha.

Adicione uma seção `inputs` no código para que os usuários possam fornecer o nome dos usuários que estão adicionando. No exemplo a seguir, alguns desses valores são dados de amostra. Seus valores podem ser diferentes.

```
inputs:
  accountName:
    type: string
    title: Account name
    encrypted: true
  displayName:
    type: string
    title: Display name
  password:
    type: string
    title: Password
    encrypted: true
  confirmPassword:
    type: string
    title: Password
    encrypted: true
  ouContainer:
    type: object
    title: AD OU container
    $data: 'vro/data/inventory/AD:OrganizationalUnit'
    properties:
      id:
        type: string
      type:
        type: string
```

- g Na seção `resources`, adicione o código `${input.input-name}` para solicitar a seleção do usuário.

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

3 Implante o modelo de nuvem.

- a Na página do designer de modelos de nuvem, clique em **Implantar**.
- b Insira o **Nome da Implantação Usuário do AD Scott**.

- c Selecione a **Versão do Modelo de Nuvem** e clique em **Seguinte**.
 - d Conclua as entradas de implantação.
 - e Clique em **Implantar**.
- 4 Monitore a solicitação de provisionamento na página **Implantações** para garantir que o usuário seja adicionado ao Active Directory e que a implantação seja bem-sucedida.

Próximo passo

Quando seu modelo de nuvem testado estiver funcionando, você poderá começar a usar o recurso personalizado **Usuário do AD** com outros modelos de nuvem.

Como criar um modelo do Cloud Assembly que inclui SSH

Você pode criar recursos personalizados que podem ser usados para criar modelos de nuvem usando fluxos de trabalho do vRealize Orchestrator. Neste caso de uso, você adiciona um recurso personalizado que adiciona um host SSH. Em seguida, esses recursos podem ser incluídos em modelos em nuvem. Esse procedimento também adiciona um fluxo de trabalho de atualização, para que os usuários alterem a configuração SSH após a implantação em vez de executarem ações individuais de dia 2.

Os recursos personalizados são objetos de ação do vRealize Orchestrator ou de extensibilidade que você gerencia por meio do vRealize Automation com as ações de ciclo de vida definidas no recurso personalizado. O serviço de modelo de nuvem chama automaticamente os fluxos de trabalho apropriados do vRealize Orchestrator ou as ações de extensibilidade quando a operação associada a uma ação de ciclo de vida específica é disparada. Você também pode estender a funcionalidade do tipo de recurso selecionando fluxos de trabalho ou ações de extensibilidade do vRealize Orchestrator que podem ser usados como operações de dia 2.

Esse caso de uso usa fluxos de trabalho incorporados fornecidos na biblioteca do vRealize Orchestrator. Ele inclui cadeias de caracteres ou valores prescritivos para demonstrar como realizar o processo. Você pode modificá-los para se adequação ao seu ambiente.

Para fins de referência, este caso de uso usa um projeto chamado **DevOpsTesting**. É possível substituir o projeto por um que você já tenha.

Pré-requisitos

- Verifique se você configurou uma integração do vRealize Orchestrator. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).
- Verifique se os fluxos de trabalho que você está usando para as ações de criar, atualizar, destruir e dia 2 existem no vRealize Orchestrator e são executados com sucesso a partir de lá.
- No vRealize Orchestrator, localize o tipo de recurso usado pelos fluxos de trabalho. Os fluxos de trabalho incluídos neste recurso personalizado devem usar o mesmo tipo de recurso. Nesse caso de uso, o tipo de recurso é `SSH:Host`. Para obter mais informações sobre validação de tipos de recursos, consulte [Tipos de recursos personalizados para modelos de nuvem do Cloud Assembly](#).

- Verifique se você sabe como configurar e implantar um modelo de nuvem de máquina.

Procedimentos

- 1 Crie um recurso personalizado de host SSH para adicionar SSH a um modelo de nuvem.

Essa etapa adiciona o recurso personalizado à tela de design de modelo de nuvem como um tipo de recurso.

- a No Cloud Assembly, selecione **Projetar > Recursos Personalizados** e clique em **Novo Recurso Personalizado**.
- b Forneça os seguintes valores.

Lembre-se de que, exceto para nomes de fluxo de trabalho, esses são valores de amostra.

Tabela 6-3.

| Configuração | Valor de amostra |
|-----------------|---|
| Nome | SSH Host - Projeto de teste de DevOps Este é o nome do recurso que aparece na paleta de tipos de recursos do modelo de nuvem. |
| Tipo de Recurso | Custom.SSHHost O tipo de recurso deve começar com Custom. e cada tipo de recurso devem ser exclusivos. Embora a inclusão de Custom. não é validado na caixa de texto. A cadeia de caracteres será adicionada automaticamente se você a remover. Esse tipo de recurso é adicionado à tela de design para que você possa usá-lo no modelo de nuvem. |

- c Para habilitar esse tipo de recurso na lista de tipos de recurso de modelo de nuvem, verifique se a opção **Ativar** está ativa.
- d Selecione a configuração de **Escopo** que disponibiliza o tipo de recurso para o projeto **DevOpsTesting**.
- e Em **Baseado em**, verifique se **Inventário do vRO** está selecionado como provedor de ação de ciclo de vida.

- f Selecione os fluxos de trabalho que definem o recurso.

| Configuração | Configuração |
|--------------------------------------|--|
| Ações de ciclo de vida - Criar | <p>Selecione o fluxo de trabalho Adicionar host SSH.</p> <p>Se você tiver várias integrações do vRealize Orchestrator, selecione o fluxo de trabalho na instância de integração usada para executar esses recursos personalizados.</p> <p>Depois de selecionar o fluxo de trabalho, o menu suspenso de tipos externos ficará disponível e será automaticamente definido como <code>SSH:Host</code>. Um tipo de origem externo poderá ser usado somente uma vez se o compartilhamento for o mesmo por projeto. Neste caso de uso, você está fornecendo o recurso personalizado apenas para o projeto DevOpsTesting. Se você tivesse outros fluxos de trabalho que exigissem o tipo <code>SSH:Host</code>, seria necessário criar recursos personalizados individuais para cada projeto.</p> |
| Ações do ciclo de vida - Atualização | Selecione o fluxo de trabalho Atualizar host SSH . |
| Ações de ciclo de vida - Destruir | Selecione o fluxo de trabalho Remover host SSH . |

- g Revise os valores de chave e tipo de esquema na guia **Propriedades** para compreender as entradas de fluxo de trabalho e poder configurar as entradas no modelo de nuvem.

O esquema lista os valores de entrada obrigatórios e opcionais definidos no fluxo de trabalho. Os valores de entrada necessários estão incluídos no YAML do modelo de nuvem.

No fluxo de trabalho **Adicionar host SSH**, `hostname`, `port` e `username` são valores de entrada necessários. As outras propriedades do esquema não são necessárias. Você também pode usar o esquema para determinar onde deseja criar associações a outros valores de campo, fluxos de trabalho ou ações. Associações não estão incluídas neste caso de uso.

- h Para concluir a criação do recurso personalizado, clique em **Criar**.

2 Crie um modelo de nuvem que adicione o host SSH ao implantá-lo.

- Selecione **Projetar > Modelos de Nuvem** e clique em **Novo a partir de > Tela em branco**.
- Insira **Máquina com host SSH** como nome para o modelo de nuvem.
- Selecione o projeto **DevOpsTesting** e clique em **Criar**.
- Adicione e configure uma máquina vSphere.

- e Na lista de recursos personalizados à esquerda da página de design de modelo de nuvem, arraste o tipo de recurso **Host SSH - Projeto DevOpsTesting** até a tela.

Observação Você pode selecionar o recurso personalizado rolando para baixo e selecionando-o no painel esquerdo ou procurando-o na caixa de texto **Pesquisar Tipos de Recurso**. Se o recurso personalizado não for exibido, clique no botão Atualizar ao lado da caixa de texto **Pesquisar Tipos de Recurso**.

Um lembrete de que o tipo de recurso está disponível porque foi configurado para o projeto. Se você estava criando um modelo de nuvem para outro projeto, não poderá ver o tipo de recurso.

- f À direita, edite o código YAML para adicionar os valores de entrada obrigatórios.

Adicione uma seção `inputs` no código para que os usuários possam fornecer o nome de usuário e o nome do host no momento da implantação. Neste exemplo, a porta padrão é 22. No exemplo a seguir, alguns desses valores são dados de amostra. Seus valores podem ser diferentes.

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g Na seção `resources`, adicione o código `${input.input-name}` para solicitar a seleção do usuário.

```
resources:
  Custom_SSHTHost_1:
    type: Custom.SSHTHost
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

3 Implante o modelo de nuvem.

- a Na página do designer de modelos de nuvem, clique em **Implantar**.
- b Digite o **Nome da implantação Teste do host SSH**.
- c Selecione a **Versão do Modelo de Nuvem** e clique em **Seguinte**.
- d Conclua as entradas de implantação.
- e Clique em **Implantar**.

- 4 Monitore a solicitação de provisionamento na página **Implantações** para garantir que o host SSH seja incluído na implantação e que ela seja bem-sucedida.

Próximo passo

Quando seu modelo de nuvem testado estiver funcionando, você poderá começar a usar o recurso personalizado SSH `Host` com outros modelos de nuvem.

Designs do Cloud Assembly que preparam para alterações de dia 2

Além das ações de dia 2 já associadas aos tipos de recursos do Cloud Assembly, você tem opções de design que permitem a preparação com antecedência para atualizações personalizadas que os usuários talvez precisem realizar.

Cuidado Para alterar uma implantação, você pode editar seu modelo de nuvem e reaplicar esse modelo ou pode usar ações de dia 2. No entanto, na maioria dos casos, você deve evitar misturar as duas abordagens.

As alterações de dia 2 no ciclo de vida, como ligar/desligar, normalmente são seguras, mas outras exigem cautela, como a adição de discos.

Por exemplo, se você adicionar discos com uma ação de dia 2 e, em seguida, usar uma abordagem mista reaplicando o modelo de nuvem, este poderá substituir a alteração de dia 2, o que pode remover discos e causar perda de dados.

A preparação para o dia 2 pode envolver o uso direto do código de modelo de nuvem ou da interface do design do Cloud Assembly.

- Você pode usar entradas no código do modelo de nuvem para que, ao atualizar a implantação ou o recurso implantado, a interface solicite novos valores.
- Você pode usar o Cloud Assembly para criar uma ação personalizada com base em um fluxo de trabalho ou uma ação do vRealize Orchestrator. A execução da ação personalizada faz com que o fluxo de trabalho ou a ação de extensibilidade realize alterações no recurso implantado ou na implantação.

Como usar entradas de modelo de nuvem para atualizações de dia 2 do vRealize Automation

Ao projetar modelos de nuvem do vRealize Automation, parâmetros de entrada permitem que os usuários de dia 2 insiram novamente as seleções na solicitação de implantação inicial.

Cuidado Algumas alterações de propriedade fazem com que um recurso seja criado novamente. Por exemplo, alterar o `connection_string.name` em um `Cloud.Service.Azure.App.Service` exclui o recurso existente e cria um novo.

Ao projetar entradas para oferecer suporte a alterações de dia 2, o esquema [Modelos hospedado em code.vmware.com](#) ajudará você a localizar as propriedades que excluem e recriam recursos.

Para obter informações sobre como criar entradas, consulte [Entrada do usuário em solicitações do vRealize Automation](#).

Para um exemplo de dia 2 específico, consulte a próxima seção.

Como mover uma máquina implantada para outra rede

Ao manter implantações e redes, talvez você precise da capacidade de realocar máquinas implantadas com o Cloud Assembly.

Por exemplo, você pode implantar em uma rede de teste primeiro e, em seguida, avançar para uma rede de produção. A técnica descrita aqui permite projetar um modelo de nuvem com antecedência para preparar-se para essas ações de dia 2. Observe que a máquina foi movida. Ela não é excluída e reimplantada.

Este procedimento apenas se aplica a recursos **Cloud.vSphere.Machine**. Ele não funcionará para máquinas independentes de nuvem implantadas no vSphere.

Pré-requisitos

- O perfil de rede do Cloud Assembly deve incluir todas as sub-redes às quais a máquina se conectará. No Cloud Assembly, você pode verificar redes acessando **Infraestrutura > Configurar > Perfis de Rede**.

O perfil de rede deve estar em uma conta e região que fazem parte do projeto apropriado do Cloud Assembly para seus usuários.

- Marque as duas sub-redes com tags diferentes. O exemplo a seguir pressupõe que **test** e **prod** sejam nomes de tags.
- A máquina implantada deve manter o mesmo tipo de atribuição de IP. Esse tipo não pode mudar de estático para DHCP, ou vice-versa, na ocasião de uma troca de rede.

Procedimentos

- 1 No Cloud Assembly, acesse **Projetar** e crie um modelo de nuvem para a implantação.
- 2 Na seção Entradas do código, adicione uma entrada que permita ao usuário selecionar uma rede.

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 Na seção de recursos do código, adicione o recurso **Cloud.Network** e conecte a máquina do vSphere a ele.

- 4 Abaixo de **Cloud.Network**, crie uma restrição que faça referência à seleção das entradas.

```
resources:
  ABCServer:
    type: Cloud.vSphere.Machine
    properties:
      name: abc-server
      . . .
    networks:
      - network: '${resource["ABCNet"].id}'
  ABCNet:
    type: Cloud.Network
    properties:
      name: abc-network
      . . .
    constraints:
      - tag: '${input.net-tagging}'
```

- 5 Continue com o design e implante-o como de costume. Na implantação, a interface solicita que você selecione a rede **test** ou **prod**.
- 6 Quando precisar fazer uma alteração de dia 2, acesse **Recursos > Implantações** e localize a implantação associada ao modelo de nuvem.
- 7 À direita da implantação, clique em **Ações > Atualizar**.
- 8 No painel Atualizar, a interface solicita da mesma maneira que você selecione a rede **test** ou **prod**.
- 9 Para trocar de rede, faça sua seleção, clique em **Seguinte** e depois em **Enviar**.

Como criar uma ação de recurso do Cloud Assembly para aplicar o vMotion a uma máquina virtual

Depois de implantar um modelo de nuvem, você pode executar ações de dia 2 que fazem alterações na implantação. O Cloud Assembly inclui várias ações de dia 2, mas talvez você queira fornecer outras. Você pode criar ações de recurso personalizadas e torná-las disponíveis para os usuários como ações de dia 2.

As ações de recurso personalizadas baseiam-se em fluxos de trabalho do vRealize Orchestrator.

Este exemplo de ação de recurso personalizada de dia 2 tem o objetivo de apresentar o processo de criação. Para usar ações de recurso de maneira eficaz, você deve ser capaz de criar fluxos de trabalho do vRealize Orchestrator e ações que executem as tarefas necessárias.

Pré-requisitos

- Verifique se você configurou uma integração do vRealize Orchestrator. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).
- Verifique se o fluxo de trabalho que você está usando para a ação de dia 2 existe no vRealize Orchestrator e é executado com êxito lá.

Procedimentos

- 1 Crie uma ação de recurso personalizada que use o vMotion para mover uma máquina virtual vSphere de um host para outro.

- a No Cloud Assembly, selecione **Projetar > Ações de Recursos** e clique em **Nova Ação de Recurso**.
- b Forneça os seguintes valores.

Lembre-se de que, exceto para nomes de fluxo de trabalho, esses são valores de amostra.

| Configuração | Valor de amostra |
|------------------|--|
| Nome | vSphere_VM_vMotion Esse é o nome que aparece na lista de ações de recursos. |
| Nome de Exibição | Mover VM Esse é o nome que os usuários visualizam no menu de ações de implantação. |

- c Clique na opção **Ativar** para habilitar essa ação no menu de ações de dia 2 para recursos que corresponde ao tipo de recurso.
- d Selecione o tipo de recurso e o fluxo de trabalho que definem a ação de dia 2.

| Configuração | Valor de amostra |
|-------------------|--|
| Tipo de Recurso | <p>Selecione o tipo de recurso Cloud.vSphere.Machine. Esse é o tipo de recurso implantado como um componente de modelo de nuvem, e não necessariamente o que está no modelo de nuvem. Por exemplo, você pode ter uma máquina independente de nuvem no seu modelo de nuvem, mas, quando ela é implantada em um vCenter Server, a máquina é Cloud.vSphere.Machine. Como a ação aplica-se ao tipo implantado, não use tipos independentes de nuvem ao definir suas ações de recurso.</p> <p>Neste exemplo, o vMotion funciona apenas para máquinas vSphere, mas você pode ter outras ações que deseja executar em vários tipos de recursos. Você deve criar uma ação para cada tipo de recurso.</p> |
| Fluxo de trabalho | <p>Selecione o fluxo de trabalho Migrar máquina virtual com vMotion.</p> <p>Se você tiver várias integrações do vRealize Orchestrator, selecione o fluxo de trabalho na instância de integração usada para executar essas ações de recurso personalizadas.</p> |

- 2 Crie uma vinculação para as propriedades do vRealize Orchestrator com as propriedades de esquema do Cloud Assembly. Ações de dia 2 do Cloud Assembly oferecem suporte a três tipos de associações.

| Tipo de associação | Descrição |
|----------------------|--|
| na solicitação | O tipo de associação de valor padrão. Quando selecionada, a propriedade de entrada é exibida no formulário de solicitação, e seu valor deve ser fornecido pelo usuário no momento da solicitação. |
| com ação vinculativa | Essa opção está disponível apenas para entradas de tipo de referência, como: <ul style="list-style-type: none"> ■ VC:VirtualMachine ■ VC:Folder O usuário seleciona uma ação que realiza a associação. A ação selecionada deve retornar o mesmo tipo que o parâmetro de entrada. A definição de propriedade correta é <code>\${properties.someProperty}</code> . |
| direto | Essa opção está disponível para propriedades de entrada que usam tipos de dados primitivos. Quando selecionada, a propriedade, com o tipo adequado, é mapeada diretamente do esquema da propriedade de entrada. O usuário seleciona a propriedade na árvore de esquema. Propriedades com tipos diferentes estão desativadas. |

Nesse caso de uso, a vinculação é uma ação do vRealize Orchestrator que faz a conexão entre o tipo de entrada do vRealize Orchestrator `VC:VirtualMachine` usado no fluxo de trabalho e o tipo de recurso do Cloud Assembly `Cloud.vSphere.Machine`. Ao configurar a vinculação, você torna a ação de dia 2 contínua para o usuário que solicita a ação `vMotion` em uma VM do vSphere. O sistema fornece o nome no fluxo de trabalho para que o usuário não precise fazer isso.

- Depois de selecionar o fluxo de trabalho **Migrar máquina virtual com o vMotion**, navegue até o painel **Vinculação de Propriedade**.
- Selecione a associação da propriedade de entrada `vm`.
- Em **Associação**, selecione **com ação vinculativa**.
A ação **findVcVmByVcAndVmUuid** é selecionada automaticamente. Essa ação vem pré-configurada com sua integração do vRealize Orchestrator no Cloud Assembly.
- Clique em **Salvar**.

- 3 Para salvar as alterações na ação de dia 2, clique em **Criar**.

- 4 Para considerar os outros parâmetros de entrada no fluxo de trabalho, você pode personalizar o formulário de solicitação que os usuários visualizam quando solicitam a ação.

- Em **Ações de Recursos**, selecione a ação de dia 2 criada recentemente.
- Clique em **Editar Parâmetros de Solicitação**.

É possível personalizar como a página de solicitação é apresentada aos usuários.

| Nome do Campo Padrão | Aparência | Valores | Restrições |
|--|---|---|-------------------|
| Pool de recursos de destino da máquina virtual. O padrão é o pool de recursos atual. | <ul style="list-style-type: none"> ■ Rótulo = Pool de recursos de destino ■ Tipo de exibição = Seletor de Valor | | |
| Host de destino para o qual migrar a máquina virtual | <ul style="list-style-type: none"> ■ Rótulo = Host de destino ■ Tipo de exibição = Seletor de Valor | | Obrigatório = Sim |
| Prioridade da tarefa de migração | Rótulo = Prioridade da tarefa | <p>Opções do valor</p> <ul style="list-style-type: none"> ■ Origem do valor = Constante <p>Na caixa de texto, insira uma lista separada por vírgulas.</p> <pre>lowPriority Low,defaultPriority Default,highPriority High</pre> | Obrigatório = Sim |
| (Opcional) Apenas migre a máquina virtual se seu estado de inicialização corresponder ao estado especificado | <p>Exclua essa caixa de texto.</p> <p>O vMotion pode mover máquinas em qualquer estado de energia.</p> | | |

- Clique em **Salvar**.

- 5 Para limitar quando a ação está disponível, você pode configurar as condições.

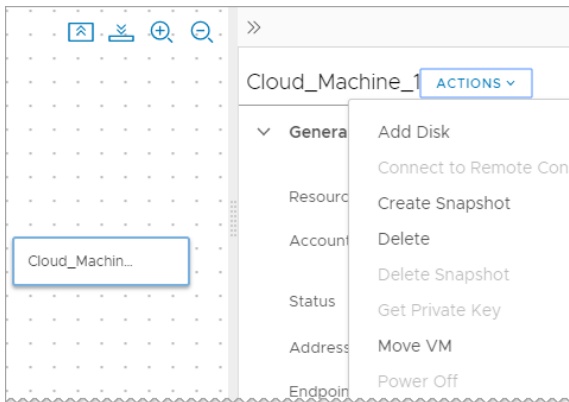
Por exemplo, você só deseja que a ação vMotion esteja disponível quando a máquina tiver quatro CPUs ou menos.

- Ative **Requer condição**.
- Insira a condição.

| Key | Operador | Valor |
|-------------------------|----------|-------|
| \${properties.cpuCount} | lessThan | 4 |

Se você precisar de condições complexas, consulte [Como criar condições avançadas para ações personalizadas do Cloud Assembly](#).

- Clique em **Atualizar**.
- 6 Verifique se a ação Mover VM está disponível para máquinas implantadas que correspondem aos critérios.
- Selecione **Implantações**.
 - Localize uma implantação que inclua uma máquina implantada que corresponda aos critérios definidos.
 - Abra a implantação e selecione a máquina.
 - Clique em Ações no painel direito e verifique se a ação **Move VM** existe.

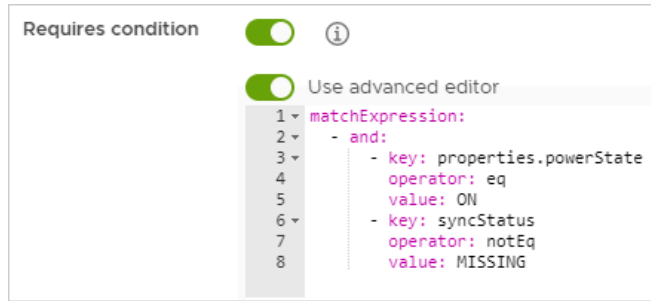


- Execute a ação.

Como criar condições avançadas para ações personalizadas do Cloud Assembly

Como alternativa à lista de condições simples no Cloud Assembly, o editor avançado permite montar expressões de critérios mais complexas para controlar quando a ação está disponível.

Ao criar uma nova ação de recurso, selecione **Requer uma condição** e **Usar editor avançado**. Em seguida, insira a expressão de critérios que você deseja.



A expressão é uma cláusula ou uma lista de cláusulas, cada uma delas no formato chave-operador-valor. A figura anterior mostra critérios onde o destino deve ser ligado e estar presente.

Cláusulas

| Cláusula | Descrição | Exemplo |
|----------|---|---|
| e | Todas as subcláusulas devem ser verdadeiras para que o resultado da expressão seja verdadeiro. | <p>Avalie como verdadeiro somente quando properties.powerState estiver LIGADO e syncStatus não estiver AUSENTE.</p> <pre>matchExpression: - and: - key: properties.powerState operator: eq value: ON - key: syncStatus operator: notEq value: MISSING</pre> |
| ou | Uma ou mais subcláusulas devem ser verdadeiras para que o resultado da expressão seja verdadeiro. | <p>Avalie como verdadeiro se properties.powerState estiver LIGADO ou DESLIGADO.</p> <pre>matchExpression: - or: - key: properties.powerState operator: eq value: ON - key: properties.powerState operator: eq value: OFF</pre> |

Operadores

| Operador | Descrição | Exemplo |
|----------|---|--|
| eq | Igual. Procure uma combinação exata. | <p>Avalie como verdadeiro quando properties.powerState estiver LIGADO.</p> <pre>matchExpression: - and: - key: properties.powerState operator: eq value: ON</pre> |
| notEq | Não igual. Evite uma combinação exata. | <p>Avalie como verdadeiro quando properties.powerState não estiver DESLIGADO.</p> <pre>matchExpression: - and: - key: properties.powerState operator: notEq value: OFF</pre> |
| hasAny | Procure uma combinação em uma coleção de objetos. | <p>Avalie como verdadeiro quando a matriz storage.disks inclui um objeto 100 IOPS EBS.</p> <pre>matchExpression: - key: storage.disks operator: hasAny value: matchExpression: - and: - key: iops operator: eq value: 100 - key: service operator: eq value: ebs</pre> |
| in | Procure uma combinação em um conjunto de valores. | <p>Avalie como verdadeiro quando properties.powerState estiver DESLIGADO ou SUSPENSO.</p> <pre>matchExpression: - and: - key: properties.powerState operator: in value: OFF, SUSPEND</pre> |
| notIn | Evite corresponder a um conjunto de valores. | <p>Avalie como verdadeiro quando properties.powerState não estiver DESLIGADO nem SUSPENSO.</p> <pre>matchExpression: - and: - key: properties.powerState operator: notIn value: OFF, SUSPEND</pre> |

| Operador | Descrição | Exemplo |
|-------------------|---|--|
| greaterThan | Procure uma combinação acima de um determinado limite. Aplica-se apenas a valores numéricos. | <p>Avalie como verdadeiro quando o primeiro objeto na matriz storage.disks tiver IOPS sobre 50.</p> <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThan value: 50</pre> |
| lessThan | Procure uma combinação sob um determinado limite. Aplica-se apenas a valores numéricos. | <p>Avalie como verdadeiro quando o primeiro objeto na matriz storage.disks tiver IOPS sob 200.</p> <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThan value: 200</pre> |
| greaterThanEquals | Procure uma combinação em ou acima de um determinado limite. Aplica-se apenas a valores numéricos. | <p>Avalie como verdadeiro quando o primeiro objeto na matriz storage.disks tiver IOPS de 100 ou superior.</p> <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThanEquals value: 100</pre> |
| lessThanEquals | Procure uma combinação em ou abaixo de um determinado limite. Aplica-se apenas a valores numéricos. | <p>Avalie como verdadeiro quando o primeiro objeto na matriz storage.disks tiver IOPS de 100 ou inferior.</p> <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThanEquals value: 100</pre> |
| matchesRegex | Use uma expressão regular para procurar uma combinação. | <p>Avalie como verdadeiro quando a properties.zone for us-east-1a ou us-east-1c.</p> <pre>matchExpression: - and: - key: properties.zone operator: matchesRegex value: (us-east-1)+(a c) {1,2}</pre> |

Exemplos

A expressão de critérios a seguir é avaliada como verdadeira quando properties.tags inclui uma tag de chave `key1` e valor `value1`.

A expressão externa usa `hasAny` porque `properties.tags` é uma matriz e você deseja avaliar como verdadeiro sempre que `key1=value1` aparece em qualquer um dos pares chave-valor na matriz.

Na expressão interna, há duas cláusulas: uma para o campo de chave e uma para o campo de valor. A matriz `properties.tags` contém pares de marcação chave-valor e você precisa corresponder aos campos chave e valor.

```
matchExpression:
- key: properties.tags
  operator: hasAny
  value:
    matchExpression:
      - and:
        - key: key
          operator: eq
          value: key1
        - key: value
          operator: eq
          value: value1
```

A expressão de critérios a seguir é semelhante ao exemplo anterior, mas agora é avaliada como verdadeira sempre que `properties.tags` incluir uma tag de `key1=value1` ou `key2=value2`.

```
matchExpression:
- or:
  - key: properties.tags
    operator: hasAny
    value:
      matchExpression:
        - and:
          - key: key
            operator: eq
            value: key1
          - key: value
            operator: eq
            value: value1
  - key: properties.tags
    operator: hasAny
    value:
      matchExpression:
        - and:
          - key: key
            operator: eq
            value: key2
          - key: value
            operator: eq
            value: value2
```

Outros exemplos de código do Cloud Assembly

O código de modelo de nuvem no Cloud Assembly pode ser praticamente ilimitado em combinação e aplicação.

Muitas vezes, um exemplo de código bem-sucedido é o melhor ponto de partida para o desenvolvimento posterior. Ao seguir um exemplo, faça as substituições para aplicar as configurações do site em termos de nomes de recursos, valores e assim por diante.

Exemplo de modelo do Cloud Assembly documentado

Ao incluir um conjunto completo de comentários, este exemplo permite que você reveja a estrutura e a finalidade das seções em um modelo do Cloud Assembly, anteriormente chamado de blueprint.

```
# *****
#
# This WordPress cloud template is enhanced with comments to explain its
# parameters.
#
# Try cloning it and experimenting with its YAML code. If you're new to
# YAML, visit yamll.org for general information.
#
# The cloud template deploys a minimum of 3 virtual machines and runs scripts
# to install packages.
#
# *****
#
# -----
# Templates need a descriptive name and version if
# source controlled in git.
# -----
name: WordPress Template with Comments
formatVersion: 1
version: 1
#
# -----
# Inputs create user selections that appear at deployment time. Inputs
# can set placement decisions and configurations, and are referenced
# later, by the resources section.
# -----
inputs:
#
# -----
# Choose a cloud endpoint. 'Title' is the visible
# option text (oneOf allows for the friendly title). 'Const' is the
# tag that identifies the endpoint, which was set up earlier, under the
# Cloud Assembly Infrastructure tab.
# -----
platform:
  type: string
  title: Deploy to
  oneOf:
    - title: AWS
      const: aws
    - title: Azure
      const: azure
    - title: vSphere
      const: vsphere
```

```

    default: vsphere

#
# -----
# Choose the operating system. Note that the Cloud Assembly
# Infrastructure must also have an AWS, Azure, and vSphere Ubuntu image
# mapped. In this case, enum sets the option that you see, meaning there's
# no friendly title feature this time. Also, only Ubuntu is available
# here, but having this input stubbed in lets you add more operating
# systems later.
# -----
osimage:
  type: string
  title: Operating System
  description: Which OS to use
  enum:
    - Ubuntu
#
# -----
# Set the number of machines in the database cluster. Small and large
# correspond to 1 or 2 machines, respectively, which you see later,
# down in the resources section.
# -----
dbenvsize:
  type: string
  title: Database cluster size
  enum:
    - Small
    - Large
#
# -----
# Dynamically tag the machines that will be created. The
# 'array' of objects means you can create as many key-value pairs as
# needed. To see how array input looks when it's collected,
# open the cloud template and click TEST.
# -----
Mtags:
  type: array
  title: Tags
  description: Tags to apply to machines
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
#
# -----
# Create machine credentials. These credentials are needed in
# remote access configuration later, in the resources section.
# -----
username:
  type: string

```



```

    minLength: 4
    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
    encrypted: true
    title: Database Password
    description: Database Password
#
# -----
# Set the database storage disk size.
# -----
databaseDiskSize:
  type: number
  default: 4
  maximum: 10
  title: MySQL Data Disk Size
  description: Size of database disk
#
# -----
# Set the number of machines in the web cluster. Small, medium, and large
# correspond to 2, 3, and 4 machines, respectively, which you see later,
# in the WebTier part of the resources section.
# -----
clusterSize:
  type: string
  enum:
    - small
    - medium
    - large
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size
#
# -----
# Set the archive storage disk size.
# -----
archiveDiskSize:
  type: number
  default: 4
  maximum: 10
  title: Wordpress Archive Disk Size
  description: Size of Wordpress archive disk
#
# -----
# The resources section configures the deployment of machines, disks,
# networks, and other objects. In several places, the code pulls from
# the preceding interactive user inputs.
# -----
resources:
#
# -----
# Create the database server. Choose a cloud agnostic machine 'type' so

```

```

# that it can deploy to AWS, Azure, or vSphere. Then enter its property
# settings.
# -----
DBTier:
  type: Cloud.Machine
  properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: mysql
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead.
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
    flavor: small
#
# -----
# Tag the database machine to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with a site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
    constraints:
      - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Also tag the database machine with any free-form tags that were created
# during user input.
# -----
    tags: '${input.Mtags}'
#
# -----
# Set the database cluster size by referencing the dbenvsize user
# input. Small is one machine, and large defaults to two.
# -----
    count: '${input.dbenvsize == "Small" ? 1 : 2}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
    networks:
      - network: '${resource.WP_Network.id}'

```

```

#
# -----
# Enable remote access to the database server. Reference the credentials
# from the user input.
# -----
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
    ABC-Company-ID: 9393
#
# -----
# Run OS commands or scripts to further configure the database machine,
# via operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
#
# -----
# Create the web server. Choose a cloud agnostic machine 'type' so that it
# can deploy to AWS, Azure, or vSphere. Then enter its property settings.
# -----
    WebTier:
      type: Cloud.Machine
      properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: wordpress
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead:
# image: '${input.osimage}'
# -----
    image: Ubuntu
#

```

```

# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
    flavor: small
#
# -----
# Set the web server cluster size by referencing the clusterSize user
# input. Small is 2 machines, medium is 3, and large defaults to 4.
# -----
    count: '${input.clusterSize== "small" ? 2 : (input.clusterSize == "medium" ? 3 : 4)}'
#
# -----
# Set an environment variable to display object information under the
# Properties tab, post-deployment. Another example might be
# {env.blueprintID}
# -----
    tags:
      - key: cas.requestedBy
        value: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
    ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
    constraints:
      - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
    networks:
      - network: '${resource.WP_Network.id}'
#
# -----
# Run OS commands or scripts to further configure the web server,
# with operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:

```

```

- apache2
- php
- php-mysql
- libapache2-mod-php
- php-mcrypt
- mysql-client
runcmd:
- mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
- i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
- mysql -u root -pmysqlpassword -h ${resource.DBTier.networks[0].address} -e
"create database wordpress_blog;"
- mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
- sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME',
'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/
mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD',
'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/
wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '$
{resource.DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp-config.php
- service apache2 reload
#
# -----
# Create the network that the database and web servers connect to.
# Choose a cloud agnostic network 'type' so that it can deploy to AWS,
# Azure, or vSphere. Then enter its property settings.
# -----
WP_Network:
  type: Cloud.Network
  properties:
#
# -----
# Descriptive name for the network. Does not become the network name
# upon deployment.
# -----
name: WP_Network
#
# -----
# Set the networkType to an existing network. You could also use a
# constraint tag to target a specific, like-tagged network.
# The other network types are private or public.
# -----
networkType: existing
#
# *****
#
# VMware hopes that you found this commented template useful. Note that
# you can also access an API to create templates, or query for input
# schema that you intend to request. See the following Swagger
# documentation.

```

```
#
# www.mgmt.cloud.vmware.com/blueprint/api/swagger/swagger-ui.html
#
# *****
```

Exemplos de recursos do vSphere no Cloud Assembly

Esses exemplos de código ilustram recursos da máquina do vSphere em modelos de nuvem do Cloud Assembly.

| Recurso | Exemplo de modelo de nuvem |
|---|--|
| Máquina virtual do vSphere com CPU, memória e sistema operacional | <pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 1 totalMemoryMB: 1024 image: ubuntu</pre> |
| Máquina do vSphere com um recurso de repositório de dados | <pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: 'HDD' capacityGb: 10 dataStore: 'datastore-01' provisioningType: thick</pre> |
| Máquina do vSphere com um disco anexado | <pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: HDD capacityGb: 10 dataStore: 'datastore-01' provisioningType: thin demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 2048 imageRef: >- https://packages.vmware.com/photon/4.0/ Rev1/ova/photon-ova-4.0-ca7c9e9330.ova attachedDisks: - source: '\${demo-vsphere-disk-001.id}'</pre> |

| Recurso | Exemplo de modelo de nuvem |
|--|---|
| Máquina do vSphere com um número dinâmico de discos | <pre> inputs: disks: type: array title: disks items: title: disks type: integer maxItems: 15 resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: image: Centos flavor: small attachedDisks: '\$ {map_to_object(resource.Cloud_Volume_1[*].id, "source")}' Cloud_Volume_1: type: Cloud.Volume allocatePerInstance: true properties: capacityGb: '\${input.disks[count.index]}' count: '\${length(input.disks)}' </pre> |
| Máquina do vSphere de uma imagem de snapshot. Acrescente uma barra e o nome do snapshot. A imagem do snapshot pode ser um clone vinculado. | <pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: imageRef: 'demo-machine/snapshot-01' cpuCount: 1 totalMemoryMB: 1024 </pre> |
| Máquina do vSphere em uma pasta específica no vCenter | <pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 1024 imageRef: ubuntu resourceGroupName: 'myFolder' </pre> |

| Recurso | Exemplo de modelo de nuvem |
|---|---|
| Máquina do vSphere com várias NICs | <pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: '\${network-01.name}' deviceIndex: 0 - network: '\${network-02.name}' deviceIndex: 1 network-01: type: Cloud.vSphere.Network properties: name: network-01 network-02: type: Cloud.vSphere.Network properties: name: network-02 </pre> |
| Máquina do vSphere com uma tag anexada no vCenter | <pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu tags: - key: env value: demo </pre> |

| Recurso | Exemplo de modelo de nuvem |
|--|---|
| Máquina do vSphere com uma especificação de personalização | <pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine image: ubuntu flavor: small customizationSpec: Linux </pre> |
| Máquina do vSphere com acesso remoto | <pre> inputs: username: type: string title: Username description: Username default: testUser password: type: string title: Password default: VMware@123 encrypted: true description: Password for the given username resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/ 16.04/release-20170307/ubuntu-16.04-server-cloudimg- amd64.ova cloudConfig: ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' runcmd: - echo "Defaults:\${input.username} ! requiretty" >> /etc/sudoers.d/\${input.username} </pre> |

Núcleos por soquete e contagem de CPUs no Cloud Assembly

O código de modelo do Cloud Assembly permite que você especifique vários núcleos por soquete para um recurso de máquina do vSphere.

Você pode especificar o número de núcleos por soquete virtual ou o número total de soquetes. Por exemplo, seus termos de licenciamento podem restringir softwares licenciados por soquete, ou os sistemas operacionais disponíveis podem reconhecer apenas um determinado número de soquetes, exigindo que CPUs adicionais sejam provisionadas como núcleos adicionais.

Adicione a propriedade `coreCount` a um modelo de nuvem no recurso de máquina do vSphere.

O valor de `coreCount` deve ser menor que ou igual ao valor da contagem de CPUs (`cpuCount`) especificado no mapeamento de tipo ou no código de recurso de máquina do vSphere no modelo de nuvem. Para obter informações relacionadas, consulte [Definindo o número de núcleos por CPU em uma máquina virtual \(1010184\)](#).

A propriedade `coreCount` é opcional e está disponível apenas para recursos de máquina do vSphere.

Um exemplo de trecho de recurso de máquina do vSphere é mostrado abaixo.

```
Cloud_vSphere_Machine_1:
  type: Cloud.vSphere.Machine
  properties:
    cpuCount: 8
    coreCount: 4
```

Informações adicionais sobre soquetes e núcleos por configurações de soquete estão disponíveis no artigo de blog em inglês [Virtual Machine vCPU and vNUMA Rightsizing – Guidelines](#).

Redes, recursos de segurança e balanceadores de carga no vRealize Automation

Você pode usar recursos e configurações de rede, segurança e balanceador de carga em designs e implantações de modelos de nuvem.

Para obter um resumo das opções de código de design de modelo de nuvem, consulte [Esquema de tipos de recursos do vRealize Automation](#).

Para obter informações relacionadas, consulte:

- [Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation](#)
- [Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation](#)
- [Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation](#)

Esses exemplos ilustram recursos de rede, segurança e balanceador de carga em designs básicos de modelos de nuvem.

Redes

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---|---|
| <p>Máquina do vSphere com várias NICs conectadas a redes vSphere e NSX com atribuição de IPs DHCP</p> | <pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: \${resource["demo-vSphere- Network"].id} deviceIndex: 0 - network: \${resource["demo-NSX- Network"].id} deviceIndex: 1 demo-vSphere-Network: type: Cloud.vSphere.Network properties: networkType: existing demo-NSX-Network: type: Cloud.NSX.Network properties: networkType: outbound</pre> |
| <p>Adicionar uma rede privada com um endereço IP estático para uma implantação de VM do Azure</p> | <pre>formatVersion: 1 inputs: {} resources: Cloud_Azure_Machine_1: type: Cloud.Azure.Machine properties: image: photon flavor: Standard_B1ls networks: - network: '\$ {resource.Cloud_Network_1.id}' assignment: static address: 10.0.0.45 assignPublicIpAddress: false Cloud_Network_1: type: Cloud.Network properties: networkType: existing</pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|--|---|
| <p>Você pode usar uma atribuição de IP estático com o vRealize IPAM (interno, conforme fornecido com o vRealize Automation, ou externo, com base no SDK IPAM do vRA, como para um dos plug-ins Infoblox disponíveis no VMware Marketplace). Outros usos de <code>assignment: static</code> não são aceitos, conforme descrito na seção <i>Ressalvas</i> do Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation.</p> | <pre>resources: demo_vm: type: Cloud.vSphere.Machine properties: image: 'photon' cpuCount: 1 totalMemoryMB: 1024 networks: - network: \${resource.demo_nw.id} assignment: static demo_nw: type: Cloud.vSphere.Network properties: networkType: existing</pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---|---|
| <p>Adicione ou edite regras de direcionamento de porta NAT e DNAT em um recurso Cloud.NSX.NAT para uma implantação existente.</p> | <pre> resources: gw: type: Cloud.NSX.Gateway properties: networks: - \${resource.akout.id} nat: type: Cloud.NSX.Nat properties: networks: - \${resource.akout.id} natRules: - translatedInstance: \$ {resource.centos.networks[0].id} index: 0 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 80 translatedPorts: 8080 destinationPorts: 8080 description: edit - translatedInstance: \$ {resource.centos.networks[0].id} index: 1 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 90 translatedPorts: 9090 destinationPorts: 9090 description: add gateway: \${resource.gw.id} centos: type: Cloud.vSphere.Machine properties: image: WebTinyCentOS65x86 flavor: small customizationSpec: Linux networks: - network: \${resource.akout.id} assignment: static akout: type: Cloud.NSX.Network properties: networkType: outbound constraints: - tag: nsxt-nat-1-M2 </pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|--|---|
| <p>Máquina de nuvem pública para usar um IP interno em vez de um IP público. Este exemplo usa uma ID de rede específica.</p> <p>Observação: a opção <code>network</code>: é usada na configuração de <code>networks</code>: para especificar uma ID de rede de destino. A opção <code>name</code>: na configuração de <code>networks</code>: foi substituída e não deve ser usada.</p> | <pre>resources: wf_proxy: type: Cloud.Machine properties: image: ubuntu 16.04 flavor: small constraints: - tag: 'platform:vsphere' networks: - network: '\${resource.wf_net.id}' assignPublicIpAddress: false</pre> |
| <p>Rede roteada para NSX-V ou NSX-T usando o tipo de recurso de rede NSX.</p> | <pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: routed</pre> |
| <p>Adicione uma tag a um recurso de NIC de máquina no modelo de nuvem.</p> | <pre>formatVersion: 1 inputs: {} resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu networks: - name: '\${resource.Cloud_Network_1.name}' deviceIndex: 0 tags: - key: 'nic0' value: null - key: internal value: true - name: '\${resource.Cloud_Network_2.name}' deviceIndex: 1 tags: - key: 'nic1' value: null - key: internal value: false</pre> |
| <p>Marque comutadores lógicos do NSX-T para uma rede de saída.</p> <p>A marcação tem suporte para o NSX-T e o VMware Cloud on AWS.</p> <p>Para obter mais informações sobre esse cenário, consulte a postagem do blog da comunidade Criando tags no NSX com o Cloud Assembly.</p> | <pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: outbound tags: - key: app value: opencart</pre> |

Grupos de segurança

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|--|---|
| <p>Grupo de segurança existente com uma tag de restrição aplicada a uma NIC de máquina.</p> <p>Para usar um grupo de segurança existente, insira <i>existente</i> para a propriedade <code>securityGroupType</code>.</p> <p>É possível atribuir tags a um recurso <code>Cloud.SecurityGroup</code> para alocar grupos de segurança existentes usando restrições de tag. Grupos de segurança que não contiverem tags não poderão ser usados no design de modelo de nuvem.</p> <p>Tags de restrição devem ser definidas para recursos de grupo de segurança <code>securityGroupType: existing</code>. Essas restrições devem corresponder às tags definidas nos grupos de segurança existentes. Tags de restrição não podem ser definidas para recursos de grupo de segurança <code>securityGroupType: new</code>.</p> | <pre>formatVersion: 1 inputs: {} resources: allowSsh_sg: type: Cloud.SecurityGroup properties: securityGroupType: existing constraints: - tag: allowSsh compute: type: Cloud.Machine properties: image: centos flavor: small networks: - network: '\${resource.prod-net.id}' securityGroups: - '\${resource.allowSsh_sg.id}' prod-net: type: Cloud.Network properties: networkType: existing</pre> |
| <p>Grupo de segurança sob demanda com duas regras de firewall ilustrando as opções de acesso a Allow e Deny.</p> | <pre>resources: Cloud_SecurityGroup_1: type: Cloud.SecurityGroup properties: securityGroupType: new rules: - ports: 5000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Allow direction: inbound name: allow_5000 protocol: TCP - ports: 7000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Deny direction: inbound name: deny_7000 protocol: TCP Cloud_vSphere_Machine_1: type: Cloud.vSphere.Machine properties: image: photon</pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|--|--|
| | <pre> cpuCount: 1 totalMemoryMB: 256 networks: - network: '\$ {resource.Cloud_Network_1.id}' assignIPv6Address: true assignment: static securityGroups: - '\$ {resource.Cloud_SecurityGroup_1.id}' Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre> |
| <p>Modelo de nuvem complexo com 2 grupos de segurança, incluindo:</p> <ul style="list-style-type: none"> ■ 1 grupo de segurança existente ■ 1 grupo de segurança sob demanda com vários exemplos de regras de firewall ■ 1 máquina do vSphere ■ 1 rede existente <p>Esta amostra ilustra diferentes combinações de protocolos e portas, serviços, CIDR IP como origem e destino, intervalo de IPs como origem ou destino e as opções para qualquer, IPv6 e (::/0). Para NICs de máquina, é possível especificar a rede conectada e o(s) grupo(s) de segurança. Você também pode especificar o índice de NIC ou um endereço IP.</p> | <pre> formatVersion: 1 inputs: {} resources: DEMO_ESG : <i>existing security group - security group 1</i>) type: Cloud.SecurityGroup properties: constraints: - tag: BlockAll securityGroupType: existing (<i>designation of existing for security group 1</i>) DEMO_ODSG: (<i>on-demand security group - security group 2</i>) type: Cloud.SecurityGroup properties: rules: (<i>multiple firewall rules in this section</i>) - name: IN-ANY (<i>rule 1</i>) source: any service: any direction: inbound access: Deny - name: IN-SSH (<i>rule 2</i>) source: any service: SSH direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 3</i>) source: 33.33.33.1-33.33.33.250 protocol: TCP ports: 223 direction: inbound access: Allow - name: IPv-6-ANY-SOURCE (<i>rule 4</i>) source: '::/0' protocol: TCP ports: 223 direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 5</i>) source: 44.44.44.1/24 protocol: UDP ports: 22-25 direction: inbound access: Allow - name: IN-EXISTING-SG (<i>rule 6</i>) source: '\${resource["DEMO_ESG"].id}' </pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---------------------|---|
| | <pre> protocol: ICMPv6 direction: inbound access: Allow - name: OUT-ANY (rule 7) destination: any service: any direction: outbound access: Deny - name: OUT-TCP-IPv6 (rule 8) destination: '2001:0db8:85a3::8a2e:0370:7334/64' protocol: TCP ports: 22 direction: outbound access: Allow - name: IPv6-ANY-DESTINATION (rule 9) destination: '::/0' protocol: UDP ports: 23 direction: outbound access: Allow - name: OUT-UDP-SERVICE (rule 10) destination: any service: NTP direction: outbound access: Allow securityGroupType: new (designation of on- demand for security group 2) DEMO_VC_MACHINE: (machine resource) type: Cloud.vSphere.Machine properties: image: PHOTON cpuCount: 1 totalMemoryMB: 1024 networks: (Machine network NICs) - network: '\${resource.DEMO_NW.id}' securityGroups: - '\${resource.DEMO_ODSG.id}' - '\${resource.DEMO_ESG.id}' DEMO_NETWORK: (network resource) type: Cloud.vSphere.Network properties: networkType: existing constraints: - tag: nsx62 </pre> |

Balancedores de carga

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|--|--|
| <p>Especifique um nível de log, algoritmo e tamanho de balanceador de carga.</p> | <p>Amostra do balanceador de carga NSX mostrando o uso do nível de log, algoritmo e tamanho:</p> <pre>resources: Cloud_LoadBalancer_1: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' loggingLevel: CRITICAL algorithm: LEAST_CONNECTION type: MEDIUM</pre> |
| <p>Associe um balanceador de carga a uma máquina nomeada ou a uma NIC de máquina nomeada. Você pode especificar <code>machine ID</code> ou <code>machine network ID</code> para adicionar a máquina ao pool do balanceador de carga. A propriedade de instâncias oferece suporte a ambas as máquinas (<code>machine by ID</code>) e NICs (<code>machine by network ID</code>).</p> <p>No primeiro exemplo, a implantação usa a configuração <code>machine by ID</code> para balancear a carga da máquina quando ela é implantada em qualquer rede.</p> <p>No segundo exemplo, a implantação usa a configuração de <code>machine by network ID</code> para balancear a carga da máquina somente quando a máquina é implantada na NIC da máquina nomeada.</p> <p>O terceiro exemplo mostra ambas as configurações usadas na mesma opção de <code>instances</code>.</p> | <p>Você pode usar a propriedade <code>instances</code> para definir uma ID de máquina ou uma ID de rede de máquinas:</p> <ul style="list-style-type: none"> ■ ID de máquina <pre>Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.id}'</pre> ■ ID de rede de máquinas <pre>Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.networks[0].id}'</pre> ■ Uma máquina especificada para a inclusão do balanceador de carga e outra NIC de máquina especificada para a inclusão do balanceador de carga: <pre>instances: - resource.Cloud_Machine_1.id - resource.Cloud_Machine_2.networks[2].id</pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---|---|
| <p>Adicione as configurações de verificação de integridade a um balanceador de carga NSX. As opções adicionais incluem <code>httpMethod</code>, <code>requestBody</code> e <code>responseBody</code>.</p> | <pre>myapp-lb: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' algorithm: ROUND_ROBIN instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /mywordpresssite/wp-admin/ install.php intervalSeconds: 60 timeoutSeconds: 10 unhealthyThreshold: 10 healthyThreshold: 2 connectionLimit: '50' connectionRateLimit: '50' maxConnections: '500' minConnections: '' internetFacing: true{code}</pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---|--|
| <p>Rede sob demanda com um balanceador de carga de 1 braço.</p> | <pre> inputs: {} resources: mp-existing: type: Cloud.Network properties: name: mp-existing networkType: existing mp-wordpress: type: Cloud.vSphere.Machine properties: name: wordpress count: 2 flavor: small image: tiny customizationSpec: Linux networks: - network: '\${resource["mp-private"].id}' mp-private: type: Cloud.NSX.Network properties: name: mp-private networkType: private constraints: - tag: nsxt mp-wordpress-lb: type: Cloud.LoadBalancer properties: name: wordpress-lb internetFacing: false network: '\${resource.mp-existing.id}' instances: '\${resource["mp-wordpress"].id}' routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.pl intervalSeconds: 60 timeoutSeconds: 30 unhealthyThreshold: 5 healthyThreshold: 2 </pre> |
| <p>Rede existente com um balanceador de carga.</p> | <pre> formatVersion: 1 inputs: count: type: integer default: 1 resources: ubuntu-vm: type: Cloud.Machine properties: name: ubuntu flavor: small image: tiny count: '\${input.count}' networks: </pre> |

| Cenário de recursos | Exemplo de código de design de modelo de nuvem |
|---------------------|---|
| | <pre> - network: '\$ {resource.Cloud_NSX_Network_1.id}' Provider_LoadBalancer_1: type: Cloud.LoadBalancer properties: name: OC-LB routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.html intervalSeconds: 60 timeoutSeconds: 5 unhealthyThreshold: 5 healthyThreshold: 2 network: '\$ {resource.Cloud_NSX_Network_1.id}' internetFacing: false instances: '\${resource["ubuntu-vm"].id}' Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: existing constraints: - tag: nsxt24prod </pre> |

Saiba mais

Para cenários de implementação de rede e grupo de segurança, consulte os blogs da VMware, como estes:

- [Um mergulho profundo no Balanceador de carga do vRealize Automation Cloud Assembly com o NSX-T](#)
- [Automação de rede com o Cloud Assembly e o NSX – Parte 1](#) (inclui o uso de contas de nuvem do NSX-T e do vCenter e do CIDR de rede)
- [Automação de rede com o Cloud Assembly e o NSX – Parte 2](#) (inclui o uso de tipos de rede existentes e de saída)
- [Automação de rede com o Cloud Assembly e o NSX – Parte 3](#) (inclui o uso de grupos de segurança existentes e sob demanda)
- [Automação de rede com o Cloud Assembly e o NSX – Parte 4](#) (inclui o uso de balanceadores de carga existentes e sob demanda)

Mais informações sobre recursos de rede em modelos de nuvem do vRealize Automation

Ao criar ou editar seus modelos de nuvem do vRealize Automation, use os recursos de rede mais apropriados para os seus objetivos. Saiba mais sobre as opções de rede do NSX e independentes de nuvem que estão disponíveis no modelo de nuvem.

Selecione um dos tipos de recursos de rede disponíveis com base na máquina e nas condições relacionadas no seu modelo de nuvem do vRealize Automation.

Recurso de rede independente de nuvem

Adicione uma rede independente de nuvem usando o recurso **Rede > Independente de Nuvem** na página **Projetar** do modelo de nuvem. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.Network`. O recurso padrão é exibido como:

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

Use uma rede independente de nuvem quando quiser especificar as características de rede para um tipo de máquina de destino que não está, ou talvez não esteja, conectada a uma rede do NSX.

O recurso de rede independente de nuvem está disponível para estes tipos de recursos:

- Máquina independente de nuvem
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

O recurso de rede independente de nuvem está disponível para estas configurações de tipo de rede (`networkType`):

- pública
- privada
- de saída
- existente

Recurso de rede do vSphere

Você adiciona uma rede do vSphere usando o recurso **Rede > vSphere** na página **Projetar** do modelo de nuvem. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.vSphere.Network`. O recurso padrão é exibido como:

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

Use uma rede do vSphere quando quiser especificar as características de rede para um tipo de máquina do vSphere (`Cloud.vSphere.Machine`).

O recurso de rede do vSphere só está disponível para um tipo de máquina `Cloud.vSphere.Machine`.

O recurso do vSphere está disponível para estas configurações de tipo de rede (`networkType`):

- pública
- privada
- existente

Para conhecer exemplos, consulte [Como usar as configurações de rede em perfis de rede e modelos de nuvem no vRealize Automation](#).

Recurso de rede do NSX

Você adiciona uma rede do NSX usando o recurso **Rede do > NSX** na página **Projetar** do modelo de nuvem. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.NSX.Network`. O recurso padrão é exibido como:

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

Use uma rede do NSX quando quiser anexar um recurso de rede a uma ou mais máquinas que foram associadas a uma conta de nuvem do NSX-V ou NSX-T. O recurso de rede NSX permite que você especifique as características de rede do NSX para um recurso de máquina vSphere que está associado a uma conta de nuvem do NSX-V ou NSX-T.

O recurso do `Cloud.NSX.Network` está disponível para estas configurações de tipo de rede (`networkType`):

- pública
- privada
- de saída
- existente

- roteadas - As redes roteadas só estão disponíveis para NSX-V e NSX-T.

Se você deseja que várias redes de saída ou roteadas compartilhem o mesmo roteador de Tier-1 do NSX-T ou Edge Service Gateway (ESG) do NSX-V, conecte um único recurso de gateway do NSX (`Cloud.NSX.Gateway`) às redes conectadas no modelo antes da implantação inicial. Se você adicionar o gateway após a implantação como uma operação de desenvolvimento iterativa ou de Dia 2, cada rede criará seu próprio roteador.

Você pode usar o recurso NAT do NSX no modelo para suportar as regras de direcionamento de porta NAT e DNAT.

Recurso de rede independente de nuvem com intenção de implantação do Azure, AWS ou GCP

VMs de provedor de nuvem pública podem exigir combinações de propriedades de modelo de nuvem específicas que não são necessariamente exigidas no NSX ou vSphere com base em implantações de máquinas. Para exemplos de código de modelo de nuvem que oferecem suporte a alguns desses cenários, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Recurso de gateway do NSX

Você pode reusar ou compartilhar um único roteador de Tier-1 do NSX-T ou um Edge Service Gateway (ESG) do NSX-V em uma única implantação usando um recurso de gateway (`Cloud.NSX.Gateway`) no modelo de nuvem. O recurso de gateway representa o Tier-1 ou ESG e pode ser conectado a várias redes na implantação. O recurso de gateway pode ser usado somente com redes de saída ou roteadas.

O recurso `Cloud.NSX.Gateway` permite que você compartilhe o roteador Tier-1 do NSX-T ou Edge Service Gateway (ESG) do NSX-V entre redes de saída ou roteadas conectadas em uma implantação.

O gateway costuma ser anexado a uma única rede de saída ou roteada. No entanto, se o gateway estiver conectado a várias redes, as redes deverão ser do mesmo tipo, por exemplo, todas de saída ou todas roteadas. O gateway pode ser conectado a várias máquinas ou balanceadores de carga que estão conectados às mesmas redes de saída ou roteadas. O gateway deve ser conectado a um balanceador de carga na rede sob demanda compartilhada para que ele possa reutilizar o roteador Tier-1 do NSX-T ou o Edge Service Gateway (ESG) do NSX-V criado pelo gateway.

Para permitir que várias redes de saída ou roteadas compartilhem o mesmo roteador T1 ou Edge, conecte inicialmente um único recurso de gateway do `Cloud.NSX.Gateway` a todas as redes. Todas as redes pretendidas e o único gateway devem ser conectados antes de implantar o modelo de nuvem, caso contrário, cada rede criará seu próprio roteador.

Para uma rede do NSX que contenha um recurso de gateway de processamento associado, as configurações do gateway são aplicadas a todas as redes associadas na implantação. Um único roteador lógico de Camada 1 do NSX-T é criado para cada implantação e compartilhado por todas as redes sob demanda e balanceadores de carga na implantação. Um único Edge do NSX-V é criado para cada implantação e compartilhado por todas as redes sob demanda e balanceadores de carga na implantação.

Você pode anexar o recurso de gateway a uma rede como uma atualização de implantação iterativa. No entanto, fazer isso não cria um roteador T1 ou Edge. A implantação de rede inicial cria o roteador.

Para redes do NSX-T que não usam um recurso de gateway associado, várias redes sob demanda no modelo de nuvem continuam a criar vários roteadores lógicos de Tier-1 na implantação.

Se o gateway contiver regras de NAT, você poderá reconfigurar ou excluir as regras de NAT ou DNAT para o roteador de Tier 1 ou Edge. Se o gateway for implantado inicialmente sem regras de NAT, ele não terá ações de Dia 2 disponíveis.

Recurso NAT do NSX

O recurso do `Cloud.NSX.NAT` permite que as regras de DNAT e o direcionamento de porta sejam anexados a todas as redes de saída conectadas por meio do recurso de gateway. Você pode anexar um recurso NAT a um recurso de gateway para o qual as regras de DNAT precisam ser configuradas.

Observação O recurso do `Cloud.NSX.Gateway` estava originalmente disponível para as regras de DNAT. No entanto, o uso do `Cloud.NSX.Gateway` como um meio de definir regras de DNAT e o direcionamento de porta foi preterido. Ele permanece disponível para compatibilidade com versões anteriores. Use o recurso de modelo de nuvem do `Cloud.NSX.NAT` para regras de DNAT e direcionamento de porta. Um aviso será exibido no modelo de nuvem se você tentar usar o tipo de recurso do `Cloud.NSX.Gateway` com especificações de regra de NAT.

O recurso do `Cloud.NSX.NAT` oferece suporte a regras de DNAT e direcionamento de porta quando conectado a uma rede do NSX-V ou NSX-T de saída.

A configuração de regras de NAT no recurso é `natRules:`. Você pode anexar o recurso de NAT ao recurso de gateway para configurar as entradas do `natRules:` no gateway. As regras de DNAT especificadas no recurso usam as máquinas ou os balanceadores de carga associados como seus destinos.

Você pode reconfigurar um NIC de máquina ou um gateway de processamento em uma implantação existente para modificar suas configurações de `natRules:` ao adicionar, reordenar, editar ou excluir regras de direcionamento de porta DNAT. Não é possível usar regras de DNAT com máquinas agrupadas em cluster. Você pode especificar regras de DNAT para máquinas individuais no cluster como parte de uma operação de Dia 2.

Opções de integração de IPAM externo

Para obter informações sobre as propriedades que estão disponíveis para uso com as suas integrações de IPAM Infoblox em designs e implantações de modelos de nuvem, consulte [Uso de propriedades específicas do Infoblox e atributos extensíveis para integrações de IPAM em modelos de nuvem do vRealize Automation](#).

Convertências por usar uma atribuição de IP estático em um modelo de nuvem

Você pode usar uma atribuição de IP estático em um modelo de nuvem do vRealize Automation somente ao usar o IPAM do vRealize Automation, ou seja, o IPAM que é o IPAM interno fornecido pelo vRealize Automation ou o IPAM derivado de um plug-in de provedor externo que foi criado usando o SDK do IPAM do vRealize Automation, por exemplo, um dos plug-ins Infoblox que estão disponíveis para download no vRealize Automation Marketplace. O uso de uma atribuição de IP estático (`assignment:static`) não é compatível em um modelo de nuvem ao usar um tópico de evento de Configuração de Rede (que é usado por uma ação de extensibilidade do Cloud Assembly (ABX) ou um fluxo de trabalho do vRealize Orchestrator). Atribuições de IP estático sem suporte causam falha na implantação.

Valor do endereço na seção Geral do modelo de nuvem implantado

Ao examinar um modelo de nuvem implantado, o valor **Endereço** na seção **Geral** do modelo é o endereço IP principal da máquina. O endereço principal costuma ser o endereço de máquina público ou de outra forma acessível. Para implantações do vSphere, o endereço IP principal é calculado pelo vRealize Automation. Todos os endereços IP para todas as NICs, incluindo suas propriedades públicas, privadas, IPv6, estáticas e dinâmicas, são considerados e classificados para determinar o endereço IP principal. Para implantações que não são do vSphere, o endereço IP principal da máquina é calculado pelo sistema de classificação de cada fornecedor de nuvem.

Operações de dia 2 disponíveis

Para obter uma lista de operações comuns de dia 2 disponíveis para recursos de modelo de nuvem e implantação, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Para obter um exemplo de como mover de uma rede para outra, consulte [Como mover uma máquina implantada para outra rede](#).

Saiba mais

Para obter informações relacionadas e exemplos que ilustram recursos e configurações de rede, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Para obter informações sobre como definir recursos de rede, consulte [Recursos de rede no vRealize Automation](#).

Para obter informações sobre como definir perfis de rede, consulte [Saiba mais sobre perfis de rede no vRealize Automation](#).

Mais sobre grupos de segurança e recursos de tag nos modelos de nuvem vRealize Automation

Ao criar ou editar seus modelos de nuvem do vRealize Automation, use as opções de recursos de segurança mais adequadas para atender aos seus objetivos.

Recurso de grupo de segurança independente de nuvem

Você adiciona um recurso de grupo de segurança usando o recurso **Grupo de Segurança > Independente de Nuvem** na página Projetar do modelo de nuvem. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.SecurityGroup`. O recurso padrão é exibido como:

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

Você especifica um recurso de grupo de segurança em um design de modelo de nuvem como existente (`securityGroupType: existing`) ou sob demanda (`securityGroupType: new`).

É possível adicionar um grupo de segurança existente ao seu modelo de nuvem ou usar um grupo de segurança existente que tenha sido adicionado a um perfil de rede.

Para NSX-V e NSX-T, bem como o NSX-T com a opção de gerenciador de políticas ativada em combinação com o VMware Cloud on AWS, você pode adicionar um grupo de segurança existente ou definir um novo grupo de segurança conforme projeta ou modifica seu modelo de nuvem. Grupos de segurança sob demanda têm suporte para o NSX-T, o NSX-V e o VMware Cloud on AWS quando usados com o gerenciador de políticas do NSX-T.

Para todos os tipos de conta de nuvem, exceto Microsoft Azure, você pode associar um ou mais grupos de segurança a um NIC de máquina. Um NIC de máquina virtual Microsoft Azure (*machineName*) só pode ser associado a um grupo de segurança.

Por padrão, a propriedade de grupo de segurança `securityGroupType` está definida como `existing`. Para criar um grupo de segurança sob demanda, insira `new` para a propriedade `securityGroupType`. Para especificar regras de firewall para um grupo de segurança sob demanda, use a propriedade `rules` na seção `Cloud.SecurityGroup` do recurso de grupo de segurança.

Grupos de segurança existentes

Grupos de segurança existentes são criados em um recurso de conta de nuvem de origem, como o NSX-T ou o Amazon Web Services. Eles são coletados por dados pelo vRealize Automation da origem. Você pode selecionar um grupo de segurança existente em uma lista de recursos disponíveis como parte de um perfil de rede do vRealize Automation. Em um design de modelo de nuvem, é possível especificar um grupo de segurança existente de forma inerente por sua associação em um perfil de rede especificado ou especificamente por nome usando a

configuração `securityGroupType: existing` em um recurso de grupo de segurança. Se você adicionar um grupo de segurança a um perfil de rede, adicione pelo menos uma tag de recurso ao perfil de rede. Recursos de grupo de segurança sob demanda exigem uma tag de restrição quando usados em um design de modelo de nuvem.

Você pode associar um recurso de grupo de segurança no seu design de modelo de nuvem a um ou mais recursos de máquina.

Observação Se você pretende usar um recurso de máquina no seu design de modelo de nuvem para provisionar em um NIC de máquina virtual da Microsoft Azure (*machineName*), deverá associar apenas o recurso de máquina a um único grupo de segurança.

Grupos de segurança sob demanda

Você pode definir grupos de segurança sob demanda à medida que define ou modifica um design de modelo de nuvem usando a configuração `securityGroupType: new` no código de recursos do grupo de segurança.

Você pode usar um grupo de segurança sob demanda para o NSX-V e o NSX-T, assim como a Amazon Web Services quando usada com o Tipo de política do NSX-T, para aplicar um conjunto específico de regras de firewall a um recurso de máquina em rede ou conjunto de recursos agrupados. Cada grupo de segurança pode conter várias regras de firewall nomeadas. É possível usar um grupo de segurança sob demanda para especificar serviços ou protocolos e portas. Observe que você pode especificar um serviço ou um protocolo, mas não ambos. É possível especificar uma porta além de um protocolo. Não será possível especificar uma porta se você especificar um serviço. Se a regra não contiver um serviço ou um protocolo, o valor padrão do serviço será Qualquer.

Você também pode especificar endereços IP e intervalos de IP em regras de firewall. Alguns exemplos de regras de firewall são mostrados em [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Quando você cria regras de firewall em um grupo de segurança do NSX-V ou NSX-T sob demanda, o padrão é permitir o tráfego de rede especificado, mas também permitir outro tráfego de rede. Para controlar o tráfego de rede, você deve especificar um tipo de acesso para cada regra. Os tipos de acesso de regra são:

- Permitir (padrão) - Permite o tráfego de rede especificado nessa regra de firewall.
- Negar - Bloqueia o tráfego de rede especificado nessa regra de firewall. Informa ativamente ao cliente que a conexão foi rejeitada.
- Descartar - Rejeita o tráfego de rede especificado nessa regra de firewall. Descarta silenciosamente o pacote como se o ouvinte não estivesse online.

Para obter um exemplo de design que usa uma regra `access: Allow` e uma regra de firewall `access: Deny`, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Observação Um administrador de nuvem pode criar um design de modelo de nuvem que contenha apenas um grupo de segurança do NSX sob demanda e pode implantar esse design para criar um recurso de grupo de segurança existente reutilizável que os membros da organização podem adicionar a perfis de rede e designs de modelo de nuvem como um grupo de segurança existente.

As regras de firewall oferecem suporte a valores CIDR de formato IPv4 ou IPv6 para endereços IP de origem e de destino. Para obter um exemplo de design que usa valores CIDR IPv6 em uma regra de firewall, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Grupos de segurança sob demanda e existentes para VMware Cloud on AWS

Você pode definir um grupo de segurança sob demanda para uma máquina VMware Cloud on AWS em um modelo de nuvem usando a configuração `securityGroupType: new` no código de recurso do grupo de segurança.

Um exemplo de snippet de código para um grupo de segurança sob demanda é mostrado abaixo:

```
resources:
  Cloud_SecurityGroup_1:
    type: Cloud.SecurityGroup
    properties:
      name: vmc-odsg
      securityGroupType: new
    rules:
      - name: datapath
        direction: inbound
        protocol: TCP
        ports: 5011
        access: Allow
        source: any
```

Você também pode definir um grupo de segurança existente para uma máquina VMware Cloud on AWS em rede e, opcionalmente, incluir a marcação de restrição, como mostrado nos exemplos a seguir:

```
Cloud_SecurityGroup_2:
  type: Cloud.SecurityGroup
  properties:
    constraints: [xyz]
    securityGroupType: existing

Cloud_SecurityGroup_3:
  type: Cloud.SecurityGroup
  properties:
    securityGroupType: existing
    constraints:
      - tag: xyz
```

Há suporte para o desenvolvimento de modelos de nuvem iterativos.

- Se um grupo de segurança estiver associado a uma ou mais máquinas na implantação, uma ação de exclusão exibirá uma mensagem informando que o grupo de segurança não pode ser excluído.
- Se um grupo de segurança não estiver associado a uma máquina na implantação, uma ação de exclusão exibirá uma mensagem informando que o grupo de segurança será excluído dessa implantação e que a ação não poderá ser desfeita. Um grupo de segurança existente é excluído do modelo de nuvem, enquanto um grupo de segurança sob demanda é destruído.

Usando tags de segurança do NSX-V e tags de VM do NSX-T

É possível visualizar e usar tags de segurança do NSX-V e tags de VM do NSX-T e NSX-T com política a partir de recursos gerenciados em modelos de nuvem do vRealize Automation.

Tags de segurança do NSX-V e do NSX-T têm suporte para uso com o vSphere. Tags de segurança do NSX-T também têm suporte para uso com o VMware Cloud on AWS.

Observação Assim como acontece com as VMs implantadas no vSphere, você pode configurar tags de máquina para que uma VM seja implantada no VMware Cloud on AWS. Você também pode atualizar a tag da máquina após a implantação inicial. Essas tags de máquina permitem que o vRealize Automation atribua dinamicamente uma VM a um grupo de segurança apropriado do NSX-T durante a implantação.

Você pode especificar tags de segurança do NSX-V usando `key: nsxSecurityTag` e um valor de tag no recurso de processamento no modelo de nuvem, como mostrado no exemplo a seguir, desde que a máquina esteja conectada a uma rede do NSX-V:

```
tags:
  - key: nsxSecurityTag
    value: security_tag_1
  - key: nsxSecurityTag
    value: security_tag_2
```

O valor especificado deve corresponder a uma tag de segurança do NSX-V especificada. Se não houver tags de segurança no NSX-V que correspondam ao valor da chave `nsxSecurityTag` especificado, a implantação falhará.

Observação A marcação de segurança do NSX-V requer que a máquina esteja conectada a uma rede do NSX-V. Se a máquina estiver conectada a uma rede do vSphere, a marcação de segurança do NSX-V será ignorada. Em ambos os casos, a máquina do vSphere também é marcada.

O NSX-T não tem uma tag de segurança separada. Qualquer tag especificada no recurso de processamento no modelo de nuvem fará com que a VM implantada seja associada a todas as tags especificadas no NSX-T. Para NSX-T, incluindo NSX-T com a Política, tags de VM também são expressas como um par de valores-chave no modelo de nuvem. A configuração `key` equivale à configuração `scope` no NSX-T, enquanto a configuração `value` equivale a `Tag Name` especificada em NSX-T.

Observe que se você tiver usado o Assistente de migração do vRealize Automation V2T para migrar suas contas de nuvem do NSX-V para o NSX-T, incluindo o NSX-T com Política, o assistente de migração criará um `nsxSecurityTag` par de chave/valor. Neste cenário, ou se o `nsxSecurityTag` for por qualquer motivo explicitamente especificado em um modelo de nuvem para uso com o NSX-T, incluindo o NSX-T com Política, a implantação criará uma tag de VM com uma configuração de Escopo vazia com um nome de Tag que corresponde ao `value` especificada. Quando você visualizar essas tags no NSX-T, a coluna Escopo ficará vazia.

Para evitar confusão, não use pares de chaves `nsxSecurityTag` quando para o NSX-T. Se você especificar um par de chave/valor `nsxSecurityTag` para uso com o NSX-T, incluindo o NSX-T com Política, a implantação criará uma tag de VM com uma configuração de Escopo vazia com um nome de tag que corresponde ao `value` especificado. Quando você visualizar essas tags no NSX-T, a coluna Escopo ficará vazia.

Usando políticas de isolamento de aplicativos em regras de firewall do grupo de segurança sob demanda

Você pode usar uma política de isolamento de aplicativos para permitir somente o tráfego interno entre os recursos provisionados pelo modelo de nuvem. Com o isolamento de aplicativos, as máquinas provisionadas pelo modelo de nuvem podem se comunicar entre si, mas não podem se conectar fora do firewall. Você pode criar uma política de isolamento de aplicativos no perfil de rede. Também pode especificar o isolamento de aplicativos em um design de modelo de nuvem usando um grupo de segurança sob demanda com uma regra de firewall Negar ou uma rede privada ou de saída.

Uma política de isolamento de aplicativo é criada com uma precedência mais baixa. Se você aplicar várias políticas, as políticas com o maior peso terão precedência.

Quando você cria uma política de isolamento de aplicativo, um nome de política é gerado automaticamente. A política também é disponibilizada para reutilização em outros designs de modelo de nuvem e iterações específicas do projeto e do endpoint de recurso associados. O nome da política de isolamento de aplicativos não é visível no modelo de nuvem, mas é visível como uma propriedade personalizada na página do projeto (**Infraestrutura > Administração > Projetos**) após a implantação do design de modelo de nuvem.

Para o mesmo endpoint associado em um projeto, qualquer implantação que exija um grupo de segurança sob demanda para o isolamento de aplicativos pode usar a mesma política de isolamento de aplicativos. Depois de criada, a política não pode ser excluída. Quando você especifica uma política de isolamento de aplicativos, o vRealize Automation procura essa política dentro do projeto e em relação ao endpoint associado. Se ele encontrar a política, esta será reutilizada. Caso contrário, ele a criará. O nome da política de isolamento de aplicativo só estará visível após sua implantação inicial na lista de propriedades personalizadas do projeto.

Usando grupos de segurança no desenvolvimento iterativo de modelos de nuvem

Ao alterar as restrições do grupo de segurança durante o desenvolvimento iterativo, em que o grupo de segurança não está associado a uma máquina no modelo de nuvem, o grupo de segurança é atualizado na iteração conforme especificado. No entanto, quando o grupo de segurança já está associado a uma máquina, a reimplantação falha. Você deve desanexar os grupos de segurança existentes e/ou propriedades de recursos do `securityGroupType` de máquinas associadas durante o desenvolvimento iterativo de modelos de nuvem e fazer a reassociação entre cada reimplantação. O fluxo de trabalho necessário é o seguinte, supondo que você tenha implantado inicialmente o modelo de nuvem.

- 1 No designer de modelos do Cloud Assembly, desanexe o grupo de segurança de todas as suas máquinas associadas no modelo de nuvem.
- 2 Reimplante o modelo clicando em **Atualizar uma implantação existente**.
- 3 Remova as propriedades `securityGroupType` e/ou tags de restrição de grupo de segurança existentes no modelo.
- 4 Adicione novas propriedades `securityGroupType` e/ou tags de restrição de grupo de segurança no modelo.

- 5 Associe as novas instâncias de propriedades `securityGroupType` e/ou tags de restrição de grupo de segurança às máquinas no modelo.
- 6 Reimplante o modelo clicando em **Atualizar uma implantação existente**.

Operações de dia 2 disponíveis

Para obter uma lista de operações comuns de dia 2 disponíveis para recursos de modelo de nuvem e implantação, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Saiba mais

Para obter informações sobre como usar um grupo de segurança para isolamento de rede, consulte [Recursos de segurança no vRealize Automation](#).

Para obter informações sobre como usar grupos de segurança em perfis de rede, consulte [Saiba mais sobre perfis de rede no vRealize Automation](#) e [Usando configurações de grupos de segurança em perfis de rede e designs de modelo de nuvem no vRealize Automation](#).

Para obter exemplos de uso de grupos de segurança em modelos de nuvem, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Mais informações sobre recursos de balanceador de carga em modelos de nuvem do vRealize Automation

Ao criar ou editar seus modelos de nuvem do vRealize Automation, use os recursos de balanceador de carga mais apropriados para os seus objetivos.

Você pode usar recursos do balanceador de carga do NSX e independentes de nuvem em um modelo de nuvem para controlar o balanceamento de carga em uma implantação.

O balanceador de carga independente de nuvem pode ser implantado em várias nuvens. Um balanceador de carga específico da nuvem pode especificar configurações e recursos avançados, que estão disponíveis somente para uma nuvem ou topologia específica. As propriedades específicas da nuvem estão disponíveis no tipo de recurso do balanceador de carga do NSX (Cloud.NSX.LoadBalancer). Se você adicionar essas propriedades em um balanceador de carga independente de nuvem (Cloud.LoadBalancer), elas serão ignoradas se, por exemplo, um balanceador de carga do Amazon Web Services ou Microsoft Azure é provisionado, mas serão respeitadas se um balanceador de carga NSX-V ou NSX-T for provisionado. Escolha um dos tipos de recursos de balanceador de carga disponíveis com base nas condições do seu modelo de nuvem do vRealize Automation.

Não é possível conectar um recurso de balanceador de carga diretamente a um recurso de grupo de segurança na tela de design.

Recurso de balanceador de carga independente de nuvem

Use um balanceador de carga independente de nuvem quando quiser especificar características de rede para qualquer tipo de máquina de destino.

Você adiciona um balanceador de carga independente de nuvem usando o recurso **Balanceador de Carga > Independente de Nuvem** na página de design do modelo de nuvem. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.LoadBalancer`. O recurso padrão é exibido como:

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```

Recurso de balanceador de carga do NSX

Use um balanceador de carga do NSX quando o modelo de nuvem contiver características específicas do NSX-V ou NSX-T (métodos de API de Política ou API de Gerente). Você pode anexar um ou mais balanceadores de carga a uma rede NSX-V ou NSX-T ou a máquinas que estão associadas a uma rede NSX-V ou NSX-T.

Você adiciona um NSX balanceador de carga usando o recurso do **balanceador de carga > NSX**. O recurso é exibido no código do modelo de nuvem como um tipo de recurso `Cloud.NSX.LoadBalancer`. O recurso padrão é exibido como:

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

Opções de balanceador de carga no código do modelo de nuvem

Adicionar um ou mais recursos de balanceador de carga ao seu modelo de nuvem permite especificar as seguintes configurações. Alguns exemplos estão disponíveis em [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

O protocolo HTTP tem suporte para todos os balanceadores de carga sob demanda.

O protocolo HTTPS tem suporte apenas para balanceadores de carga sob demanda que estão associados a uma conta de nuvem do NSX-T cujo modo NSX está definido como **Política**. Contas de nuvem do NSX-T cujo modo NSX está definido como **Manager** não podem usar o protocolo HTTPS.

■ Especificação da máquina

Você pode especificar recursos de máquina nomeados para participar de um pool de balanceamento de carga. Como alternativa, você pode especificar que um NIC de máquina específico participe do pool do balanceador de carga.

Essa opção está disponível somente para o recurso do balanceador de carga **NSX** (`Cloud.NSX.LoadBalancer`).

- `recurso.Cloud_Machine_1.id`

Especifica que o balanceador de carga inclui a máquina identificada no código do modelo de nuvem como `Cloud_Machine_1`.

- `recurso.Cloud_Machine_2.networks[2].id`

Especifica que o balanceador de carga inclui apenas a máquina identificada no código do modelo de nuvem como `Cloud_Machine_2` quando ela é implantada no NIC de máquina `Cloud_Machine_2.networks[2]`.

- Nível de registro em log

O valor de nível de log especifica um nível de gravidade para o log de erros. As opções são NONE, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, INFO, DEBUG e NOTICE. O valor do nível de registro em log aplica-se a todos os balanceadores de carga no modelo de nuvem. Essa opção é específica para o NSX. Para balanceadores de carga que têm um pai, a configuração do nível de registro em log do pai substitui qualquer configuração de nível de registro em log em seus herdeiros.

Para obter informações relacionadas, consulte os tópicos como [Adicionar balanceadores de carga](#) na documentação do produto NSX.

- Tipo

Use um tipo de balanceador de carga para especificar um tamanho de dimensionamento. O padrão é pequeno. Essa opção é específica para o NSX. Para balanceadores de carga que têm um pai, a configuração de tipo do pai substitui qualquer configuração de tipo em seus herdeiros.

- Pequeno

Correlaciona para compacto no NSX-V e pequeno no NSX-T.

- Médio

Correlaciona para grande no NSX-V e médio no NSX-T.

- Grande

Correlaciona com o quad-grande no NSX-V e grande no NSX-T.

- Extragrande

Correlaciona com o extragrande no NSX-V e grande no NSX-T.

Para obter informações relacionadas, consulte os tópicos como [Dimensionamento dos recursos do balanceador de carga](#) na documentação do produto NSX.

Essa opção está disponível para o recurso de balanceador de carga do **NSX** (`Cloud.NSX.LoadBalancer`).

- Algoritmo (pool de servidores)

Use um método de balanceamento de algoritmo para controlar como as conexões de entrada são distribuídas entre os membros do pool de servidores. O algoritmo pode ser usado em um pool de servidores ou diretamente em um servidor. Todos os algoritmos de balanceamento de carga ignoram os servidores que atendem a qualquer uma das seguintes condições:

- O estado do administrador é definido como DESATIVADO.
- O estado do administrador é definido como GRACEFUL_DISABLED e não há nenhuma entrada de persistência correspondente.
- O estado de verificação de integridade ativo ou passivo está INATIVO.
- O limite de conexão para o máximo de conexões simultâneas do pool de servidores foi atingido.

Essa opção é específica para o NSX.

- **IP_HASH**

Seleciona um servidor com base em um hash do endereço IP de origem e do peso total de todos os servidores em execução.

Correlaciona com IP-HASH no NSX-V e NSX-T.

- **LEAST_CONNECTION**

Distribui solicitações de clientes para vários servidores com base no número de conexões já existentes no servidor. Novas conexões são enviadas para o servidor com o menor número de conexões. Ignora o peso dos membros do pool de servidores, mesmo se eles estão configurados.

Correlaciona com LEASTCONN no NSX-V e LEAST_CONNECTION no NSX-T.

- **ROUND_ROBIN**

As solicitações de clientes que entram são percorridas por uma lista de servidores disponíveis, capazes de gerenciar a solicitação. Ignora o peso dos membros do pool de servidores, mesmo se eles estão configurados. Padrão.

Correlaciona com ROUND_ROBIN no NSX-V e NSX-T.

- **WEIGHTED_LEAST_CONNECTION**

Cada servidor recebe um valor de peso que indica como ele é executado em relação a outros servidores no pool. O valor determina quantas solicitações de clientes são enviadas para um servidor em comparação com outros servidores no pool. Esse algoritmo de balanceamento de carga se concentra em usar o valor de peso para distribuir a carga de forma justa entre os recursos do servidor disponíveis. Por padrão, o valor do peso será 1 se o valor não estiver configurado e a opção de início lento estiver ativada.

Correlaciona com WEIGHTED_LEAST_CONNECTION no NSX-T. Não há correlação no NSX-V.

- **WEIGHTED_ROUND_ROBIN**

Cada servidor recebe um valor de peso que indica como ele é executado em relação a outros servidores no pool. O valor determina quantas solicitações de clientes são enviadas para um servidor em comparação com outros servidores no pool. Esse algoritmo de balanceamento de carga se concentra em usar o valor de peso para distribuir a carga de forma justa entre os recursos do servidor disponíveis.

Correlaciona com WEIGHTED_ROUND_ROBIN no NSX-T. Não há correlação no NSX-V.

■ URI

A parte esquerda do URI tem hash e é dividida pelo peso total dos servidores em execução. O resultado designa qual servidor receberá a solicitação. Isso garante que um URI sempre seja direcionado para o mesmo servidor se nenhum servidor ficar ativo ou inativo. O parâmetro do algoritmo do URI tem duas opções: `uriLength=<len>` e `uriDepth=<dep>`. O intervalo do parâmetro de comprimento deve ser $1 \leq \text{len} < 256$. O intervalo do parâmetro de profundidade deve ser $1 \leq \text{dep} < 10$. Os parâmetros de comprimento e profundidade são seguidos por um número inteiro positivo. Essas opções podem equilibrar servidores com base somente no início do URI. O parâmetro de comprimento indica que o algoritmo só deve considerar os caracteres definidos no início do URI para calcular o hash. O parâmetro de profundidade indica a profundidade máxima do diretório a ser usada para calcular o hash. Conta-se um nível para cada barra na solicitação. Se ambos os parâmetros forem especificados, a avaliação parará quando um deles for atingido.

Correlaciona com o URI no NSX-V. Não há correlação no NSX-T.

■ HTTPHEADER

O nome do cabeçalho HTTP é pesquisado em cada solicitação HTTP. O nome do cabeçalho entre parênteses não diferencia maiúsculas de minúsculas. Se o cabeçalho estiver ausente ou não contiver nenhum valor, o algoritmo round robin será aplicado. O parâmetro de algoritmo HTTPHEADER tem uma opção `headerName=<name>`.

Correlaciona com HTTPHEADER no NSX-V. Não há correlação no NSX-T.

■ URL

O parâmetro URL especificado no argumento é pesquisado na cadeia de consulta de cada solicitação HTTP GET. Se o parâmetro for seguido por um sinal de igual = e um valor, o valor terá hash e será dividido pelo peso total dos servidores em execução. O resultado designa qual servidor receberá 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 fique ativo ou inativo. Se nenhum valor ou parâmetro for encontrado, será aplicado um algoritmo round robin. O parâmetro de algoritmo URL tem uma opção `urlParam=<url>`.

Correlaciona com a URL no NSX-V. Não há correlação no NSX-T.

Para obter informações relacionadas, consulte tópicos como [Adicionar um pool de servidores para balanceamento de carga](#) na NSXdocumentação do produto.

■ Monitor de integridade

Use as opções do monitor de integridade para testar se um servidor está disponível. Há suporte para o monitoramento de integridade ativa para protocolos HTTP, ICMP, TCP e UDP. O monitoramento passivo da integridade apenas está disponível para o NSX-T.

Essa opção é específica para o NSX.

■ httpMethod

Método HTTP a ser usado para detectar o status do servidor para a solicitação de verificação de integridade. Os métodos são GET, HEAD, OPTIONS, PUT ou POST.

■ requestBody

Conteúdo do corpo da solicitação de verificação de integridade. Usado, e exigido, pelos protocolos HTTP, TCP e UDP.

■ responseBody

Verificação de integridade esperada no conteúdo do corpo da resposta. Se a cadeia de caracteres recebida corresponder a esse corpo de resposta, o servidor será considerado íntegro. Usado, e exigido, pelos protocolos HTTP, TCP e UDP.

Observação Se você usar o protocolo de monitoramento UDP, os parâmetros `UDP Data Sent` e `UDP Data Expected` serão necessários. As propriedades `requestBody` e `responseBody` mapeiam para esses parâmetros.

Essa opção está disponível para o recurso de balanceador de carga do NSX (`Cloud.NSX.LoadBalancer`).

Para obter informações relacionadas, consulte tópicos como [Configurar um monitor de integridade ativo](#) na documentação do produto NSX.

■ Verificação de integridade

Use opções de verificação de integridade para especificar como o balanceador de carga executa as verificações de integridade.

Essa opção só está disponível para o recurso do balanceador de carga do NSX (`Cloud.NSX.LoadBalancer`).

Consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#) para obter uma amostra das configurações disponíveis de verificação da integridade.

Opções de balanceador de carga e tipos de rede do NSX-V e do NSX-T

As opções do balanceador de carga dependem da rede à qual o recurso de balanceador de carga está associado no design do modelo de nuvem. Você pode configurar um balanceador de carga relativo ao tipo de rede e às condições de rede.

■ Rede sob demanda

Se os processamentos do balanceador de carga estiverem anexados a uma rede sob demanda, um novo roteador de Camada 1 será criado e anexado ao roteador de Camada 0 especificado no perfil de rede. Em seguida, o balanceador de carga é anexado ao Roteador de camada 1. O anúncio VIP do roteador de Camada 1 será habilitado se o VIP estiver em uma rede existente. Se uma rede sob demanda estiver configurada para DHCP, ela e o balanceador de carga compartilharão o roteador de Camada 1.

■ Rede existente

Se o balanceador de carga estiver anexado a uma rede existente, ele será criado com o Roteador de camada 1 da rede existente. Um novo de balanceador de carga será criado somente se não houver um balanceador de carga anexado ao roteador de Camada 1. Se o balanceador de carga já existir, novos servidores virtuais serão anexados a ele. Se a rede existente não estiver conectada a um Roteador de camada 1, um novo Roteador de camada 1 será criado e anexado a um Roteador de camada 0 definido no perfil de rede, o anúncio VIP do Roteador de camada 1 não será ativado.

O vRealize Automation não oferece suporte a um balanceador de carga de dupla articulação (balanceador de carga inline) do NSX-T em duas redes existentes diferentes. Observe que, em um cenário de balanceador de carga de dupla articulação, o uplink de VIP está em uma rede existente, enquanto as máquinas-membro do pool estão conectadas a uma rede sob demanda. Para especificar o balanceamento de carga ao usar uma rede existente, você deve configurar um balanceador de carga de articulação única em que a mesma rede existente é usada para o VIP do balanceador de carga e para as máquinas-membro do pool. No entanto, a partir do vRealize Automation 8.4.2, se você estiver usando um balanceador de carga selecionado no perfil de rede, poderá fazer o balanceamento de carga entre as máquinas em duas redes existentes diferentes se houver conectividade entre elas.

■ Isolamento de rede definido no perfil de rede

Para tipos de rede `outbound` ou `private`, você pode especificar as configurações de isolamento de rede em um perfil de rede para emular um novo grupo de segurança. Como as máquinas estão anexadas a uma rede existente e as configurações de isolamento estão definidas no perfil, essa opção é semelhante a um balanceador de carga criado em uma rede existente. A diferença é que para habilitar o caminho de dados, o IP da Porta de uplink da camada 1 é adicionado ao grupo de segurança de isolamento.

Você pode especificar configurações de balanceador de carga para redes associadas ao NSX usando um recurso de balanceador de carga do NSX no design do modelo de nuvem.

Para saber mais, consulte a postagem de blog da VMware [vRA Cloud Assembly Load Balancer with NSX-T Deep Dive](#).

Redefinindo o nível de log ou as configurações de tipo quando vários balanceadores de carga compartilham um NSX-T de Camada 1 ou um NSX-V Edge

Ao usar um modelo de nuvem que contém vários balanceadores de carga que compartilham um roteador de Camada 1 no endpoint do NSX-T ou um roteador de Edge no endpoint do NSX-V, redefinir o nível de log ou as configurações de tipo em um dos recursos do balanceador de carga não atualiza as configurações dos outros balanceadores de carga. Configurações sem correspondência causam inconsistências no NSX. Para evitar inconsistências ao redefinir essas configurações de nível de log e/ou tipo, use os mesmos valores de reconfiguração para todos os recursos do balanceador de carga no modelo de nuvem que compartilham um Tier 1 ou Edge no seu endpoint do NSX associado.

Operações de dia 2 disponíveis

Quando você expande ou reduz uma implantação que contém um balanceador de carga, este é configurado para incluir máquinas recém-adicionadas ou para interromper máquinas de balanceamento de carga destinadas a destruição.

Para obter uma lista de operações comuns do dia 2 que estão disponíveis para modelos de nuvem e implantações, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Saiba mais

Para obter informações sobre como definir configurações de balanceador de carga em um perfil de rede, consulte [Saiba mais sobre perfis de rede no vRealize Automation](#).

Para exemplos de designs de modelo de nuvem que incluem balanceadores de carga, consulte [Redes, recursos de segurança e balanceadores de carga no vRealize Automation](#).

Modelo de nuvem habilitado para Puppet com acesso de nome de usuário e senha

Neste exemplo, é adicionado o gerenciamento de configuração do Puppet a um modelo de nuvem implantado em um recurso de processamento do vCenter com acesso de nome de usuário e senha.

Este procedimento mostra um exemplo de como criar um recurso implantável ativado para Puppet que requer autenticação de nome de usuário e senha. O acesso de nome de usuário e senha significa que o usuário deve fazer login manualmente a partir do recurso de processamento da máquina principal Puppet a fim de invocar o gerenciamento de configuração do Puppet.

Opcionalmente, é possível configurar a autenticação de acesso remoto que configura o gerenciamento de configuração em um modelo de nuvem para que o recurso de processamento cuide da autenticação com a máquina principal do Puppet. Com o acesso remoto ativado, o recurso de processamento gera automaticamente uma chave para satisfazer a autenticação de senha. Um nome de usuário válido ainda é necessário.

Consulte [Exemplos de modelo de nuvem de gerenciamento de configuração do AWS Puppet](#) e [Exemplos de modelo de nuvem de configuração do Puppet no vCenter](#) para obter mais exemplos de como configurar diferentes cenários do Puppet nos blueprints do Cloud Assembly.

Pré-requisitos

- Configure uma instância do Puppet Enterprise em uma rede válida.
- Adicione sua instância do Puppet Enterprise ao Cloud Assembly usando o recurso Integrações. Consulte [Configurar a integração com o Puppet Enterprise no Cloud Assembly](#)
- Configure uma conta do vSphere e um recurso de processamento do vCenter.

Procedimentos

- 1 Adicione um componente de gerenciamento de configuração do Puppet a um recurso de processamento do vSphere na tela para o modelo de nuvem desejado.
 - a Selecione **Infraestrutura > Gerenciar > Integrações**.
 - b Clique em **Adicionar Integração** e selecione Puppet.
 - c Digite as informações apropriadas na página de configuração do Puppet.

| Configuração | Descrição | Valor de exemplo |
|--------------------------------------|--|---|
| Nome do Host | Nome do host ou endereço IP da máquina primária do Puppet | Puppet-Ubuntu |
| Porta SSH | Porta SSH para comunicação entre o Cloud Assembly e a máquina primária do Puppet. (Opcional) | N/D |
| Segredo de Autoassinatura | O segredo compartilhado configurado na máquina primária do Puppet que os nós devem fornecer para suportar as solicitações de certificado de autoassinatura. | Específico do usuário |
| Localização | Indica se a máquina primária do Puppet está em uma nuvem privada ou pública. Observação A implantação entre nuvens só terá suporte se houver conectividade entre o recurso de processamento de implantação e a máquina primária do Puppet. | |
| Cloud proxy | Não é necessário para contas de nuvem pública, como o Microsoft Azure ou o Amazon Web Services. Se estiver usando uma conta de nuvem baseada no vCenter, selecione o cloud proxy apropriado para a sua conta. | N/D |
| Nome de Usuário | Nome de usuário SSH e RBAC para a máquina primária do Puppet. | Específico do usuário. O valor de YAML é '\${input.username}' |
| Senha | Senha SSH e RBAC para a máquina primária do Puppet. | O valor de YAML específico do usuário é '\${input.password}' |
| Usar comandos sudo para este usuário | Selecione para usar os comandos sudo para o procidd. | verdadeiro |
| Nome | Nome da máquina primária do Puppet. | PEMasterOnPrem |
| Descrição | | |

- 2 Adicione as propriedades username e password ao Puppet YAML, conforme mostrado no exemplo a seguir.

- 3 Certifique-se de que o valor da propriedade `remoteAccess` para o YAML do modelo de nuvem Puppet esteja definido como `authentication: username and password`, conforme mostrado no exemplo abaixo.

Exemplo: Código YAML do nome de usuário e senha do vCenter

O exemplo a seguir mostra o código YAML representativo para adicionar nome de usuário e autenticação de senha em um recurso de processamento do vCenter.

```
inputs:
  username:
    type: string
    title: Username
    description: Username to use to install Puppet agent
    default: puppet
  password:
    type: string
    title: Password
    default: VMware@123
    encrypted: true
    description: Password for the given username to install Puppet agent
resources:
  Puppet-Ubuntu:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      imageRef: >-
        https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ubuntu-16.04-server-
cloudimg-amd64.ova
      remoteAccess:
        authentication: usernamePassword
        username: '${input.username}'
        password: '${input.password}'
  Puppet_Agent:
    type: Cloud.Puppet
    properties:
      provider: PEMasterOnPrem
      environment: production
      role: 'role::linux_webserver'
      username: '${input.username}'
      password: '${input.password}'
      host: '${Puppet-Ubuntu.*}'
      useSudo: true
      agentConfiguration:
        certName: '${Puppet-Ubuntu.address}'
```

Exemplos de modelo de nuvem de gerenciamento de configuração do AWS Puppet

Há várias opções para configurar modelos de nuvem para oferecer suporte ao gerenciamento de configuração baseado em Puppet nos recursos de processamento do AWS.

Gerenciamento do Puppet no AWS com nome de usuário e senha

| Exemplo de... | Amostra de blueprint YAML |
|---|--|
| autenticação da configuração de nuvem em qualquer Imagem da Máquina Amazon com suporte. | <pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6/+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} !requiretty" >> /etc/sudoers.d/\${input.username} Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre> |
| Autenticação de configuração de nuvem em uma Imagem da Máquina Amazon personalizada com um usuário existente. | <pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 </pre> |

| Exemplo de... | Amostra de blueprint YAML |
|---------------|---|
| | <pre> resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config runCmd: - sudo sed -e 's/.*PasswordAuthentication no.*/ PasswordAuthentication yes/' -i /etc/ssh/sshd_config - sudo service sshd restart Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre> |

Gerenciamento do Puppet no AWS com a PublicPrivateKey gerada

| Exemplo de... | Amostra de blueprint YAML |
|--|--|
| Autenticação remoteAccess.authentication no AWS com o acesso à generatedPublicPrivateKey. | <pre> inputs: {} resources: Machine: type: Cloud.AWS.EC2.Instance properties: flavor: small imageRef: ami-a4dc46db remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' useSudo: true </pre> |

Exemplos de modelo de nuvem de configuração do Puppet no vCenter

Há várias opções para configurar modelos de nuvem a fim de oferecer suporte ao gerenciamento de configuração baseado em Puppet nos recursos de processamento do vCenter.

Puppet no vSphere com nome de usuário e autenticação de senha

O exemplo a seguir mostra um código YAML de exemplo para Puppet em um OVA do vSphere com autenticação de nome de usuário e senha.

Tabela 6-4.

| Exemplo de... | Amostra de blueprint YAML |
|---|---|
| O código YAML para Puppet em um OVA do vSphere com autenticação de nome de usuário e senha. | <pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre> |
| O código YAML para Puppet em um OVA do vSphere com autenticação de nome de usuário e senha no recurso de processamento. | <pre> inputs: username: type: string title: Username default: puppet </pre> |

Tabela 6-4. (continuação)

| Exemplo de... | Amostra de blueprint YAML |
|---|--|
| | <pre> password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre> |
| O código YAML para Puppet em um vCenter com autenticação de senha ativada para acesso remoto no recurso de processamento. | <pre> inputs: username: type: string title: Username description: Username to use to install Puppet agent default: puppet password: type: string title: Password default: VMware@123 encrypted: true </pre> |

Tabela 6-4. (continuação)

| Exemplo de... | Amostra de blueprint YAML |
|---------------|--|
| | <pre> description: Password for the given username to install Puppet agent resources: Puppet-Ubuntu: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.password}' Puppet_Agent: type: Cloud.Puppet properties: provider: PEMasterOnPrem environment: production role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' host: '\${Puppet-Ubuntu.*}' useSudo: true agentConfiguration: certName: '\${Puppet-Ubuntu.address}' </pre> |

Puppet no vSphere com autenticação PublicPrivateKey gerada

Tabela 6-5.

| Exemplo de... | Amostra de blueprint YAML |
|---|---|
| O código YAML para Puppet em um OVA do vSphere com autenticação de PublicPrivateKey gerada no recurso de processamento. | <pre> inputs: {} resources: Machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' - echo "Defaults:\${input.username}" </pre> |

Esquema de propriedades de recursos do vRealize Automation

O editor de infraestrutura como código do vRealize Automation permite que você clique ou passe o mouse para obter ajuda sobre a sintaxe e a complementação do código. Para exibir o conjunto completo de propriedades de recurso de modelo de nuvem, às vezes chamadas de propriedades personalizadas, consulte o esquema de recursos consolidado.

O esquema está disponível no site do VMware {code}. Siga o link e clique em **Modelos** para listar os objetos de recursos que estão disponíveis para modelos de nuvem, anteriormente chamados de blueprints.

- [Esquema de tipo de recurso do vRealize Automation no VMware {code}](#)

Propriedades especiais do Cloud Assembly

O Cloud Assembly oferece suporte a um pequeno número de propriedades que podem ser úteis fora de ambientes de produção ou em outras situações especiais. As propriedades não aparecem no esquema.

Cuidado As propriedades a seguir devem ser aplicadas apenas nos casos em que a personalização do SO guest não está sendo testada ou esperada.

| | |
|---------------|---|
| awaitIp | <p>Por padrão, o status de provisionamento do vRealize Automation não será relatado como Concluído até que o SO guest esteja totalmente ligado e a configuração tenha sido concluída.</p> <p>O uso de <code>awaitIp: false</code> permite que o provisionamento seja concluído mesmo que a configuração completa não ocorra.</p> <p>ATENÇÃO: o uso desta configuração conclui o processo de provisionamento mais cedo, mas pode resultar em uma máquina não configurada sem endereço IP.</p> |
| awaitHostName | <p>Semelhante à <code>awaitIp</code>, o uso de <code>awaitHostName: false</code> permite que o provisionamento seja concluído, mesmo que a máquina possa não ter sido configurada com um nome de host.</p> |

Outras maneiras de criar modelos do Cloud Assembly

Além de construir um modelo do Cloud Assembly em uma tela em branco, você pode aproveitar o código existente.

Clonagem de modelos de nuvem

Para clonar um modelo, vá para **Projetar**, selecione uma origem e clique em **Clonar**. Um modelo de nuvem é clonado para criar uma cópia com base na origem e, em seguida, atribuir o clone a um novo projeto ou usá-lo como código inicial para um novo aplicativo.

Carregar e baixar

É possível carregar, baixar e compartilhar o código YAML do modelo de nuvem de qualquer forma que faça sentido para o seu site. É possível até mesmo modificar o código do modelo usando editores externos e ambientes de desenvolvimento.

Observação Uma boa maneira de validar o código de modelo compartilhado é inspecioná-lo no editor de código do Cloud Assembly na página de projeto.

Integrando o Cloud Assembly a um repositório

Um repositório de controle de origem do Git integrado pode disponibilizar modelos de nuvem para usuários qualificados como base para uma nova implantação. Consulte [Como usar a integração do Git no Cloud Assembly](#).

Estendendo e automatizando ciclos de vida de aplicativos com extensibilidade

É possível estender ciclos de vida de aplicativos usando ações de extensibilidade ou fluxos de trabalho do vRealize Orchestrator com assinaturas de extensibilidade.

Com a extensibilidade do Cloud Assembly, é possível atribuir uma ação de extensibilidade ou um fluxo de trabalho do vRealize Orchestrator a um evento usando assinaturas. Quando o evento especificado ocorre, a assinatura inicia a ação ou fluxo de trabalho a ser executado e todos os assinantes são notificados.

Ações de extensibilidade

Ações de extensibilidade são scripts pequenos e leves de código usados para especificar uma ação e como essa ação deve ser realizada. Você pode importar ações de extensibilidade de modelos de ação do Cloud Assembly predefinidos ou de um arquivo ZIP. Também pode usar o editor de ações para criar scripts personalizados para suas ações de extensibilidade. Quando vários scripts de ação são vinculados em um script, você cria um fluxo de ação. Ao usar fluxos de ação, é possível criar uma sequência de ações. Para obter informações sobre como usar fluxos de ação, consulte [O que é um fluxo de ação](#).

Fluxos de trabalho do vRealize Orchestrator

Ao integrar o Cloud Assembly ao seu ambiente existente do vRealize Orchestrator, você pode usar fluxos de trabalho nas suas assinaturas de extensibilidade.

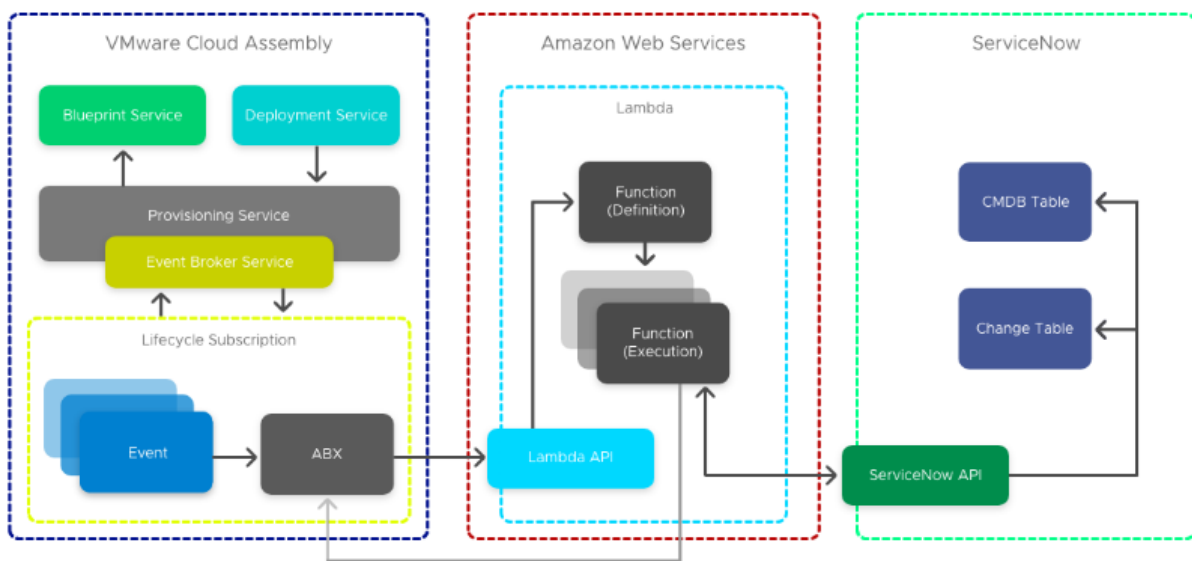
Assinaturas de ação de extensibilidade

É possível atribuir uma ação de extensibilidade a uma assinatura do Cloud Assembly para estender o ciclo de vida do aplicativo.

Observação As seguintes assinaturas são exemplos de caso de uso e não abrangem toda a funcionalidade da ação de extensibilidade.

Como integrar o Cloud Assembly com o ServiceNow usando ações de extensibilidade

Com as ações de extensibilidade, é possível integrar o Cloud Assembly a um ITSM empresarial, como o ServiceNow.

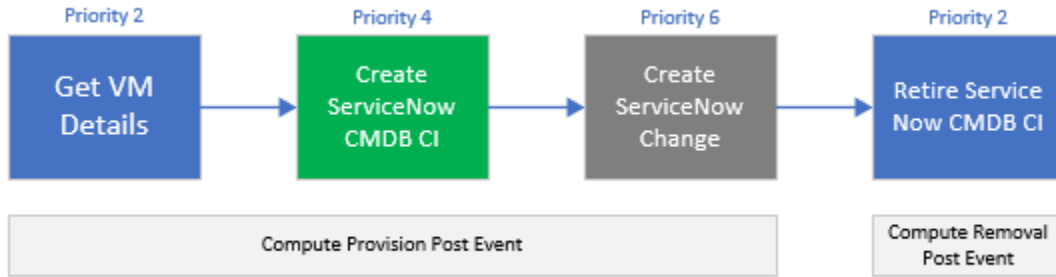


Os usuários corporativos normalmente integram sua plataforma de gerenciamento de nuvem a uma plataforma de gerenciamento de serviços de TI (ITSM) e a um database de gerenciamento de configuração (CMDB) para conformidade. Seguindo este exemplo, é possível integrar o Cloud Assembly ao ServiceNow para CMDB e ITSM usando scripts de ação de extensibilidade.

Observação Também é possível integrar o ServiceNow ao Cloud Assembly usando fluxos de trabalho do vRealize Orchestrator. Para obter informações sobre como integrar o ServiceNow usando fluxos de trabalho, consulte [Como integrar o Cloud Assembly para o ITSM ao ServiceNow usando fluxos de trabalho do vRealize Orchestrator](#).

Para criar essa integração, serão usados quatro scripts de ação de extensibilidade. Os três primeiros scripts são iniciados em sequência durante o provisionamento no provisionamento de processamento após o evento. O quarto script é disparado na remoção de processamento após evento.

Para obter mais informações sobre tópicos de eventos, consulte [Tópicos de eventos fornecidos com o Cloud Assembly](#).



Obter Detalhes da VM

O script Obter Detalhes da VM adquire detalhes adicionais de payload necessários para a criação de CI e um token de identidade, que é armazenado no Amazon Web Services Systems Manager Parameter Store (SSM). Além disso, esse script atualiza `customProperties` com propriedades adicionais para uso posterior.

Criar CI do CMDB do ServiceNow

O script Criar CI do CMDB do ServiceNow passa a URL da instância do ServiceNow como uma entrada e armazena a instância no SSM para atender aos requisitos de segurança. Esse script também lê a resposta do identificador de registro exclusivo do CMDB do ServiceNow (`sys_id`). Ele o transmite como saída e grava a propriedade personalizada `serviceNowSysId` durante a criação. Esse valor é usado para marcar a CI como desativada quando a instância é destruída.

Observação Talvez seja preciso alocar permissões adicionais à sua função do vRealize Automation services na Amazon Web Services para permitir que o Lambda acesse o SSM Parameter Store.

Criar Alteração do ServiceNow

Esse script conclui a integração do ITSM passando a URL da instância do ServiceNow como uma entrada e armazenando as credenciais do ServiceNow como SSM para atender aos requisitos de segurança.

Criar Alteração do ServiceNow

O script de desativação de CI do ServiceNow solicita que o ServiceNow pare e marque a CI como desativada com base na propriedade personalizada `serviceNowSysId` que foi criada no script de criação.

Pré-requisitos

- Antes de configurar esta integração, filtre todas as assinaturas de evento com a propriedade condicional de modelo de nuvem: `event.data["customProperties"]`
`["enable_servicenow"] === "true"`

Observação Essa propriedade existe em modelos de nuvem que necessitam de uma integração do ServiceNow.

- Baixe e instale o Python.

Para obter mais informações sobre filtragem de assinaturas, consulte [Criar uma assinatura de extensibilidade](#).

Procedimentos

- 1 Abra um prompt de linha de comando na Máquina Virtual.
- 2 Execute o script Obter Detalhes da VM.

```
from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    baseUri = inputs['url']
    casToken = client.get_parameter(Name="casToken",WithDecryption=True)

    url = baseUri + "/iaas/login"
    headers = {"Accept":"application/json","Content-Type":"application/json"}
    payload = {"refreshToken":casToken['Parameter']['Value']}

    results = requests.post(url,json=payload,headers=headers)

    bearer = "Bearer "
    bearer = bearer + results.json()["token"]

    deploymentId = inputs['deploymentId']
    resourceId = inputs['resourceIds'][0]

    print("deploymentId: " + deploymentId)
    print("resourceId:" + resourceId)

    machineUri = baseUri + "/iaas/machines/" + resourceId
    headers = {"Accept":"application/json","Content-Type":"application/json",
    "Authorization":bearer }
    resultMachine = requests.get(machineUri,headers=headers)
    print("machine: " + resultMachine.text)

    print( "serviceNowCPUCount: " + json.loads(resultMachine.text)["customProperties"]
    ["cpuCount"] )
    print( "serviceNowMemoryInMB: " + json.loads(resultMachine.text)["customProperties"]
    ["memoryInMB"] )

    #update customProperties
    outputs = {}
    outputs['customProperties'] = inputs['customProperties']
    outputs['customProperties']['serviceNowCPUCount'] = int(json.loads(resultMachine.text)
    ["customProperties"]["cpuCount"])
    outputs['customProperties']['serviceNowMemoryInMB'] = json.loads(resultMachine.text)
    ["customProperties"]["memoryInMB"]
    return outputs
```

3 Execute a ação de criação do item de configuração do CMDB.

```
from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):

    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    table_name = "cmdb_ci_vmware_instance"
    url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'name': inputs['customProperties']['serviceNowHostname'],
        'cpus': int(inputs['customProperties']['serviceNowCPUCount']),
        'memory': inputs['customProperties']['serviceNowMemoryInMB'],
        'correlation_id': inputs['deploymentId'],
        'disks_size': int(inputs['customProperties']['provisionGB']),
        'location': "Sydney",
        'vcenter_uuid': inputs['customProperties']['vcUuid'],
        'state': 'On',
        'sys_created_by': inputs['__metadata']['userName'],
        'owned_by': inputs['__metadata']['userName']
    }
    results = requests.post(
        url,
        json=payload,
        headers=headers,
        auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
    )
    print(results.text)

    #parse response for the sys_id of CMDB CI reference
    if json.loads(results.text)['result']:
        serviceNowResponse = json.loads(results.text)['result']
        serviceNowSysId = serviceNowResponse['sys_id']
        print(serviceNowSysId)

    #update the serviceNowSysId customProperty
    outputs = {}
    outputs['customProperties'] = inputs['customProperties']
    outputs['customProperties']['serviceNowSysId'] = serviceNowSysId;
    return outputs
```

4 Execute o script de ação de criação.

```
from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
```

```

snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
table_name = "change_request"
url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
payload = {
    'short_description': 'Provision CAS VM Instance'
}
results = requests.post(
    url,
    json=payload,
    headers=headers,
    auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
)
print(results.text)

```

Resultados

O Cloud Assembly foi integrado com êxito ao ITSM ServiceNow.

Próximo passo

Quando desejar, será possível desativar sua CI usando a ação de desativação do item de configuração do CMDB:

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    tableName = "cmdb_ci_vmware_instance"
    sys_id =inputs['customProperties']['serviceNowSysId']
    url = "https://" + inputs['instanceUrl'] + "/api/now/"+tableName+"/"+{0}".format(sys_id)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'state': 'Retired'
    }

    results = requests.put(
        url,
        json=payload,
        headers=headers,
        auth=(inputs['username'], inputs['password'])
    )
    print(results.text)

```

Para obter mais informações sobre como usar ações de extensibilidade para integrar o ServiceNow no Cloud Assembly, consulte [Estender o Cloud Assembly com Extensibilidade com base na ação para a integração do ServiceNow](#).

Como marcar máquinas virtuais durante o provisionamento usando ações de extensibilidade

Use ações de extensibilidade junto com assinaturas para automatizar e simplificar a marcação de VMs.

Como administrador de nuvem, é possível criar implantações que são automaticamente marcadas com entradas e saídas especificadas usando as ações e as assinaturas de extensibilidade.

Quando uma nova implantação é criada no projeto que contém a tag de assinatura da VM, o evento de implantação dispara o script da Tag VM para ser executado e as tags são aplicadas automaticamente. Isso poupa tempo, promove a eficiência e permite um gerenciamento de implantação mais fácil.

Pré-requisitos

- Acesso a credenciais de administrador de nuvem.
- Função da Amazon Web Services para funções do Lambda.

Procedimentos

- 1 Navegue até **Extensibilidade > Library > Ações > Nova Ação** e crie uma nova ação com os seguintes parâmetros.

| Parâmetro | Descrição |
|-------------------|--|
| Nome da Ação | Nome da ação de extensibilidade, preferencialmente usando TagVM como prefixo ou sufixo. |
| Projeto | A ação de extensibilidade é testada em relação a esse projeto. |
| Modelo de ação | Tag VM |
| Tempo de Execução | Python |
| Origem do script | Script de gravação |

- 2 Insira **Manipulador** como **Função principal**.
- 3 Adicione entradas de marcação para testar a ação de extensibilidade.
Por exemplo, `resourceNames = ["DB_VM"]` e `target = world`.
- 4 Para salvar a ação, clique em **Salvar**.
- 5 Para testar sua ação, clique em **Testar**.
- 6 Para sair do editor de ações, clique em **Fechar**.
- 7 Navegue até **Extensibilidade > Assinaturas**.
- 8 Clique em **Nova Assinatura**.

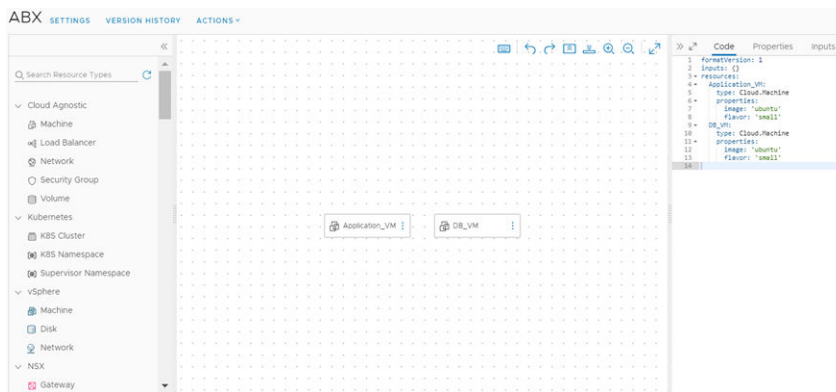
9 Digite os seguintes detalhes da assinatura.

| Detalhe | Configuração |
|------------------------|--|
| Tópico de evento | Selecione um tópico de evento relacionado à fase de marcação da VM. Por exemplo, Alocação de Processamento. Observação As tags devem fazer parte dos parâmetros de evento do tópico de evento selecionado. |
| Bloqueio | Defina o tempo limite para a assinatura como 1 minuto. |
| Ação/Fluxo de trabalho | Selecione um tipo executável de ação de extensibilidade e selecione sua ação de extensibilidade personalizada. |

10 Para salvar sua assinatura de ação de extensibilidade personalizada, clique em **Salvar**.

11 Navegue até **Projetar > Modelos de Nuvem** e crie um modelo de nuvem a partir de uma tela em branco.

12 Adicione duas máquinas virtuais ao modelo de nuvem: Application_VM e DB_VM.



13 Para implantar as VMs, clique em **Implantar**.

14 Durante a implantação, verifique se o evento é iniciado e se a ação de extensibilidade é executada.

15 Para verificar se as tags foram aplicadas corretamente, navegue até **Recursos > Recursos > Máquinas Virtuais**.

Como posso configurar um nome de controlador de interface de rede usando ações de extensibilidade

Você pode configurar o nome da interface de um controlador de interface de rede (network interface controller, NIC) usando chamadas de API IaaS aplicadas por meio de ações de extensibilidade.

Para configurar o nome da interface de um NIC, você deve fazer chamadas `GET` e `PATCH` para a API IaaS do vRealize Automation. Ao fazer uma chamada `GET` para `https://fqdn_do_seu_vRA/iaas/api/machines/{id}`, você pode recuperar o link do NIC referente ao recurso de processamento que deseja modificar. Depois disso, você pode fazer uma chamada `PATCH` para `https://fqdn_do_seu_vRA/iaas/api/machines/{id}/network-interfaces/{nicId}`, que inclui o nome da interface do NIC como payload, para adicionar um novo nome ao NIC.

O cenário a seguir usa um script Python de amostra que pode ser usado para a configuração do nome da interface do NIC. Para seus próprios casos de uso, você pode usar um script e uma linguagem de script diferente, como Node.js.

Pré-requisitos

- Você somente pode configurar o nome da interface do NIC antes de provisionar um recurso de processamento. Portanto, apenas o tópico do evento **Provisionamento de Processamento** pode ser selecionado para assinaturas de extensibilidade relevantes.
- Você somente pode configurar os nomes de interface para NICs que usam o Microsoft Azure como provedor.

Procedimentos

- 1 Crie a ação de extensibilidade.
 - a Navegue até **Extensibilidade > Ações**.
 - b Clique em **Nova Ação**.
 - c Insira um nome e um projeto para a ação de extensibilidade e clique em **Seguinte**.

- d Adicione o script de configuração da NIC.

Veja abaixo um script de exemplo do Python:

```
import json

def handler(context, inputs):

    # Get the machine info, which contains machine nic link
    response = context.request('/iaas/api/machines/'+inputs["resourceIds"][0], "GET",
    {})

    # Build PATCH machine nic payload here
    name = "customized-nic-02";
    data = {'name':name};

    # Convert machine data string to json object
    response_json = json.loads(response["content"])

    # Patch machine nic
    response_patch = context.request(response_json["_links"]["network-interfaces"]
    ["hrefs"][0] + "?apiVersion=2021-07-15", 'PATCH', data)

    # return value is empty since we are not changing any compute provisioning
    parameters
    outputs = {}
    return outputs
```

O script de exemplo anterior executa duas operações principais por meio da API IaaS. Primeiro, o script usa uma chamada `GET` para recuperar o link do NIC e, depois, usa uma chamada `PATCH` para aplicar o nome da interface. Nesse exemplo, o nome da interface do NIC está codificado no script como "customized-nic-02".

- e Para concluir a edição da ação de extensibilidade, clique em **Salvar**.

2 Crie uma assinatura de extensibilidade.

- a Navegue até **Extensibilidade > Assinaturas**.
- b Clique em **Nova Assinatura**.
- c Insira um nome para a assinatura de extensibilidade.
- d Em **Tópico de Evento**, selecione **Provisionamento de Processamento** como o tópico do evento para a assinatura de extensibilidade.
- e Em **Ação/fluxo de trabalho**, selecione a ação de extensibilidade que você criou para a configuração do NIC.
- f Ative o bloqueio de eventos.

Ao habilitar o bloqueio, você garante que o processo de provisionamento esteja bloqueado até que a ação de extensibilidade termine sua execução.

- g Para concluir a edição da assinatura de extensibilidade, clique em **Salvar**.

Resultados

A nova assinatura de extensibilidade é executada quando um evento de provisionamento de processamento é disparado e configura o nome da interface do NIC para que os recursos de processamento sejam provisionados.

Saiba mais sobre ações de extensibilidade

A extensibilidade com base em ações usa scripts de código simplificados no Cloud Assembly para automatizar ações de extensibilidade.

A extensibilidade baseada em ações fornece uma interface de mecanismo de tempo de execução leve e flexível, na qual é possível definir pequenas ações programáveis por script e configurá-las para iniciar quando os eventos especificados em assinaturas de extensibilidade ocorrerem.

É possível criar esses scripts de código de ação de extensibilidade no Cloud Assembly, ou no seu ambiente local, e atribuí-los a assinaturas. Os scripts de ação de extensibilidade são usados para automação mais leve e simples de tarefas e etapas. Para obter mais informações sobre como integrar o Cloud Assembly a um servidor vRealize Orchestrator, consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).

A extensibilidade com base em ações fornece:

- Uma alternativa aos fluxos de trabalho do vRealize Orchestrator, usando ações programáveis por script pequenas e reutilizáveis, para personalizações e integrações leves.
- Uma maneira de reutilizar modelos de ação, que contenham ações parametrizadas reutilizáveis.

É possível criar ações de extensibilidade escrevendo um código de script de ação definido pelo usuário ou importando um código de script predefinido como um pacote .ZIP. A extensibilidade baseada em ações é compatível com Node.js, Python e ambientes de tempo de execução do PowerShell. Os tempos de execução Node.js e Python dependem do Amazon Web Services Lambda. Portanto, você deve ter uma assinatura ativa com o Amazon Web Services Identity and Access Management (IAM) e configurar a Amazon Web Services como um endpoint no Cloud Assembly. Para obter informações sobre os conceitos básicos do Amazon Web Services Lambda, consulte [ABX: extensibilidade sem servidor de serviços do Cloud Assembly](#).

Observação As ações de extensibilidade são específicas do projeto.

Como criar ações de extensibilidade

Com o Cloud Assembly, você pode criar ações de extensibilidade para uso em assinaturas de extensibilidade.

Ações de extensibilidade são maneiras altamente personalizáveis, leves e flexíveis para estender ciclos de vida de aplicativos usando códigos de script e modelos de ação definidos pelo usuário. Os modelos de ação contêm parâmetros predefinidos que ajudam a configurar a base da ação de extensibilidade.

Existem dois métodos para criar uma ação de extensibilidade:

- Gravar um código definido pelo usuário para um script de ação de extensibilidade.

Observação Escrever código definido pelo usuário no editor de ação de extensibilidade pode exigir uma conexão ativa com a Internet.

- Importar um pacote de implantação como um pacote ZIP para uma ação de extensibilidade. Para obter informações sobre como criar um pacote ZIP para ações de extensibilidade, consulte [Criar um pacote ZIP para ações de extensibilidade de tempo de execução do Python](#), [Criar um pacote ZIP para ações de extensibilidade de tempo de execução do Node.js](#) ou [Criar um pacote ZIP para ações de extensibilidade de tempo de execução do PowerShell](#).

As etapas a seguir descrevem o procedimento para criar uma ação de extensibilidade que usa a Amazon Web Services como um provedor de FaaS.

Pré-requisitos

- Associação em um projeto ativo e válido.
- Função do Amazon Web Services configurada para funções do Lambda. Por exemplo, `AWSLambdaBasicExecutionRole`.
- Função de administrador de nuvem ou permissões de `iam:PassRole` habilitadas.

Procedimentos

- 1 Selecione **Extensibilidade > Biblioteca > Ações**.
- 2 Clique em **Nova Ação**.
- 3 Insira um nome para a ação e selecione um projeto.
- 4 (Opcional) Adicione uma descrição para a sua ação.
- 5 Clique em **Seguinte**.
- 6 Pesquise e selecione um modelo de ação.

Observação Para criar uma ação personalizada sem usar um modelo de ação, selecione **Script personalizado**.

Novos parâmetros configuráveis são exibidos.

- 7 Selecione **Script de Gravação** ou **Importar pacote**.
- 8 Selecione o tempo de execução da ação.
- 9 Insira um nome de **Função principal** para o ponto de entrada da ação.

Observação Para ações importadas de um pacote ZIP, a função principal também deve incluir o nome do arquivo de script que contém o ponto de entrada. Por exemplo, se o arquivo de script principal se chamar `main.py` e seu ponto de entrada for `handler (context, inputs)`, o nome da função principal deverá ser `main.handler`.

- 10 Defina os parâmetros de entrada e saída da ação.
- 11 (Opcional) Adicione segredos ou constantes de ação de extensibilidade às suas entradas padrão.

Observação Para obter mais informações sobre segredos e constantes de ação de extensibilidade, consulte [Como posso criar segredos para uso em ações de extensibilidade](#) e [Como posso criar constantes de ação de extensibilidade](#).

- 12 (Opcional) Adicione dependências de aplicativos à ação.

Observação Para scripts do PowerShell, você pode definir suas dependências de aplicativos para que elas sejam resolvidas em relação ao repositório da Galeria do PowerShell. Para definir as dependências do aplicativo de forma que elas sejam resolvidas no repositório público, use o seguinte formato:

```
@{
    Name = 'Version'
}

e.g.

@{
    Pester = '4.3.1'
}
```

Observação Para ações importadas de um pacote ZIP, dependências de aplicativos são adicionadas automaticamente.

- 13 Para definir limites de memória e tempo limite, habilite a opção **Definir limites e tempo limite personalizados**.
- 14 Para testar a ação, clique em **Salvar** e **Testar**.

Próximo passo

Depois que a ação de extensibilidade for criada e verificada, será possível atribuí-la a uma assinatura.

Observação Assinaturas de extensibilidade usam a versão mais recente de uma ação de extensibilidade. Depois de criar uma nova versão de uma ação, clique em **Versões** no canto superior direito da janela do editor. Para liberar a versão da ação que você deseja usar na sua assinatura, clique em **Liberar**.

Criar um pacote ZIP para ações de extensibilidade de tempo de execução do Python

Você pode criar um pacote ZIP que contenha o script Python e as dependências usadas por suas ações de extensibilidade do Cloud Assembly.

Há dois métodos de criar o script para suas ações de extensibilidade:

- Escrever o script diretamente no editor de ações de extensibilidade no Cloud Assembly.

- Criar o script no seu ambiente local e adicioná-lo, com quaisquer dependências relevantes, a um pacote ZIP.

Ao usar um pacote ZIP, você pode criar um modelo pré-configurado personalizado de scripts de ação e dependências que é possível importar para o Cloud Assembly para uso em ações de extensibilidade.

Além disso, você pode usar um pacote ZIP em cenários em que os módulos associados a dependências no seu script de ação não podem ser resolvidos pelo serviço do Cloud Assembly, como quando o seu ambiente não tem acesso à Internet.

Você também pode usar um pacote ZIP para criar ações de extensibilidade que contenham vários arquivos de script do Python. O uso de vários arquivos de script pode ser útil para organizar a estrutura do seu código de ação de extensibilidade.

Pré-requisitos

Se você estiver usando o Python 3,3 ou anterior, baixe e configure o instalador do pacote PIP. Consulte [Índice de pacotes Python](#).

Procedimentos

- 1 Na máquina local, crie uma pasta para o script de ação e as dependências.
Por exemplo, `/home/user1/zip-action`.
- 2 Adicione um ou mais scripts de ação Python principais à pasta.
Por exemplo, `/home/user1/zip-action/main.py`.
- 3 (Opcional) Adicione quaisquer dependências do seu script Python à pasta.
 - a Crie um arquivo `requirements.txt` que contenha suas dependências. Consulte [Arquivos de requisitos](#).
 - b Abra um shell do Linux.

Observação O tempo de execução da extensibilidade com base em ações no Cloud Assembly é baseado no Linux. Portanto, quaisquer dependências do Python compiladas em um ambiente do Windows poderão inutilizar o pacote ZIP gerado para a criação de ações de extensibilidade. Portanto, você deve usar um shell do Linux.

- c Instale o arquivo `requirements.txt` na pasta de script executando o seguinte comando:

```
pip install -r requirements.txt --target=home/user1/zip-action
```


- 4 Na pasta atribuída, selecione seus elementos de script e, se aplicável, seu arquivo `requirements.txt` e compacte-os em um pacote ZIP.

Observação Ambos os elementos de scripts e de dependências devem ser armazenados no nível raiz do pacote ZIP. Ao criar o pacote ZIP em um ambiente Linux, você pode se deparar com um problema em que o conteúdo do pacote não está armazenado no nível raiz. Se você se deparar com esse problema, crie o pacote executando o comando `zip -r` no seu Shell de linha de comando.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Próximo passo

Use o pacote ZIP para criar um script de ação de extensibilidade. Consulte [Como criar ações de extensibilidade](#).

Criar um pacote ZIP para ações de extensibilidade de tempo de execução do Node.js

Você pode criar um pacote ZIP que contenha o script Node.js e as dependências usadas por suas ações de extensibilidade do Cloud Assembly.

Há dois métodos de criar o script para suas ações de extensibilidade:

- Escrever o script diretamente no editor de ações de extensibilidade no Cloud Assembly.
- Criar o script no seu ambiente local e adicioná-lo, com quaisquer dependências relevantes, a um pacote ZIP.

Ao usar um pacote ZIP, você pode criar um modelo pré-configurado personalizado de scripts de ação e dependências que é possível importar para o Cloud Assembly para uso em ações de extensibilidade.

Além disso, você pode usar um pacote ZIP em cenários em que os módulos associados a dependências no seu script de ação não podem ser resolvidos pelo serviço do Cloud Assembly, como quando o seu ambiente não tem acesso à Internet.

Além disso, você pode usar pacotes para criar ações de extensibilidade que contenham vários arquivos de script Node.js. O uso de vários arquivos de script pode ser útil para organizar a estrutura do seu código de ação de extensibilidade.

Procedimentos

- 1 Na máquina local, crie uma pasta para o script de ação e as dependências.

Por exemplo, `/home/user1/zip-action`.

- 2 Adicione um ou mais scripts de ação Node.js principais à pasta.

Por exemplo, `/home/user1/zip-action/main.js`.

3 (Opcional) Adicione quaisquer dependências do seu script Node.js à pasta.

- a Crie um arquivo `package.json` com dependências na sua pasta de script. Consulte [Criando um arquivo package.json](#) e [Especificando dependências e devDependencies em um arquivo package.json](#).
- b Abra um shell de linha de comando.
- c Navegue até a pasta que você criou para o script de ação e as dependências.

```
cd /home/user1/zip-action
```

- d Instale o arquivo `package.json` na pasta de script executando o seguinte comando:

```
npm install --production
```

Observação Esse comando cria um diretório `node_modules` na sua pasta.

- 4 Na pasta atribuída, selecione seus elementos de script e, se aplicável, seu diretório `node_modules` e compacte-os em um pacote ZIP.

Observação Ambos os elementos de scripts e de dependências devem ser armazenados no nível raiz do pacote ZIP. Ao criar o pacote ZIP em um ambiente Linux, você pode se deparar com um problema em que o conteúdo do pacote não está armazenado no nível raiz. Se você se deparar com esse problema, crie o pacote executando o comando `zip -r` no seu Shell de linha de comando.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Próximo passo

Use o pacote ZIP para criar um script de ação de extensibilidade. Consulte [Como criar ações de extensibilidade](#).

Criar um pacote ZIP para ações de extensibilidade de tempo de execução do PowerShell

Você pode criar um pacote ZIP que contenha seu script do PowerShell e módulos de dependências para uso em ações de extensibilidade.

Há dois métodos de criar o script para suas ações de extensibilidade:

- Escrever o script diretamente no editor de ações de extensibilidade no Cloud Assembly.
- Criar o script no seu ambiente local e adicioná-lo, com quaisquer dependências relevantes, a um pacote ZIP.

Ao usar um pacote ZIP, você pode criar um modelo pré-configurado personalizado de scripts de ação e dependências que é possível importar para o Cloud Assembly para uso em ações de extensibilidade.

Observação Você não precisa definir cmdlets do PowerCLI como dependências ou agrupá-los em um pacote ZIP. Os cmdlets do PowerCLI vêm pré-configurados com o tempo de execução do PowerShell do seu serviço do Cloud Assembly.

Além disso, você pode usar um pacote ZIP em cenários em que os módulos associados a dependências no seu script de ação não podem ser resolvidos pelo serviço do Cloud Assembly, como quando o seu ambiente não tem acesso à Internet.

Você também pode usar um pacote ZIP para criar ações de extensibilidade que contenham vários arquivos de script do PowerShell. O uso de vários arquivos de script pode ser útil para organizar a estrutura do seu código de ação de extensibilidade.

Pré-requisitos

Verifique se você está familiarizado com o PowerShell e o PowerCLI. Você pode encontrar uma imagem do Docker com o PowerShell Core, o PowerCLI 10, o PowerNSX e vários exemplos de script e módulos da comunidade no [Docker Hub](#).

Procedimentos

- 1 Na máquina local, crie uma pasta para o script de ação e as dependências.

Por exemplo, `/home/user1/zip-action`.

- 2 Adicione o script do PowerShell principal com uma extensão `.psm1` à pasta.

O script a seguir apresenta uma função simples do PowerShell chamada `main.psm1`:

```
function handler($context, $payload) {  
  
    Write-Host "Hello " $payload.target  
  
    return $payload  
}
```

Observação A saída de uma ação de extensibilidade do PowerShell é baseada na última variável exibida no corpo da função. Todas as outras variáveis na função incluída são descartadas.

- 3 (Opcional) Adicione uma configuração de proxy ao script principal do PowerShell usando os parâmetros do `context`. Consulte [Usar parâmetros de contexto para adicionar uma configuração de proxy no script do PowerShell](#).

4 (Opcional) Adicione quaisquer dependências para o seu script do PowerShell.

Observação Seu script de dependências do PowerShell deve usar a extensão `.psm1`. Use o mesmo nome para o script e a subpasta em que ele foi salvo.

- a Faça login em um shell do PowerShell no Linux.

Observação O tempo de execução da extensibilidade com base em ações no Cloud Assembly é baseado no Linux. Quaisquer dependências do PowerShell compiladas em um ambiente do Windows poderão inutilizar o pacote ZIP gerado. Todas as dependências de terceiros instaladas devem ser compatíveis com o VMware Photon OS, pois os scripts do PowerShell são executados no Photon OS.

- b Navegue até a pasta `/home/user1/zip-action`.
- c Baixe e salve o módulo do PowerShell que contém as dependências, executando o cmdlet `Save-Module`.

```
Save-Module -Name <module name> -Path ./
```

- d Repita a subetapa anterior para quaisquer módulos de dependências adicionais.

Importante Verifique se cada módulo de dependências está localizado em uma subpasta separada. Para obter mais informações sobre como gravar e gerenciar módulos do PowerShell, consulte [Como escrever um módulo de script do PowerShell](#).

5 Na pasta atribuída, selecione seus elementos de script e, se aplicável, suas subpastas de módulo de dependências e compacte-os em um pacote ZIP.

Observação As subpastas de script e de módulo de dependência devem ser armazenadas no nível raiz do pacote ZIP. Ao criar o pacote ZIP em um ambiente Linux, você pode se deparar com um problema em que o conteúdo do pacote não está armazenado no nível raiz. Se você se deparar com esse problema, crie o pacote executando o comando `zip -r` no seu Shell de linha de comando.

```
cd seu_script_e_pasta_dependências
zip -r ../seu_ZIP_ação.zip *
```

Próximo passo

Use o pacote ZIP para criar um script de ação de extensibilidade. Consulte [Como criar ações de extensibilidade](#).

Usar parâmetros de contexto para adicionar uma configuração de proxy no script do PowerShell. Você pode ativar a comunicação via proxy de rede no script do PowerShell usando os parâmetros `context`.

Alguns cmdlets do PowerShell podem exigir que você defina um proxy de rede como uma variável de ambiente na função do PowerShell. As configurações de proxy são fornecidas para a função do PowerShell com os parâmetros `$context.proxy.host` e `$context.proxy.port`.

Você pode adicionar esses parâmetros `context` no início do script do PowerShell.

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

Se os cmdlets oferecerem suporte ao parâmetro `-Proxy`, você também poderá passar o valor do proxy diretamente para os cmdlets específicos do PowerShell.

Configurar ações de extensibilidade específicas da nuvem

É possível configurar ações de extensibilidade para trabalhar com contas de nuvem.

Ao criar uma ação de extensibilidade, você pode configurá-la e vinculá-la a várias contas com base na nuvem:

- Microsoft Azure
- Amazon Web Services

Pré-requisitos

É necessária uma conta de nuvem válida.

Procedimentos

- 1 Selecione **Extensibilidade > Biblioteca > Ação**.
- 2 Clique em **Nova Ação**.
- 3 Insira os parâmetros da ação conforme necessário.
- 4 No menu suspenso **Provedor FaaS**, selecione o provedor da sua conta de nuvem ou selecione **Seleção Automática**.

Observação Ao selecionar **Auto**, a ação define automaticamente o provedor FaaS.

- 5 Clique em **Salvar**.

Resultados

A ação de extensibilidade é vinculada para uso com a conta de nuvem especificada.

Configurar ações de extensibilidade locais

Você pode configurar suas ações de extensibilidade para usar um provedor de FaaS local, em vez de uma conta de nuvem da Amazon Web Services ou do Microsoft Azure.

Ao usar um provedor de FaaS local para suas ações de extensibilidade, você pode usar serviços locais, como LDAP, CMDB ou centros de dados do vCenter, nas suas assinaturas de extensibilidade do Cloud Assembly.

Procedimentos

- 1 Selecione **Extensibilidade > Biblioteca > Ações**.
- 2 Clique em **Nova Ação**.
- 3 Insira um nome e um projeto para a ação de extensibilidade.
- 4 (Opcional) Insira uma descrição para a ação de extensibilidade.
- 5 Clique em **Seguinte**.
- 6 Crie ou importe o script de ação de extensibilidade.
- 7 Clique no menu suspenso **Provedor FaaS** e selecione **Local**.
- 8 Para salvar a nova ação de extensibilidade, clique em **Salvar**.

Próximo passo

Use a ação de extensibilidade criada nas suas assinaturas de extensibilidade do Cloud Assembly.

Como posso criar segredos para uso em ações de extensibilidade

Você pode adicionar entradas criptografadas à sua ação de extensibilidade usando segredos em nível de projeto.

Com segredos, é possível adicionar valores de entrada criptografados às suas ações de extensibilidade. A criptografia é útil para casos de uso em que suas entradas são usadas para gerenciar dados sensíveis, como senhas e certificados. Os segredos estão disponíveis para todos os provedores FaaS e tempos de execução.

Observação Você também pode adicionar valores de entrada criptografados usando constantes de ação. Consulte [Como posso criar constantes de ação de extensibilidade](#).

O acesso a segredos depende do projeto em que foram criados. Os segredos criados no Projeto A, por exemplo, são acessíveis apenas aos usuários incluídos no Projeto A.

Segredos usam a função `context.getSecret()` para descriptografar o valor do segredo quando ele é adicionado ao seu script. Essa função usa o nome do segredo como parâmetro. Por exemplo, você pode usar um segredo chamado `abxsecret` como um parâmetro de entrada criptografado na sua ação. Para adicionar esse parâmetro de entrada ao script de ação, você deve usar `context.getSecret(inputs["abxsecret"])`.

Procedimentos

- 1 Crie um novo segredo.
 - a Navegar até **Infraestrutura > Administração > Segredos**.
 - b Selecione **Novo Segredo**.

- c Insira o nome do projeto ao qual o segredo está atribuído.

Observação A ação de extensibilidade à qual você deseja atribuir o segredo deve fazer parte do mesmo projeto que o segredo.

- d Insira um nome para o seu segredo.
- e Insira o valor que você deseja atribuir ao segredo.
- f (Opcional) Insira uma descrição.
- g Clique em **Criar**.

2 Adicione seu segredo a uma ação de extensibilidade.

- a Selecione uma ação de extensibilidade existente ou crie uma nova ação de extensibilidade.
- b Em **Entradas Padrão**, marque a caixa de seleção **Segredo**.
- c Pesquise seu segredo e inclua-o nas entradas de ação de extensibilidade.
- d Adicione o segredo ao script da ação de extensibilidade usando a função `context.getSecret()`.
- e Para testar seu segredo, clique em **Testar**.

Como posso criar constantes de ação de extensibilidade

Você pode criar e armazenar constantes para uso em ações de extensibilidade.

Com constantes de ação de extensibilidade, você pode adicionar valores de entrada criptografados às suas ações de extensibilidade. A criptografia é útil para casos de uso em que suas entradas são usadas para gerenciar dados sensíveis, como senhas e certificados. As constantes estão disponíveis para todos os provedores FaaS e tempos de execução.

Observação Ao contrário de segredos, constantes de ação de extensibilidade só podem ser usadas para segredos de extensibilidade. Para obter mais informações sobre segredos, consulte [Como posso criar segredos para uso em ações de extensibilidade](#).

Constantes de ação de extensibilidade são acessíveis a todos os usuários incluídos na sua organização.

Elas usam a função do `context.getSecret()` para serem executadas como parte do seu script. Essa função usa o nome da constante como um parâmetro. Por exemplo, você pode usar uma constante de ação de extensibilidade chamada `abxconstant` como um parâmetro de entrada criptografado na sua ação. Para adicionar esse parâmetro de entrada ao script de ação, você deve usar `context.getSecret(inputs["abxconstant"])`.

Procedimentos

- 1 Crie uma constante de ação de extensibilidade.
 - a Navegue até **Extensibilidade > Biblioteca > Ações**.
 - b Selecione **Constantes de Ação**.

- c Para criar uma constante, clique em **Nova Constante de Ação**.
- d Insira um nome e valor para a constante e clique em **Salvar**.
- 2 Adicione sua constante a uma ação de extensibilidade.
 - a Selecione uma ação de extensibilidade existente ou crie uma nova ação de extensibilidade.
 - b Em **Entradas Padrão**, marque a caixa de seleção **Segredo**.
 - c Pesquise sua constante e adicione-a às entradas de ação de extensibilidade.
 - d Adicione a constante ao script da ação de extensibilidade usando a função `context.getSecret()`.
 - e Para testar sua constante de ação de extensibilidade, clique em **Testar**.

Criar ações de extensibilidade compartilhadas

Como administrador do Cloud Assembly, você pode criar ações de extensibilidade que podem ser compartilhadas entre projetos sem exportar e importar a ação.

Para obter informações sobre como exportar e importar ações de extensibilidade, consulte [Exportar e importar ações de extensibilidade](#).

Pré-requisitos

Crie dois ou mais projetos na sua organização do Cloud Assembly.

Procedimentos

- 1 Selecione **Extensibilidade > Biblioteca > Ações**.
- 2 Clique em **Nova Ação**.
- 3 Digite um nome para a ação de extensibilidade.
- 4 (Opcional) Digite uma descrição para a ação de extensibilidade.
- 5 Selecione um projeto no qual sua ação de extensibilidade será criada.
- 6 Marque a caixa de seleção **Compartilhar com todos os projetos nesta organização**.
- 7 Clique em **Seguinte**.
- 8 Crie ou importe o script de ação e salve a ação de extensibilidade.

Observação Você pode ativar ou desativar o compartilhamento em **Configurações**. Se a ação de extensibilidade for usada em inscrições, você não poderá desativar o compartilhamento. Para desativar o compartilhamento, você deve remover a ação de extensibilidade das suas inscrições.

- 9 Crie uma inscrição de extensibilidade, adicione a ação de extensibilidade compartilhada e defina o escopo de assinatura para **Qualquer projeto**.

Observação Para obter mais informações sobre a criação de assinaturas de extensibilidade, consulte [Criar uma assinatura de extensibilidade](#).

A assinatura de extensibilidade é acionada por eventos correspondentes em qualquer um dos seus projetos.

Próximo passo

Você também pode importar ações de extensibilidade compartilhadas como uma fonte de conteúdo no catálogo do Service Broker. Quando você selecionar o projeto de origem, digite o projeto no qual a ação de extensibilidade foi criada. Para obter mais informações sobre como adicionar ações de extensibilidade ao Service Broker, consulte [Adicionar ações de extensibilidade ao catálogo do Service Broker](#).

Registro em log do Azure para ações de extensibilidade baseadas em Python

Agora, você pode usar as funções de registro em log do Microsoft Azure 3.x no seu script de ação de extensibilidade.

As ações de extensibilidade no Cloud Assembly agora usam a API de Scripting do Microsoft Azure 3.x que substitui a versão anterior 1.x. A API de Scripting do Microsoft Azure 3.x é baseada em Linux e é executada em um ambiente de contêiner.

Por causa dessa alteração de versão, as funções de log inseridas no script de ações de extensibilidade que usam o Microsoft Azure como provedor de FaaS (Função como Serviço) funcionam de maneira diferente. Os próximos dois exemplos de script demonstram as diferentes funções de registro em log usadas nas duas versões da API.

Exemplo de script do Microsoft Azure 1.x.

```
def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    print(greeting)

    outputs = {
        "greeting": greeting
    }

    return outputs
```

Exemplo de script do Microsoft Azure 3.x.

```
import logging

def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    logging.info(greeting)

    outputs = {
```

```
"greeting": greeting
}

return outputs
```

O exemplo anterior demonstra que a versão 3.x adiciona a função `import logging` no início do script enquanto substitui a função `print()` pela função `logging.info()`. Para continuar usando o log com ações de extensibilidade criadas na API do Microsoft Azure 1.x, você deve alterar as funções de log no seu script para que ele corresponda ao exemplo do Microsoft Azure 3.x.

Para obter mais informações sobre registro em log, consulte o [Guia do desenvolvedor de funções do Azure para Python](#).

Exportar e importar ações de extensibilidade

Com o Cloud Assembly, você pode exportar e importar ações de extensibilidade para uso em diferentes projetos.

Pré-requisitos

Uma ação de extensibilidade existente.

Procedimentos

1 Exporte uma ação de extensibilidade.

- a Navegue até **Extensibilidade > Biblioteca > Ações**.
- b Selecione uma ação de extensibilidade e clique em **Exportar**.

O script de ação e suas dependências são salvos no seu ambiente local como um arquivo ZIP.

2 Importe uma ação de extensibilidade.

- a Navegue até **Extensibilidade > Biblioteca > Ações**.
- b Clique em **Importar**.
- c Selecione a ação de extensibilidade exportada e atribua-a a um projeto.
- d Clique em **Importar**.

Observação Se a ação de extensibilidade importada já estiver atribuída ao projeto especificado, você será solicitado a selecionar uma política de resolução de conflitos.

O que é um fluxo de ação

Fluxos de ação são um conjunto de scripts de ação de extensibilidade usados para estender ainda mais os ciclos de vida e a automação.

Todos os fluxos de ação começam com `flow_start` e terminam com `flow_end`. É possível vincular vários scripts de ação de extensibilidade juntos, usando os seguintes elementos de fluxo de ação:

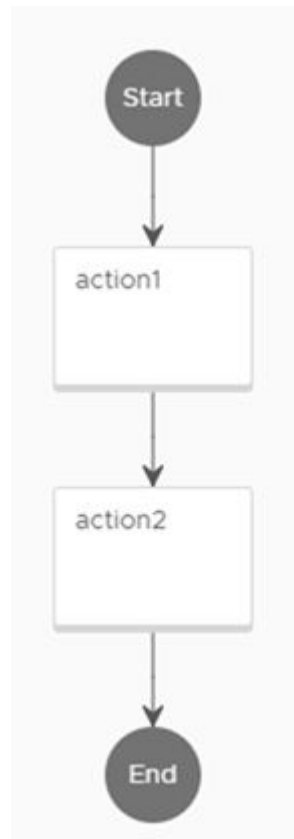
- **Fluxos de ação sequenciais** — vários scripts de ação de extensibilidade em execução sequencial.
- **Fluxos de ação de bifurcação** — vários scripts de ação de extensibilidade ou fluxos que dividem as vias para contribuir para a mesma saída.
- **Unir fluxos de ação** — vários scripts de extensibilidade ou fluxos que se unem e contribuem para a mesma saída.
- **Fluxos de ação condicionais** — vários scripts de ação de extensibilidade ou fluxos que são executados depois que uma condição for satisfeita.

Fluxos de ação sequenciais

Vários scripts de ação de extensibilidade em execução sequencial.

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

Observação É possível retornar automaticamente a uma ação anterior, atribuindo-a como a ação `next`. Por exemplo, neste exemplo, ao invés de `next: flow_end`, é possível digitar `next: action1` para executar novamente a `action1` e reiniciar a sequência de ações.



Fluxos de ação de bifurcação

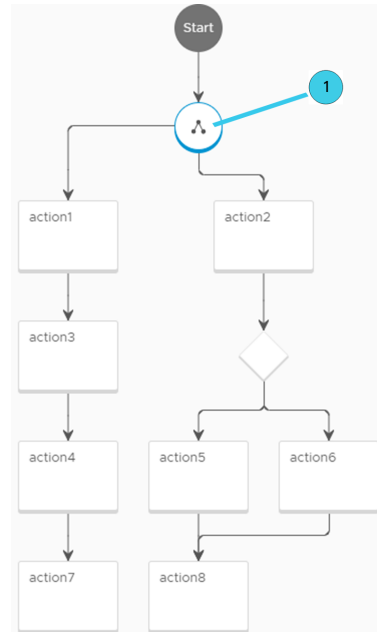
Vários scripts de ação ou fluxo de extensibilidade que dividem os caminhos para contribuir com a mesma saída.

```

version: "1"
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
  action2:
    action: <action_name>

```

Observação É possível retornar automaticamente a uma ação anterior, atribuindo-a como a ação `next: .` Por exemplo, ao invés de `next: flow_end` para finalizar o fluxo de ação, é possível digitar `next: action1` para executar novamente a `action1` e reiniciar a sequência de ações.



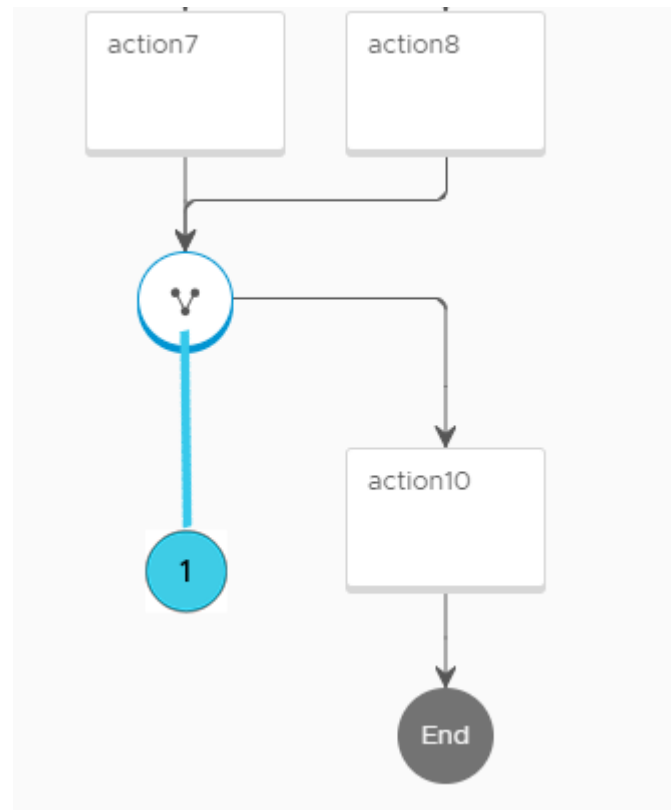
1 Elemento de bifurcação

Unir fluxos de ação

Vários scripts de ação ou fluxos de extensibilidade que unem os caminhos e contribuem para a mesma saída.

```
version: "1"
action7:
  action: <action_name>
  next: joinElement
action8:
  action: <action_name>
  next: joinElement
joinElement:
  join:
    type: all
    next: action10
action10:
  action: <action_name>
  next: flow_end
```

Observação É possível retornar automaticamente a uma ação anterior, atribuindo-a como a ação `next:`. Por exemplo, neste exemplo, ao invés de `next: flow_end`, é possível digitar `next: action1` para executar novamente a `action1` e reiniciar a sequência de ações.



1 Elemento de união

Fluxos de ação condicionais

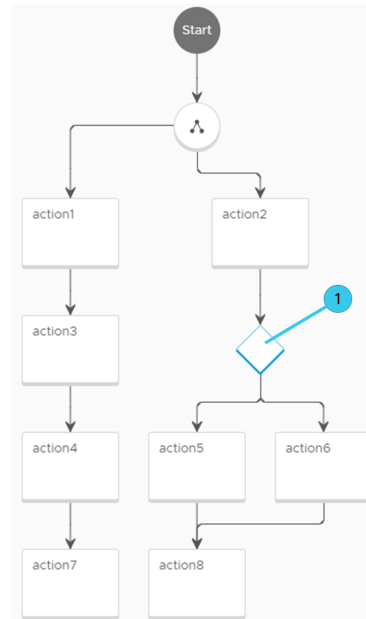
Vários scripts de ação ou fluxos de extensibilidade que são executados quando uma condição é satisfeita usando um elemento de opção.

Em alguns casos, a condição deve ser igual a `true` para que a ação seja executada. Outros casos, como visto neste exemplo, exigem que os valores de parâmetro sejam atendidos antes que uma ação possa ser executada. Se nenhuma das condições for atendida, o fluxo de ação falhará.

```

version: 1
id: 1234
name: Test
inputs: ...
outputs: ...
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
    next: joinElement
  action2:
    action: <action_name>
    next: switchAction
  switchAction:
    switch:
      "${1 == 1}": action5
      "${1 != 1}": action6
  action5:
    action: <action_name>
    next: action8
  action6:
    action: <action_name>
    next: action8
  action8:
    action: <action_name>

```



1 Elemento de opção

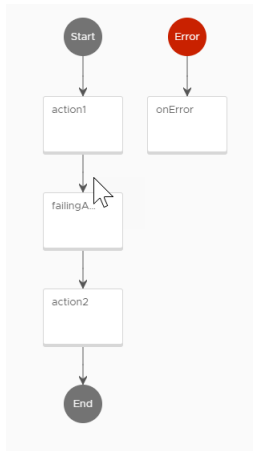
Observação É possível retornar automaticamente a uma ação anterior, atribuindo-a como a ação `next:`. Por exemplo, ao invés de `next: flow_end` para finalizar o fluxo de ação, é possível digitar `next: action1` para executar novamente a `action1` e reiniciar a sequência de ações.

Como usar um manipulador de erro com fluxos de ação

É possível configurar seu fluxo de ação para emitir um erro em estágios especificados do fluxo usando um elemento manipulador de erro.

Um elemento manipulador de erro exige duas entradas:

- Mensagem de erro especificada da ação com falha.
- Entradas de fluxo de ação.



Se uma ação no fluxo falhar e o fluxo de ação contiver um elemento manipulador de erro, uma mensagem de erro será emitida, alertando sobre a falha na ação. O manipulador de erro é uma ação autônoma. O script a seguir é um exemplo de um manipulador de erro que pode ser usado em um fluxo de ação.

```
def handler(context, inputs):

    errorMsg = inputs["errorMsg"]
    flowInputs = inputs["flowInputs"]

    print("Flow execution failed with error {0}".format(errorMsg))
    print("Flow inputs were: {0}".format(flowInputs))

    outputs = {
        "errorMsg": errorMsg,
        "flowInputs": flowInputs
    }

    return outputs
```

É possível exibir as execuções bem-sucedidas e com falha na janela Execuções de Ação.

| | Status | Run ID | Action |
|--------------------------|-----------|--------------------------|-------------------|
| <input type="checkbox"/> | Completed | 8a76996b6839fe3c01684... | error-handler |
| <input type="checkbox"/> | Failed | 8a76996b6839fe3c01684... | failing-action |
| <input type="checkbox"/> | Completed | 8a76996b6839fe3c01684... | simple-hello |
| <input type="checkbox"/> | Completed | 8a76996b6839fe3c01684... | flow-with-handler |

Neste exemplo, o fluxo de ação do manipulador com fluxo, que contém um elemento manipulador de erro, foi executado com êxito. No entanto, uma das ações no fluxo falhou, o que iniciou o manipulador de erro para emitir um erro.

Como rastrear execuções de ação

A guia Execuções de Ação mostra um log das ações de extensibilidade de assinatura disparadas e seus status.

É possível visualizar o log de execuções de ação usando **Extensibilidade > Atividade > Execuções de Ação**. Também é possível filtrar a lista de execuções de ação para mostrar uma ou mais propriedades de uma vez só.

Solução de problemas de falha nas execuções de ação de extensibilidade

Se a ação de extensibilidade for executada, será possível executar etapas de solução de problemas para corrigi-la.

Quando uma ação executada falha, é possível receber uma mensagem de erro, um status de falha e um log com falha. Se a ação executada falhar, será devido a uma falha na implantação ou no código.

| Problema | Solução |
|----------------------|--|
| Falha na implantação | Essas falhas são um resultado de problemas relacionados à configuração da conta de nuvem, à implantação de ação ou a outras dependências que podem impedir que a ação seja implantada. Certifique-se de que o projeto usado esteja definido na conta de nuvem configurada e que foram concedidas permissões para executar funções. Antes de iniciar a ação novamente, é possível testar a ação em relação a um projeto específico na página de detalhes da ação. |
| Falha de código | Essas falhas são resultado de scripts ou código inválidos. Use os logs de execução de ação para solucionar problemas e corrigir os scripts inválidos. |

Assinaturas de fluxo de trabalho de extensibilidade

É possível usar seus fluxos de trabalho hospedados no vRealize Orchestrator com o Cloud Assembly para estender o ciclo de vida do aplicativo.

Como modificar as propriedades da máquina virtual usando uma assinatura de fluxo de trabalho do vRealize Orchestrator

É possível usar um fluxo de trabalho do vRealize Orchestrator existente para modificar as propriedades da máquina virtual e adicionar máquinas virtuais ao Active Directory.

Os parâmetros de tópicos de eventos definem o formato de payload das mensagens do serviço do agente de eventos (EBS). Para receber e usar o payload da mensagem do EBS dentro de um fluxo de trabalho, será necessário definir os parâmetros de entrada do fluxo de trabalho `inputProperties`.

Pré-requisitos

- Função de usuário administrador de nuvem

- Fluxos de trabalho locais existentes do vRealize Orchestrator.
- Integração e conexão com êxito ao servidor do cliente vRealize Orchestrator.

Procedimentos

- 1 Selecione **Extensibilidade > Assinaturas**.
- 2 Clique em **Nova Assinatura**.
- 3 Crie uma assinatura com os seguintes parâmetros:

| Parâmetro | Valor |
|------------------------|--|
| Nome | RenameVM |
| Tópico de evento | Selecione um tópico de evento adequado para a integração vRealize Orchestrator desejada. Por exemplo, alocação de processamento. |
| Bloqueio/sem bloqueio | Sem bloqueio |
| Ação/fluxo de trabalho | Selecione um tipo executável do vRealize Orchestrator. Selecione o fluxo de trabalho desejado. Por exemplo, Definir nome da VM. |

- 4 Para salvar a assinatura, clique em **Salvar**.
- 5 Atribua e ative sua assinatura criando um modelo de nuvem ou implantando um modelo de nuvem existente.

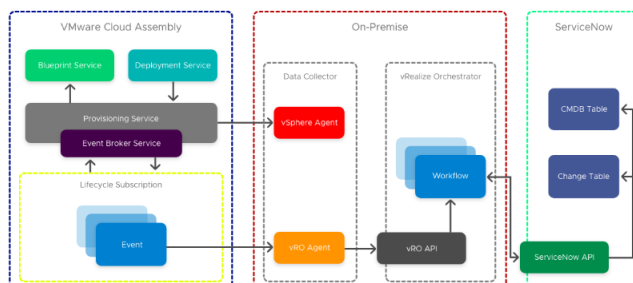
Próximo passo

Verifique se o fluxo de trabalho foi iniciado com êxito por um dos seguintes métodos:

- Verifique o log de execução do fluxo de trabalho, **Extensibilidade > Atividade > Execuções do Fluxo de Trabalho**.
- Abra o cliente do vRealize Orchestrator e verifique o status do fluxo de trabalho navegando até ele para conferir o status ou abrindo a guia de logs específicos.

Como integrar o Cloud Assembly para o ITSM ao ServiceNow usando fluxos de trabalho do vRealize Orchestrator

Usando fluxos de trabalho hospedados do vRealize Orchestrator, é possível integrar o Cloud Assembly ao ServiceNow para conformidade de ITSM.



Os usuários corporativos normalmente integram sua plataforma de gerenciamento de nuvem a uma plataforma de gerenciamento de serviços de TI (ITSM) e a um database de gerenciamento de configuração (CMDB) para conformidade. Seguindo este exemplo, é possível integrar o Cloud Assembly ao ServiceNow para CMDB e ITSM usando fluxos de trabalho hospedados do vRealize Orchestrator. Durante o uso das integrações e dos fluxos de trabalho do vRealize Orchestrator, as tags de capacidade serão especialmente úteis se houver várias instâncias para ambientes diferentes. Para obter mais informações sobre tags de capacidade, consulte [Como usar tags de capacidade no Cloud Assembly](#).

Observação Também é possível integrar o ServiceNow ao Cloud Assembly usando scripts de ação de extensibilidade. Para obter informações sobre como integrar o ServiceNow usando scripts de ação de extensibilidade, consulte [Como integrar o Cloud Assembly com o ServiceNow usando ações de extensibilidade](#).

Neste exemplo, a integração do ServiceNow é composta por três fluxos de trabalho de alto nível. Cada fluxo de trabalho tem suas próprias assinaturas para que você possa atualizar e iterar cada componente individualmente.

- O log básico do ponto de entrada de assinatura de eventos identifica o usuário solicitante e a VM do vCenter, se aplicável.
- Fluxo de trabalho de integração — separa objetos e alimenta as entradas no fluxo de trabalho técnico, gerencia as atualizações de log, propriedade e saída.
- Fluxo de trabalho técnico — integração de sistema downstream para API ServiceNow para criar a API da IaaS de IC do CMDB, CR e Cloud Assembly com propriedades de máquina virtual fora do payload.

Pré-requisitos

- Um ambiente do vRealize Orchestrator autônomo ou agrupado em clusters.
- Uma integração com o vRealize Orchestrator no Cloud Assembly. Para obter informações sobre como integrar um vRealize Orchestrator autônomo com o Cloud Assembly, consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).

Procedimentos

- 1 Crie e salve um arquivo de configuração no vRealize Orchestrator que contenha a configuração comum usada em vários fluxos de trabalho.
- 2 Salve o token de API do Cloud Assembly no mesmo local, como o arquivo de configuração da Etapa 1.

Observação O token de API do Cloud Assembly tem validade.

- 3 Crie um fluxo de trabalho no vRealize Orchestrator com o elemento de script fornecido. Este script faz referência e localiza um host REST. Ele também padroniza as ações REST que usam um parâmetro opcional de um token, que é adicionado como um cabeçalho de autorização extra.

```

var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "CASRestHost"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attribute
Name)

var ConfigurationElement =
System.getModule("au.com.cs.example").getConfigurationElementByName(configName,configPath);
System.debug("ConfigurationElement:" + ConfigurationElement);
var casToken = ConfigurationElement.getAttributeWithKey("CASToken")["value"]
if(!casToken){
    throw "no CAS Token";
}
//REST Template
var opName = "casLogin";
var opTemplate = "/iaas/login";
var opMethod = "POST";

// create the REST operation:
var opLogin =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cas API Token
var contentObject = {"refreshToken":casToken}
postContent = JSON.stringify(contentObject);

var loginResponse =
System.getModule("au.com.cs.example").executeOp(opLogin,null,postContent,null);

try{
    var tokenResponse = JSON.parse(loginResponse)['token']
    System.debug("token: " + tokenResponse);
} catch (ex) {
    throw ex + " No valid token";
}

//REST Template Machine Details
var opName = "machineDetails";
var opTemplate = "/iaas/machines/" + resourceId;
var opMethod = "GET";

var bearer = "Bearer " + tokenResponse;

var opMachine =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

```

```
// (Rest Operation, Params, Content, Auth Token)
var vmResponse =
System.getModule("au.com.cs.example").executeOp(opMachine,null,"",bearer) ;

try{
    var vm = JSON.parse(vmResponse);
} catch (ex) {
    throw ex + " failed to parse vm details"
}

System.log("cpuCount: " + vm["customProperties"]["cpuCount"]);
System.log("memoryInMB: " + vm["customProperties"]["memoryInMB"]);

cpuCount = vm["customProperties"]["cpuCount"];
memoryMB = vm["customProperties"]["memoryInMB"];
```

Esse script envia a saída `cpuCount` e `memoryMB` para o fluxo de trabalho principal e atualiza as propriedades das `customProperties` existentes. Esses valores podem ser usados em fluxos de trabalho subsequentes ao criar o CMDB.

- 4 Adicione o elemento de script Criar IC do ServiceNow CMDB ao seu fluxo de trabalho. Esse elemento localiza o host REST do ServiceNow usando o item de configuração, cria uma operação REST para a tabela `cmdb_ci_vmware_instance`, cria uma cadeia de caracteres de objeto de conteúdo com base em entradas do fluxo de trabalho para postar dados e gera o `sys_id`retornado.

```
var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "serviceNowRestHost"
var tableName = "cmdb_ci_vmware_instance"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attribute
Name)

//REST Template
var opName = "serviceNowCreatCI";
var opTemplate = "/api/now/table/" + tableName;
var opMethod = "POST";

// create the REST operation:
var opCI =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cmdb_ci_vm_vmware table content to post;
var contentObject = {};
contentObject["name"] = hostname;
contentObject["cpus"] = cpuTotalCount;
contentObject["memory"] = MemoryInMB;
contentObject["correlation_id"] = deploymentId
contentObject["disks_size"] = diskProvisionGB
```

```

contentObject["location"] = "Sydney";
contentObject["vcenter_uuid"] = vcUuid;
contentObject["state"] = "On";
contentObject["owned_by"] = owner;

postContent = JSON.stringify(contentObject);
System.log("JSON: " + postContent);

// (Rest Operation, Params, Content, Auth Token)
var ciResponse =
System.getModule("au.com.cs.example").executeOp(opCI,null,postContent,null) ;

try{
    var cmdbCI = JSON.parse(ciResponse);
} catch (ex) {
    throw ex + " failed to parse ServiceNow CMDB response";
}

serviceNowSysId = cmdbCI['result']['sys_id'];

```

- 5 Usando a saída do fluxo de trabalho secundário, crie um objeto de propriedades usando o `customProperties` existente e substitua a propriedade `serviceNowSysId` pelo valor do ServiceNow. Esse ID exclusivo é usado no CMDB para marcar uma instância como desativada na destruição.

Resultados

O Cloud Assembly foi integrado com êxito ao ITSM ServiceNow. Para obter mais informações sobre como é possível usar fluxos de trabalho para integrar o ServiceNow no Cloud Assembly, consulte [Estender o Cloud Assembly com vRealize Orchestrator para a integração do ServiceNow](#).

Saiba mais sobre assinaturas de fluxo de trabalho

Ao usar uma integração do vRealize Orchestrator com o Cloud Assembly, é possível estender os ciclos de vida de aplicativos com fluxos de trabalho.

O vRealize Automation inclui uma implantação incorporada do vRealize Orchestrator. Você pode usar a biblioteca de fluxos de trabalho dessa implantação incorporada do vRealize Orchestrator nas suas assinaturas. É possível criar, modificar e excluir fluxos de trabalho usando o cliente vRealize Orchestrator.

Você também pode integrar uma implantação externa do vRealize Orchestrator ao Cloud Assembly. Consulte [Configurar uma integração do vRealize Orchestrator no Cloud Assembly](#).

Boas práticas para a criação de fluxos de trabalho do vRealize Orchestrator

Uma inscrição de fluxo de trabalho baseia-se em um tópico de evento específico e nos parâmetros de evento desse tópico. Para garantir que as assinaturas iniciem os fluxos de trabalho do vRealize Orchestrator, é necessário configurá-las com os parâmetros de entrada corretos para que elas trabalhem com os dados de eventos.

Parâmetros de entrada do fluxo de trabalho

O fluxo de trabalho personalizado pode incluir todos os parâmetros ou um único parâmetro que consome todos os dados no payload.

Para usar um único parâmetro, configure um parâmetro com um tipo de `Properties` e nome `inputProperties`.

Parâmetros de saída de fluxo de trabalho

O fluxo de trabalho personalizado pode incluir parâmetros de saída que sejam relevantes para eventos subsequentes necessários para um tipo de tópico de evento de resposta.

Se um tópico de evento espera uma resposta, os parâmetros de saída de fluxo de trabalho devem corresponder aos parâmetros do esquema de respostas.

Como rastrear execuções de fluxo de trabalho

A janela **Execuções de Fluxo de Trabalho** exibe os logs dos fluxos de trabalho de assinatura disparados e seu status.

Você pode visualizar os logs das suas execuções de fluxo de trabalho navegando até **Extensibilidade > Atividade > Execuções de Fluxo de Trabalho**.

Solução de problemas de assinaturas de fluxo de trabalho com falha

Se a assinatura de fluxo de trabalho falhar, será possível realizar etapas de solução de problemas para corrigi-la.

As execuções de fluxo de trabalho com falha podem fazer com que a assinatura de fluxo de trabalho não seja iniciada ou concluída. A falha na execução do fluxo de trabalho pode resultar de vários problemas comuns.

| Problema | Causa | Solução |
|---|--|--|
| A assinatura de fluxo de trabalho do vRealize Orchestrator não foi iniciada ou concluída com êxito. | É configurada uma assinatura de fluxo de trabalho para executar um fluxo de trabalho personalizado quando a mensagem de evento é recebida, mas esse fluxo de trabalho não é executado ou concluído com êxito. | <ol style="list-style-type: none"> 1 Verifique se as condições da assinatura de fluxo de trabalho foram salvas corretamente. 2 Verifique se as condições da assinatura de fluxo de trabalho estão configuradas corretamente. 3 Verifique se o vRealize Orchestrator contém o fluxo de trabalho especificado. 4 Verifique se o fluxo de trabalho está configurado corretamente no vRealize Orchestrator. |
| Sua solicitação de aprovação da assinatura de fluxo de trabalho do vRealize Orchestrator não foi executada. | Foi configurada uma assinatura de fluxo de trabalho de pré-aprovação ou pós-aprovação para executar um fluxo de trabalho do vRealize Orchestrator. O fluxo de trabalho não é executado quando uma máquina que corresponde aos critérios definidos é solicitada no catálogo de serviços. | <p>Para executar uma assinatura de fluxo de trabalho de aprovação com êxito, é necessário verificar se todos os componentes estão configurados corretamente.</p> <ol style="list-style-type: none"> 1 Verifique se a política de aprovação está ativa e aplicada corretamente. 2 Verifique se a assinatura de fluxo de trabalho está configurada e salva corretamente. 3 Examine os logs de eventos para mensagens relacionadas a aprovações. |
| Sua solicitação de aprovação da assinatura de fluxo de trabalho do vRealize Orchestrator foi rejeitada. | <p>É configurada uma assinatura de pré-aprovação ou pós-aprovação do fluxo de trabalho que executa o fluxo de trabalho especificado do vRealize Orchestrator, mas a solicitação é inesperadamente rejeitada no nível externo de aprovação.</p> <p>Uma causa possível é um erro interno na execução do fluxo de trabalho no vRealize Orchestrator. Por exemplo, o fluxo de trabalho está ausente ou o servidor do vRealize Orchestrator não está em execução.</p> | <ol style="list-style-type: none"> 1 Examine os logs para mensagens relacionadas a aprovações. 2 Verifique se o servidor do vRealize Orchestrator está em execução. 3 Verifique se o vRealize Orchestrator contém o fluxo de trabalho especificado. |

Saiba mais sobre assinaturas de extensibilidade

É possível estender ciclos de vida de aplicativos usando ações de extensibilidade ou fluxos de trabalho hospedados do vRealize Orchestrator com assinaturas de extensibilidade.

Quando ocorre um evento de disparo em seu ambiente, a assinatura é iniciada e a ação de fluxo de trabalho ou de extensibilidade especificada é executada. É possível visualizar eventos do sistema no log de eventos, execuções de fluxo de trabalho na janela de execuções de fluxo de trabalho e a execuções de ação na janela de execuções de ação. As assinaturas são específicas do projeto, o que significa que elas estão vinculadas a modelos de nuvem e implantações por meio do projeto especificado.

Terminologia de extensibilidade

Ao trabalhar com assinaturas de extensibilidade no Cloud Assembly, você pode se deparar com alguns termos específicos das assinaturas e do serviço de agente de eventos.

Tabela 6-6. Terminologia de extensibilidade

| Termo | Descrição |
|---------------------------------|---|
| Tópico de evento | <p>Descreve um conjunto de eventos que têm o mesmo objetivo lógico e a mesma estrutura. Cada evento é uma instância de um tópico de evento.</p> <p>É possível atribuir parâmetros de bloqueio a determinados tópicos de evento. Para obter mais informações, consulte Bloqueio de tópicos de evento.</p> |
| Evento | Indica uma alteração no estado no produtor ou em qualquer uma das entidades gerenciadas por ele. O evento é a entidade que registra informações sobre a ocorrência do evento. |
| Serviço de agente de eventos | O serviço que distribui as mensagens publicadas por um produtor aos consumidores assinantes. |
| Payload | Os dados de evento que contêm todas as propriedades relevantes associadas a esse tópico de evento. |
| Assinatura | Indica que um assinante está interessado em ser notificado sobre um evento ao assinar um tópico de evento e definir os critérios que disparam a notificação. As assinaturas vinculam ações de extensibilidade ou fluxos de trabalho a eventos de disparo usados para automatizar partes do ciclo de vida dos aplicativos. |
| Assinante | Os usuários notificados pelos eventos publicados no serviço de agente de eventos com base na definição da assinatura. O assinante também pode ser chamado de consumidor. |
| Administrador de sistema | Um usuário com privilégios para criar, ler, atualizar e excluir assinaturas do fluxo de trabalho do tenant e assinaturas do fluxo de trabalho do sistema usando o Cloud Assembly. |
| Assinatura de fluxo de trabalho | Especifica o tópico de evento e as condições que disparam um fluxo de trabalho do vRealize Orchestrator. |
| Assinatura de ação | Especifica o tópico de evento e as condições que disparam uma ação de extensibilidade a ser executada. |

Tabela 6-6. Terminologia de extensibilidade (continuação)

| Termo | Descrição |
|-------------------------|---|
| Fluxo de trabalho | Um fluxo de trabalho do vRealize Orchestrator que é integrado no Cloud Assembly. É possível vincular esses fluxos de trabalho a eventos nas assinaturas. |
| Ação de extensibilidade | Um script de código simplificado que pode ser executado depois que um evento é disparado em uma assinatura. As ações de extensibilidade são semelhantes a fluxos de trabalho, mas são mais leves. As ações de extensibilidade podem ser personalizadas de dentro do Cloud Assembly. |
| Execuções de Ação | Acessível por meio da guia Execuções de Ação . Uma execução de ação é um log detalhado de ações de extensibilidade que foram executadas em resposta a eventos de disparo. |

Bloqueio de tópicos de evento

Alguns tópicos de eventos oferecem suporte para eventos de bloqueio. O comportamento de uma assinatura de extensibilidade depende se o tópico oferece suporte ou não a esses tipos de eventos e de como você configura a assinatura.

As assinaturas de extensibilidade do Cloud Assembly podem usar dois tipos amplos de tópicos de evento: tópicos de eventos sem bloqueio e tópicos de eventos de bloqueio. O tipo de tópico de evento define o comportamento da assinatura de extensibilidade.

Tópicos de eventos sem bloqueio

Tópicos de eventos sem bloqueio permitem apenas a criação de assinaturas sem bloqueio. Assinaturas sem bloqueio são disparadas de forma assíncrona, e você não pode depender da ordem em que as assinaturas são disparadas.

Bloqueio de tópicos de evento

Alguns tópicos de eventos oferecem suporte para bloqueio. Se uma assinatura estiver marcada como uma assinatura com bloqueio, nenhuma das mensagens que atenderem às condições definidas serão recebidas por outras assinaturas com condições correspondentes até que o item executável da assinatura com bloqueio seja executado.

Assinaturas com bloqueio são executadas por ordem de prioridade. O valor de prioridade mais alto é 0 (zero). Se houver mais de uma assinatura com bloqueio para o mesmo tópico de evento com o mesmo nível de prioridade, as assinaturas serão executadas em ordem alfabética inversa com base no nome da assinatura. Após o processamento de todas as assinaturas com bloqueio, a mensagem será enviada a todas as assinaturas sem bloqueio ao mesmo tempo. Como as assinaturas com bloqueio são executadas de forma sincronizada, a carga de eventos alterados inclui o evento atualizado quando as assinaturas subsequentes são notificadas.

Você pode usar tópicos de eventos com bloqueio para gerenciar várias assinaturas que são dependentes umas das outras.

Por exemplo, é possível ter duas assinaturas de fluxo de trabalho de provisionamento, nas quais a segunda assinatura depende dos resultados da primeira. A primeira assinatura altera uma propriedade durante o provisionamento, enquanto a segunda registra a nova propriedade, como um nome de máquina, em um sistema de arquivos. A assinatura de `ChangeProperty` é priorizada como 0, enquanto a assinatura de `RecordProperty` é priorizada como 1, pois a segunda assinatura usa os resultados da primeira. Quando uma máquina for provisionada, a assinatura de `ChangeProperty` começa a ser executada. Como as condições da assinatura de `RecordProperty` são baseadas em uma condição pós-provisionamento, um evento dispara a assinatura de `RecordProperty`. No entanto, como o fluxo de trabalho `ChangeProperty` é um fluxo de trabalho com bloqueio, o evento apenas será recebido quando ele for finalizado. Quando o nome da máquina for alterado e a primeira assinatura de fluxo de trabalho for finalizada, a segunda assinatura de fluxo de trabalho será executada e registrará o nome da máquina no sistema de arquivos.

Item Executável de Recuperação

Para tópicos de eventos com bloqueio, você pode adicionar um item executável de recuperação à assinatura. O item executável de recuperação em uma assinatura será executado se o item executável primário falhar. Por exemplo, você pode criar uma assinatura de fluxo de trabalho na qual o item executável primário é um fluxo de trabalho que cria registros em um sistema CMDB, como o ServiceNow. Mesmo que a assinatura de fluxo de trabalho falhe, alguns registros podem ser criados no sistema CMDB. Nesse cenário, um item executável de recuperação pode ser usado para limpar os registros deixados no sistema CMDB pelo item executável com falha.

Para casos de uso que incluem várias assinaturas dependentes umas das outras, você pode adicionar uma propriedade `ebs.recover.continuation` ao item executável de recuperação. Com essa propriedade, você pode direcionar se o serviço de extensibilidade deve continuar com a próxima assinatura na sua cadeia caso a assinatura atual falhe.

Tópicos de eventos fornecidos com o Cloud Assembly

O Cloud Assembly inclui tópicos de eventos predefinidos.

Tópicos de eventos

Os tópicos de eventos são as categorias que agrupam eventos semelhantes. Quando atribuído a uma assinatura, os tópicos de eventos definem o evento que dispara a assinatura. Os tópicos de evento a seguir são fornecidos por padrão com o Cloud Assembly. Todos os tópicos podem ser usados para adicionar ou atualizar propriedades personalizadas ou tags do recurso. Se uma ação de extensibilidade ou um fluxo de trabalho do vRealize Orchestrator falhar, a tarefa correspondente também falhará.

Tabela 6-7. Tópicos de evento do Cloud Assembly

| Tópico de evento | Bloqueável | Descrição |
|--------------------------------------|------------|---|
| Cloud template configuration | Não | Emitido quando ocorre um evento de configuração de modelo de nuvem, como a criação ou a exclusão de um modelo de nuvem. Esse tópico de evento pode ser útil para notificar sistemas externos sobre tais eventos. |
| Cloud template version configuration | Não | Emitido quando ocorre um novo evento de controle de versão de modelo de nuvem, como a criação, a liberação, o cancelamento da liberação ou a restauração de uma versão. Esse tópico de evento pode ser útil com integrações de sistemas de controle de versão de terceiros. |
| Compute allocation | Sim | Emitido antes da alocação de <code>resourcenames</code> e <code>hostselections</code> . Ambas as propriedades podem ser modificadas nesse estágio. Emitido uma vez para um cluster de máquinas. |
| Compute gateway post provisioning | Sim | Emitido depois que um recurso de gateway de processamento é provisionado. |
| Compute gateway post removal | Sim | Emitido após a remoção de um gateway de processamento. |
| Compute gateway provisioning | Sim | Emitido antes de um gateway de processamento ser provisionado. |
| Compute gateway removal | Sim | Emitido antes de um gateway de processamento ser removido. |
| Compute initial power on | Sim | Emitido depois que um recurso é provisionado na camada do hypervisor, mas antes que o recurso seja ligado pela primeira vez. Atualmente, esse tópico de evento é compatível apenas com o vSphere. Eventos são enviados para cada máquina em um cluster. Observação Você pode pular a ativação inicial do recurso. |
| Compute nat post provisioning | Sim | Emitido depois de um recurso NAT de processamento ser provisionado. |
| Compute nat post removal | Sim | Emitido depois de um recurso NAT de processamento ser removido. |
| Compute nat provisioning | Sim | Emitido antes de um NAT de processamento ser provisionado. |

Tabela 6-7. Tópicos de evento do Cloud Assembly (continuação)

| Tópico de evento | Bloqueável | Descrição |
|--------------------------------|------------|---|
| Compute nat removal | Sim | Emitido antes de um NAT de processamento ser removido. |
| Compute post provision | Sim | Emitido depois que um recurso é provisionado. Eventos são enviados para cada máquina em um cluster. |
| Compute post removal | Sim | emitido depois que um recurso de computação é removido. Eventos são enviados para cada máquina em um cluster. |
| Compute provision | Sim | Emitido antes que o recurso seja provisionado na camada do hypervisor. Eventos são enviados para cada máquina em um cluster. Observação É possível alterar o endereço IP alocado. |
| Compute removal | Sim | Emitido antes de o recurso ser removido. Eventos são enviados para cada máquina em um cluster. |
| Compute reservation | Sim | Emitido no momento da reserva. Emitido uma vez para um cluster de máquinas. Observação É possível alterar a ordem do posicionamento. |
| Custom resource post provision | Sim | Emitido para eventos de pós-provisionamento acionados por operações de recursos personalizados. |
| Custom resource pre provision | Sim | Emitido para eventos de pré-provisionamento acionados por operações de recursos personalizados. |
| Deployment action completed | Sim | Emitido após a conclusão de uma ação de implantação. |
| Deployment action requested | Sim | Emitido antes da conclusão de uma ação de implantação. |
| Deployment completed | Sim | Emitido após a implantação de uma solicitação de catálogo ou modelo de nuvem. |
| Deployment onboarded | Não | Emitido quando uma nova implantação é integrada. |
| Deployment requested | Sim | Emitido antes da implantação de uma solicitação de catálogo ou modelo de nuvem. |

Tabela 6-7. Tópicos de evento do Cloud Assembly (continuação)

| Tópico de evento | Bloqueável | Descrição |
|--------------------------------------|------------|--|
| Deployment resource action completed | Sim | Emitido após a implantação de uma ação de recurso. |
| Deployment resource action requested | Sim | Emitido antes da implantação de uma ação de recurso. |
| Deployment resource completed | Sim | Emitido após o provisionamento de um recurso de implantação. |
| Deployment resource requested | Sim | Emitido antes do provisionamento de um recurso de implantação. |
| Disk allocation | Sim | Emitido para a pré-alocação de recursos de disco. |
| Disk attach | Sim | <p>Emitido antes que um disco seja anexado a uma máquina. O <code>Disk attach</code> é um evento de leitura e gravação. As propriedades de disco compatíveis com write-back são:</p> <ul style="list-style-type: none"> ■ <code>diskFullPaths</code> ■ <code>diskDatastoreNames</code> ■ <code>diskParentDirs</code> <p>Todas as três propriedades do vSphere específicas de disco são necessárias para atualizações. Todas as outras propriedades são somente leitura.</p> <p>Observação O write-back é opcional para as vSphere primeira classe de discos.</p> |
| Disk detach | Sim | Emitido depois que um disco é desanexado de uma máquina. O <code>Disk detach</code> é um evento de somente leitura. |
| Disk post removal | Sim | Emitido após a exclusão de um recurso de disco. |
| Disk post resize | Sim | Emitido após o redimensionamento de um recurso de disco. |
| Kubernetes cluster allocation | Sim | Emitido para a pré-alocação de recursos para um cluster do Kubernetes. |
| Kubernetes cluster post provision | Sim | Emitido após a provisão de um cluster do Kubernetes. |
| Kubernetes cluster post removal | Sim | Emitido após a exclusão de um cluster do Kubernetes. |
| Kubernetes cluster provision | Sim | Emitido antes de um cluster do Kubernetes ser provisionado. |

Tabela 6-7. Tópicos de evento do Cloud Assembly (continuação)

| Tópico de evento | Bloqueável | Descrição |
|--|------------|--|
| Kubernetes cluster removal | Sim | Emitido antes que o processo de exclusão de um cluster do Kubernetes seja iniciado. |
| Kubernetes namespace allocation | Sim | Emitido durante a pré-alocação para recursos do namespace do Kubernetes. |
| Kubernetes namespace post provision | Sim | Emitido depois que um recurso do namespace do Kubernetes é provisionado. |
| Kubernetes namespace post removal | Sim | Emitido depois de um recurso de namespace Kubernetes ser removido. |
| Kubernetes namespace provision | Sim | Emitido antes de um namespace do Kubernetes ser provisionado. |
| Kubernetes namespace removal | Sim | Emitido antes de um recurso de cluster de namespace ser removido. |
| Kubernetes supervisor namespace allocation | Sim | Emitido durante a pré-alocação para recursos do namespace do supervisor do Kubernetes. |
| Kubernetes supervisor namespace post provision | Sim | Emitido depois que um namespace do supervisor é provisionado. |
| Kubernetes supervisor namespace post removal | Sim | Emitido depois de um recurso de namespace de supervisor ser removido. |
| Kubernetes supervisor namespace provision | Sim | Emitido antes de um namespace do supervisor ser provisionado. |
| Kubernetes supervisor namespace removal | Sim | Emitido antes de um recurso de namespace do supervisor ser removido. |
| Load balancer post provision | Sim | Emitido após o provisionamento de um balanceador de carga. |
| Load balancer post removal | Sim | Emitido após a remoção de um balanceador de carga. |
| Load balancer provision | Sim | Emitido antes do provisionamento de um balanceador de carga. |
| Load balancer removal | Sim | Emitido antes da remoção de um balanceador de carga. |
| Network Configure | Sim | Emitido quando a rede é configurada durante a alocação de processamento. |
| Observação O tópico Configurar Rede oferece suporte a vários endereços IP/NICs. | | |

Tabela 6-7. Tópicos de evento do Cloud Assembly (continuação)

| Tópico de evento | Bloqueável | Descrição |
|-------------------------------|------------|---|
| Network post provisioning | Sim | Emitido após um recurso de rede ser provisionado. |
| Network post removal | Sim | Emitido após a remoção de um recurso de rede. |
| Network provisioning | Sim | Emitido antes de um recurso de rede ser provisionado. |
| Network removal | Sim | Emitido antes de um recurso de rede ser removido. |
| Project Lifecycle Event Topic | Não | Emitido quando um projeto é criado, atualizado ou excluído. |
| Provisioning request | Sim | Emitido antes de um grupo de segurança ser removido. |
| Security group post provision | Sim | Emitido após um grupo de segurança ser provisionado. |
| Security group post removal | Sim | Emitido após um grupo de segurança ser removido. |
| Security group provisioning | Sim | Emitido antes de um grupo de segurança ser provisionado. |
| Security group removal | Sim | Emitido antes de um grupo de segurança ser removido. |

Parâmetros de evento

Depois de adicionar um tópico de evento, é possível visualizar os parâmetros desse tópico de evento. Estes parâmetros de evento definem a estrutura de payload do evento ou `inputProperties`. Alguns parâmetros de evento não podem ser modificados e marcados como somente leitura. Você pode identificar esses parâmetros somente leitura clicando no ícone de informações à direita do parâmetro.

Remover log de evento de extensibilidade

A página eventos de extensibilidade mostra uma lista de todos os eventos que ocorreram no ambiente.

É possível visualizar os logs de eventos de extensibilidade navegando até **Extensibilidade > Eventos**. Também é possível filtrar a lista de eventos por uma ou mais propriedades de uma vez. Para visualizar detalhes adicionais de um evento individual, selecione o ID do evento.

| ID | Timestamp | Event Topic | User Name | Target ID | Description |
|--------------------------------------|--------------------|-------------|-----------|-----------|-------------|
| cbaf56ce-a324-f5ae-5dd1-66d1e59f1a6 | 04/28/20, 1:10 PM | N/A | N/A | endpoints | CREATE |
| ef621f51-2906-dce2-14ab-68c17132d756 | 03/25/20, 4:22 PM | N/A | N/A | endpoints | CREATE |
| 468e8e55-cf27-e77e-0179-1b5b736717b3 | 03/25/20, 10:12 AM | N/A | N/A | endpoints | CREATE |
| d9482883-d1ae-5899-fb06-852c202cc178 | 03/20/20, 2:41 PM | N/A | N/A | endpoints | CREATE |
| 38584d40-e663-631f-7098-3747aa528d12 | 01/30/20, 5:35 PM | N/A | N/A | endpoints | CREATE |

Criar uma assinatura de extensibilidade

Usando uma integração com o vRealize Orchestrator, ou ações de extensibilidade com o Cloud Assembly, você pode criar assinaturas para estender seus aplicativos.

Assinaturas de extensibilidade permitem estender aplicativos, disparando fluxos de trabalho ou ações em eventos de ciclo de vida específicos. Também é possível aplicar filtros às suas assinaturas para definir condições booleanas para o evento especificado. Por exemplo, o evento e o fluxo de trabalho ou a ação apenas serão disparados se a expressão booleana for `'true'`. Isso é útil para cenários em que você deseja controlar quando eventos, ações ou fluxos de trabalho são disparados.

Pré-requisitos

- Verifique se você tem a função de usuário de administrador da nuvem.
- Se estiver usando fluxos de trabalho do vRealize Orchestrator:
 - A biblioteca do Cliente vRealize Orchestrator incorporado ou a biblioteca de qualquer instância externa integrada do vRealize Orchestrator.
- Se você estiver usando ações de extensibilidade:
 - Scripts de ação de extensibilidade existentes. Para obter mais informações, consulte [Como criar ações de extensibilidade](#).

Procedimentos

- 1 Selecione **Extensibilidade > Assinaturas**.
- 2 Clique em **Nova Assinatura**.
- 3 Digite os detalhes da assinatura.
- 4 Defina o **Escopo da organização** para a assinatura.

Observação Para obter mais informações sobre como criar assinaturas de extensibilidade para provedores e tenants de organização, consulte [Criar assinaturas de extensibilidade para provedores ou tenants](#).

- 5 Selecione um **Tópico de Evento**.

- 6 (Opcional) Defina as condições para o tópico de evento.

Observação As condições podem ser criadas usando uma expressão de sintaxe JavaScript. Essa expressão pode incluir operadores booleanos, como "&&" (AND), "||" (OR), "^" (XOR) e "!" (NOT). Você também pode usar operadores aritméticos, como "==" (equal to), "!=" (not equal to), ">=" (greater than or equal), "<=" (less than or equal), ">" (greater than) e "<" (less than). Expressões booleanas mais complexas podem ser criadas a partir de expressões mais simples. Para acessar o payload do evento de acordo com os parâmetros de tópicos especificados, use 'event.data' ou qualquer uma das propriedades de cabeçalho do evento: `sourceType`, `sourceIdentity`, `timeStamp`, `eventType`, `eventTopicId`, `correlationType`, `correlationId`, `description`, `targetType`, `targetId`, `userName` e `orgId`.

- 7 Em **Ação/fluxo de trabalho**, selecione um item executável para a assinatura de extensibilidade.
- 8 (Opcional) Se aplicável, configure o comportamento de bloqueio para o tópico de evento.
- 9 (Opcional) Para definir o escopo de projeto da assinatura de extensibilidade, desmarque **Qualquer Projeto** e clique em **Adicionar Projetos**.

Observação Se o escopo de organização da assinatura estiver definido como **Qualquer organização de tenant**, o escopo de projeto sempre será definido como **Qualquer Projeto** e não será possível alterá-lo. Você apenas poderá alterar o escopo de projeto se o escopo de organização estiver definido como a organização do provedor.

- 10 Para salvar a assinatura, clique em **Salvar**.

Resultados

Sua assinatura foi criada. Quando ocorre um evento categorizado pelo tópico de evento selecionado, o fluxo de trabalho ou a ação de extensibilidade vinculado do vRealize Orchestrator é iniciado, e todos os assinantes são notificados.

Próximo passo

Depois de criar sua assinatura, é possível criar ou implantar um modelo de nuvem para vincular e usar a assinatura. Você também pode verificar o status do fluxo de trabalho ou da ação de extensibilidade executada na guia **Extensibilidade** do Cloud Assembly. Para assinaturas contendo fluxos de trabalho do vRealize Orchestrator, também é possível monitorar as execuções e o status do fluxo de trabalho do Cliente do vRealize Orchestrator.

Usando assinaturas de extensibilidade para gerenciar a expiração da implantação

Você pode gerenciar implantações expiradas e seus recursos usando a ação `Expire` juntamente com tópicos de eventos existentes.

Após a expiração de uma concessão de implantação no seu ambiente, você poderá usar tópicos de eventos de extensibilidade para realizar tarefas, como interromper o backup ou monitorar qualquer recurso de implantação. Para realizar essas operações de dia 2, a API do vRealize Automation usa uma ação `Expire` em nível de sistema. Essa ação é disparada automaticamente pelo sistema sempre que uma concessão de implantação na sua organização expira. O gatilho da ação `Expire` precede o evento de desligamento para todos os recursos associados a essa implantação.

Observação Em versões anteriores do produto, o evento de desligamento era disparado no nível de implantação após a expiração da concessão. Agora, o evento de desligamento é disparado no nível do recurso para cada recurso de implantação que está no estado ligado.

A ação `Expire` está incluída na payload de eventos existentes, como **Ação de implantação solicitada** e **Ação de implantação concluída**, e usa o parâmetro `deploymentid` para realizar as tarefas pré-expiração e pós-expiração associadas aos recursos de implantação.

Observação A ação `Expire` é disparada aproximadamente de 10 a 15 minutos após a expiração da concessão de implantação. O sistema não aciona eventos de expiração de concessão antes da expiração real da concessão. `Expire` é uma ação no nível do sistema, e os usuários não podem disparar os eventos associados a ela manualmente.

Para o caso de uso atual, você está usando o tópico de evento **Ação de implantação solicitada** junto com a ação `Expire` para fazer backup de uma máquina virtual na sua implantação como um modelo. Para esse caso, o backup é realizado usando um fluxo de trabalho do vRealize Orchestrator, mas a mesma tarefa também pode ser realizada usando uma ação de extensibilidade como o item executável da assinatura.

Procedimentos

- 1 Navegue até **Extensibilidade > Assinaturas** e clique em **Nova Assinatura**.
- 2 Insira um nome para a assinatura.
- 3 Em **Status**, verifique se a assinatura está ativada.
- 4 Em **Tópico de Evento**, selecione o tópico de evento **Ação de implantação solicitada**.
- 5 Ative a opção **Condição** e adicione um filtro para a ação de expiração:

```
event.data.actionName == 'Expire'
```

Observação O tópico de evento **Ação de implantação solicitada** pode ser acionado por diferentes operações de implantação de dia 2, como alterar a duração da concessão da implantação. Adicionar o filtro de ação de expiração de concessão garante que a assinatura seja disparada apenas para eventos de expiração.

6 Em **Ação/fluxo de trabalho**, adicione o fluxo de trabalho do vRealize Orchestrator.

O esquema desse fluxo de trabalho de amostra inclui uma tarefa programável por script e um elemento de fluxo de trabalho que inclui o fluxo de trabalho **Clonar máquina virtual, sem personalização**, que vem pré-configurado com o vRealize Orchestrator. O elemento de tarefa programável por script inclui o seguinte script de amostra:

```
System.log("Lease expiry action triggered to clone a VM...")

System.log("Deployment Id is: " + inputProperties.deploymentId);
inputHeaders = new Properties();
deploymentId = inputProperties.deploymentId;
pathUriVariable = "/deployment/api/deployments/" + deploymentId + "/resources";
var restClient = vRAHost.createRestClient();
var request = restClient.createRequest("GET", pathUriVariable, null);
var keys = inputHeaders.keys;
for(var key in keys){
    request.setHeader(keys[key], inputHeaders.get(keys[key]));
}
var response = restClient.execute(request);
System.log("Content as string: " + response.contentAsString);
var content = response.contentAsString;
var obj = JSON.parse(content);

var object = new Properties(obj);
var contentJson = object.content;
for (var i = 0; i < contentJson.length; i++) {
    var resources = contentJson[i];

    var resourceProperties = resources.properties;
    System.log("Resource name is: " + resourceProperties.resourceName)
    resourceName = resourceProperties.resourceName;
}

var query = "xpath:name='" + resourceName + "'";
var vms=Server.findAllForType("VC:VirtualMachine", query);
vcVM=vms[0];

System.log("VM input is: " + vcVM);
dataStoreOutput = dataStore
template= true;
name="test-vm-name"
```

7 Decida se deseja definir a assinatura como com bloqueio ou sem bloqueio.

Observação Tornar a assinatura com bloqueio significa que o evento de desligamento para os recursos de implantação é disparado somente depois que o item executável, neste caso, o fluxo de trabalho de expiração de concessão, conclui sua execução com êxito. Tornar a assinatura sem bloqueio significa que o evento de desligamento é acionado para os recursos de implantação, independentemente do status da execução do fluxo de trabalho.

8 Para concluir a edição da assinatura, clique em **Salvar**.

Próximo passo

Depois que a assinatura de extensibilidade for acionada pelo evento de expiração de concessão e a execução do fluxo de trabalho for bem-sucedida, navegue até o vSphere Web Client e valide se a sua máquina virtual foi convertida em um modelo.

Solução de problemas com uma assinatura de extensibilidade

Solucionar problemas de falhas na assinatura de extensibilidade.

Quando a assinatura falha, geralmente é reflexo de erros no seu fluxo de trabalho ou script de ação de extensibilidade.

Exibir parâmetros e payload do tópico

É possível usar um script de parâmetros de tópico de assinatura de despejo para exibir os parâmetros e o payload específicos da máquina virtual em determinado estágio de evento.

Esse script é especialmente útil para depurar e verificar as entradas disponíveis para o fluxo de trabalho do vRealize Orchestrator. Para exibir todos os parâmetros de sua máquina virtual, use o seguinte script com o fluxo de trabalho:

```
function dumpProperties(props, lvl) {
    var keys = props.keys;
    var prefix = ""
    for (var i=0; i<lvl; i++){
        prefix = prefix + " ";
    }
    for (k in keys){
        var key = keys[k];
        var value = props.get(keys[k])
        if ("Properties" == System.getObjectType(value)) {
            System.log(prefix + key + "[")
            dumpProperties(value, (lvl+2));
            System.log(prefix+ "]")
        } else{
            System.log( prefix + key + ":" + value)
        }
    }
}

dumpProperties(inputProperties, 0)

customProps = inputProperties.get("customProperties")
```

Histórico da versão da assinatura

Se a sua assinatura falhar, será possível visualizar o histórico da versão.

Visualização do histórico da versão da assinatura

A guia **Histórico de Versões** do editor de assinatura pode mostrar o histórico de alterações da sua assinatura, incluindo o usuário e a data da alteração. Você também pode comparar diferentes versões de assinatura clicando em **Comparar com**. Se a assinatura falhar ou estiver em execução incorreta, o histórico da versão poderá ajudar a identificar a causa.

Gerenciando implantações e recursos no Cloud Assembly

7

Como administrador de nuvem ou desenvolvedor de modelos de nuvem, você usa a guia Recursos para gerenciar seus recursos. Os recursos podem ser aqueles que você implantou, mas também podem ser aqueles descobertos em suas contas de nuvem, recursos descobertos que você integrou ou de outra forma disponíveis para gerenciamento pelo Cloud Assembly

Este capítulo inclui os seguintes tópicos:

- [Como gerenciar implantações do Cloud Assembly](#)
- [Gerenciando recursos no Cloud Assembly](#)

Como gerenciar implantações do Cloud Assembly

Como administrador de nuvem ou desenvolvedor de modelos de nuvem do Cloud Assembly, você usa a página Implantações para gerenciar suas implantações e os recursos associados. É possível solucionar falhas em processos de provisionamento, fazer alterações em recursos e destruir implantações não utilizadas.

As implantações incluem modelos de nuvem implantados e recursos integrados. Também é possível que os recursos criados usando a API de IaaS apareçam como implantações.

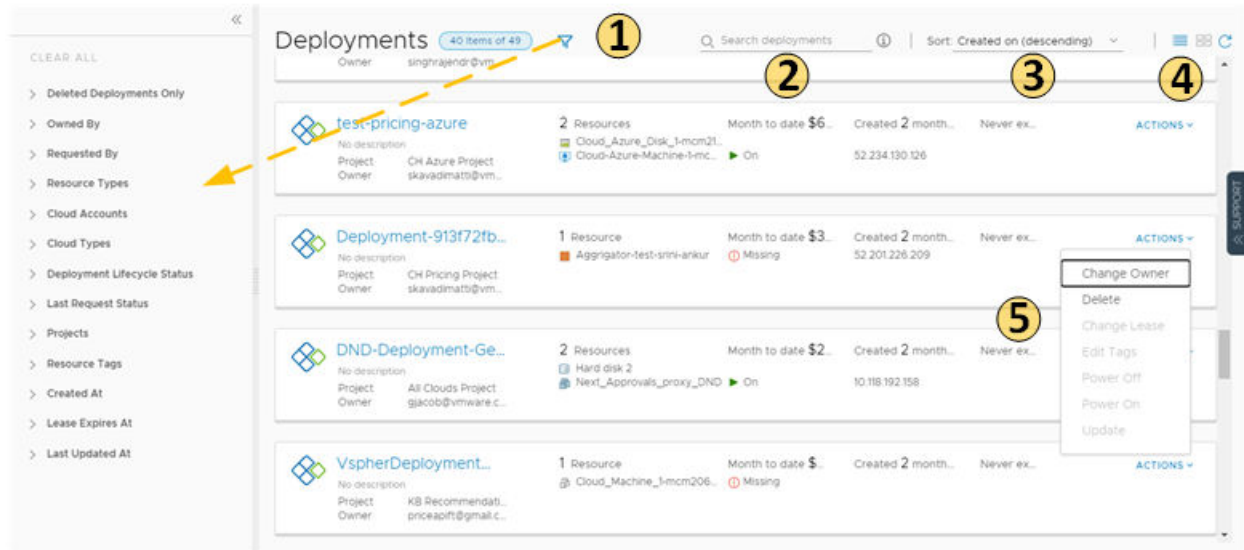
Se você gerencia um pequeno número de implantações, os cartões de implantação fornecem uma exibição gráfica para gerenciá-las. Se você gerencia um grande número de implantações, a lista de implantações e a lista de recursos fornecem uma exibição de gerenciamento mais robusta.

Para visualizar suas implantações, selecione **Recursos > Implantações**.

Trabalhando com cartões de implantação e a lista de implantações

É possível localizar e gerenciar as implantações usando a lista de cartões. É possível filtrar ou pesquisar implantações específicas e depois executar ações sobre essas implantações.

Figura 7-1. Exibições de cartões da página de implantações



1 Filtre as solicitações com base nos atributos.

Por exemplo, você pode filtrar com base em proprietário, projetos, data de expiração da concessão ou outras opções de filtragem. Ou talvez você queira localizar todas as implantações para dois projetos com uma determinada tag. Quando você construir o filtro para os projetos e o exemplo de tag, os resultados estarão em conformidade com os seguintes critérios: (Project1 OR Project2) AND Tag1.

Os valores que você vê no painel de filtro dependem das implantações atuais que você tem permissão para exibir ou gerenciar.

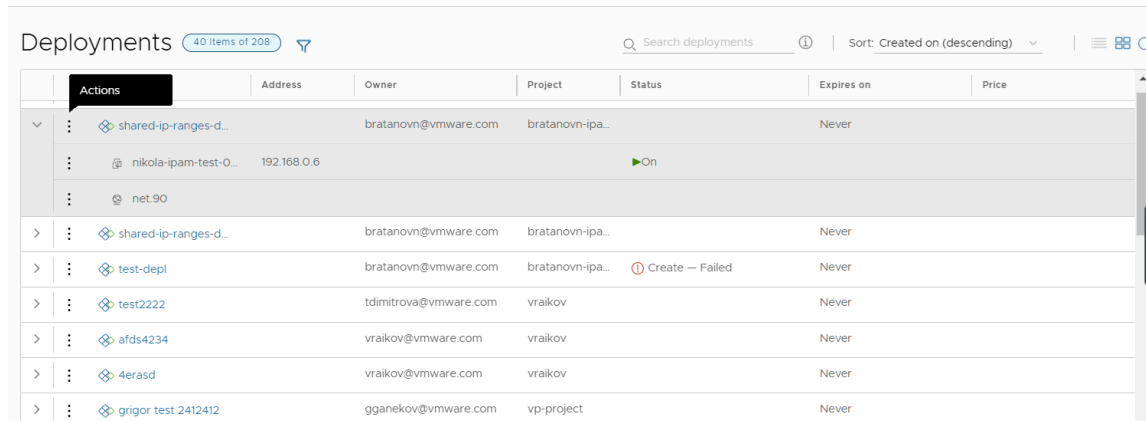
A maioria dos filtros e como usá-los é relativamente óbvia. Informações adicionais sobre alguns desses filtros são fornecidas abaixo.

- 2 Procure por implantações com base nas palavras-chave ou no solicitante.
- 3 Classifique a lista para ordenar por hora ou nome.
- 4 Alterne entre o cartão de implantação e as exibições de lista de implantações.
- 5 Execute ações no nível da implantação na implantação, incluindo a exclusão de implantações não utilizadas para recuperar recursos.

Também é possível ver os custos de implantação, as datas de expiração e o status.

Você pode alternar entre o cartão e a exibição de lista no canto superior direito da página, à direita da caixa de texto Classificar. A exibição de lista para ser usada gerenciar várias implantações em menos páginas.

Figura 7-2. Exibição de lista da páginas de implantações



| Actions | Address | Owner | Project | Status | Expires on | Price |
|--|-------------|-----------------------|------------------|-----------------|------------|-------|
| <ul style="list-style-type: none"> shared-ip-ranges-d... nikola-ipam-test-0... net.90 | 192.168.0.6 | bratanovn@vmware.com | bratanovn-ipa... | On | Never | |
| shared-ip-ranges-d... | | bratanovn@vmware.com | bratanovn-ipa... | Never | Never | |
| test-depl | | bratanovn@vmware.com | bratanovn-ipa... | Create — Failed | Never | |
| test2222 | | tdimitrova@vmware.com | vraikov | Never | Never | |
| afds4234 | | vraikov@vmware.com | vraikov | Never | Never | |
| 4erasd | | vraikov@vmware.com | vraikov | Never | Never | |
| grigor test 2412412 | | gganekov@vmware.com | vp-project | Never | Never | |

Trabalhando com filtros de implantação selecionados

A tabela a seguir não é uma lista definitiva de opções de filtro. A maioria deles é evidente. No entanto, alguns dos filtros exigem um pouco mais de conhecimento.

Tabela 7-1. Informações de filtro selecionadas

| Nome do filtro | Descrição |
|---|--|
| Recursos otimizáveis apenas | Se você tiver integrado o vRealize Operations Manager e estiver usando a integração para identificar recursos recuperáveis, poderá ativar o filtro para limitar a lista de implantações qualificadas. |
| Status do Ciclo de Vida da Implantação | <p>Os filtros Status do Ciclo de Vida da Implantação e Status da Última Solicitação podem ser usados individualmente ou em combinação, particularmente se você gerencia um grande número de implantações. Exemplos estão incluídos no final da seção Status da última solicitação, abaixo.</p> <p>O Status do Ciclo de Vida da Implantação filtra o estado atual da implantação com base nas operações de gerenciamento.</p> <p>Esse filtro não está disponível para implantações excluídas.</p> <p>Os valores que você vê no painel de filtro dependem do estado atual das implantações listadas. Talvez você não veja todos os valores possíveis. A lista a seguir inclui todos os valores possíveis. Ações de dia 2 são incluídas no status da Atualização.</p> <ul style="list-style-type: none"> ■ Criar - Bem-sucedida ■ Criar - Em Andamento ■ Criar - Falha ■ Atualizar - Bem-sucedida ■ Atualizar - Em Andamento ■ Atualizar - Falha ■ Excluir - Em Andamento ■ Excluir - Falha |
| Filtros de Status da Última Solicitação | <p>O Status da Última Solicitação filtra a última operação ou ação que foi realizada na implantação.</p> <p>Esse filtro não está disponível para implantações excluídas.</p> <p>Os valores que você vê no painel de filtro dependem das últimas operações que foram realizadas nas implantações listadas. Talvez você não veja todos os valores possíveis. A lista a seguir compreende todos os valores possíveis.</p> <ul style="list-style-type: none"> ■ Pendente. A primeira etapa de uma solicitação em que a ação é enviada, mas o processo de implantação ainda não foi iniciado. ■ Falhou. A solicitação sofreu uma falha durante qualquer etapa do processo de implantação. ■ Cancelada. A solicitação foi cancelada por um usuário enquanto o processo de implantação estava sendo processado e ainda não foi concluído. ■ Bem-sucedida. A solicitação criou, atualizou ou excluiu uma implantação com êxito. |

Tabela 7-1. Informações de filtro selecionadas (continuação)

| Nome do filtro | Descrição |
|----------------|--|
| | <ul style="list-style-type: none"> ■ Em Andamento. O processo de implantação está em execução. Estados de implantação adicionais, por exemplo, Inicialização e Conclusão, que você vê na guia Histórico da implantação não são fornecidos como filtros, mas é possível usar o filtro Em Andamento para localizar implantações nesses estados. ■ Aprovação Pendente. A solicitação acionou uma ou mais políticas de aprovação. O processo está aguardando uma resposta à solicitação de aprovação. ■ Aprovação Rejeitada. A solicitação foi negada pelos aprovadores nas políticas de aprovação acionadas. A solicitação não continua. <p>Os exemplos a seguir ilustram como usar os filtros Status do Ciclo de Vida da Implantação e Status da Última Solicitação individualmente ou juntos.</p> <ul style="list-style-type: none"> ■ Para encontrar todas as solicitações de exclusão que falharam, selecione Excluir - Falha no filtro Status do Ciclo de Vida da Implantação. ■ Para encontrar todas as solicitações que estão aguardando aprovação, selecione Aprovação Pendente no filtro Status da Última Solicitação . ■ Para encontrar as solicitações de exclusão em que a solicitação de aprovação ainda está pendente, selecione Excluir - Em Andamento no filtro Status do Ciclo de Vida da Implantação e Aprovação Pendente no filtro Status da Última Solicitação. |

Como monitorar implantações no Cloud Assembly

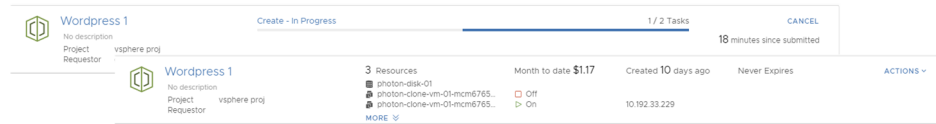
Depois de implantar um modelo de nuvem do Cloud Assembly, é possível monitorar sua solicitação para garantir que os recursos sejam provisionados e estejam em execução. A partir do cartão de implantação, é possível verificar o provisionamento de seus recursos. Em seguida, pode-se examinar os detalhes da implantação. Por fim, você pode visualizar e filtrar implantações excluídas por até 90 dias após a exclusão.

Procedimentos

- 1 Selecione **Recursos > Implantações** e localize sua implantação usando o filtro e a pesquisa, se necessário.

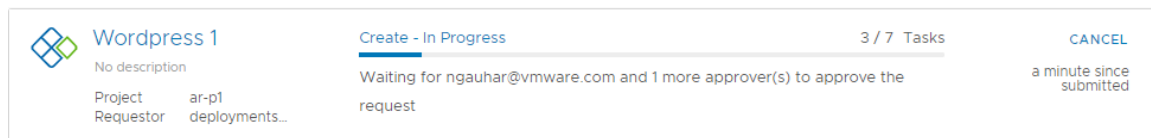
2 Revise o status do cartão.

Se a implantação estiver em andamento, a barra de processos indicará o número de tarefas restantes. Se a implantação foi concluída com êxito, o cartão exibirá os detalhes básicos sobre



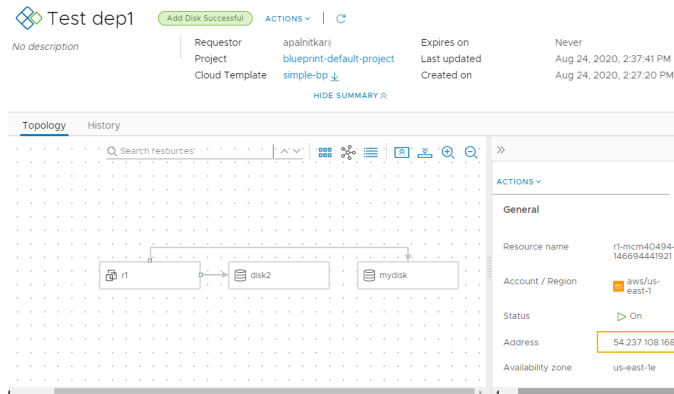
a implantação.

Se uma política de aprovação for acionada para a sua solicitação, você poderá vê-la em um estado em andamento com o nome de pelo menos um aprovador. As políticas de aprovação são definidas no Service Broker pelo seu administrador. Os aprovadores estão definidos na política. Os aprovadores aprovam as solicitações no Service Broker. Você também pode encontrar aprovações em ações de dia 2.



3 Para determinar onde seus recursos foram implantados, clique no nome da implantação e revise os detalhes na página Topologia.

Você provavelmente vai precisar do endereço IP para o componente principal. Ao clicar em cada componente, observe as informações fornecidas que são específicas para o componente. Neste exemplo, o endereço IP é realçado.



A disponibilidade do link externo depende do provedor de nuvem. Onde estiver disponível, é necessário ter a credencial nesse provedor para acessar o componente.

Próximo passo

- É possível alterar sua implantação. Consulte [Como gerenciar o ciclo de vida de uma implantação do Cloud Assembly concluída](#).
- Se a implantação falhar, consulte [O que fazer se uma implantação do Cloud Assembly falhar](#).

O que fazer se uma implantação do Cloud Assembly falhar

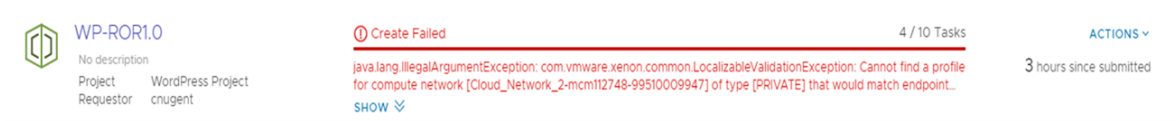
A solicitação de implantação pode falhar por muitos motivos. Pode ser devido ao tráfego de rede, à falta de recursos no provedor de nuvem de destino ou a uma especificação de implantação com falha. Ou a implantação foi bem-sucedida, mas parece não estar funcionando. Você pode usar o Cloud Assembly para examinar a sua implantação, analisar as mensagens de erro e determinar se o problema é o ambiente, a especificação de carga de trabalho solicitada ou algo mais.

Use este fluxo de trabalho para começar a investigação. O processo pode revelar que a falha ocorreu devido a um problema ambiental transitório. A reimplantação da solicitação depois de verificar se as condições foram melhoradas resolve este tipo de problema. Em outros casos, sua investigação pode exigir que examine outras áreas em detalhes.

Como membro do projeto, é possível revisar os detalhes da solicitação no Cloud Assembly.

Procedimentos

- 1 Para determinar se uma solicitação falhou, selecione **Recursos > Implantações** e localize o cartão de implantação.



As implantações com falha são indicadas no cartão.

- a Revise a mensagem de erro.
- b Para obter mais informações, clique no nome da implantação para os detalhes da implantação.

2 Na página detalhes da implantação, clique na guia **Histórico**.

WP - ROR2 Create Failed ACTIONS | C

No description

Requestor: fritz
Project: Tiger Team
Cloud Template: WordPress Template

Expires on: Never
Last updated: Sep 9, 2020, 12:06:42 PM
Created on: Sep 9, 2020, 12:06:38 PM

HIDE SUMMARY

Topology History

Sep 9, 2020, 12:06:42 PM CREATE fritz 2.a

Create Failed Requested by: fritz Provisioning diagram 2.c

Events Request details

| Timestamp | Status | Resource type | Resource name | Details 2.b |
|------------------|-------------------------|---------------|--------------------|--|
| Sep 9, 2020, ... | REQUEST_FAILED | | | Could not find any profile to match network 'WP-Network-Private' of type 'EXISTING' with constraints '[type:isolated-net, env:dev]'. |
| Sep 9, 2020, ... | COMPLETION_FINISHED | | | |
| Sep 9, 2020, ... | COMPLETION_IN_PROGRE... | | | |
| Sep 9, 2020, ... | ALLOCATE_FAILED | Cloud.Network | WP-Network-Private | Could not find any profile to match |

8 Events

- a Revise a árvore de eventos para ver onde o processo de provisionamento falhou. Essa árvore é útil, quando a alteração falha ao modificar uma implantação.

A árvore também mostra quando você executa ações de implantação. É possível usar a árvore para solucionar falhas de alterações.

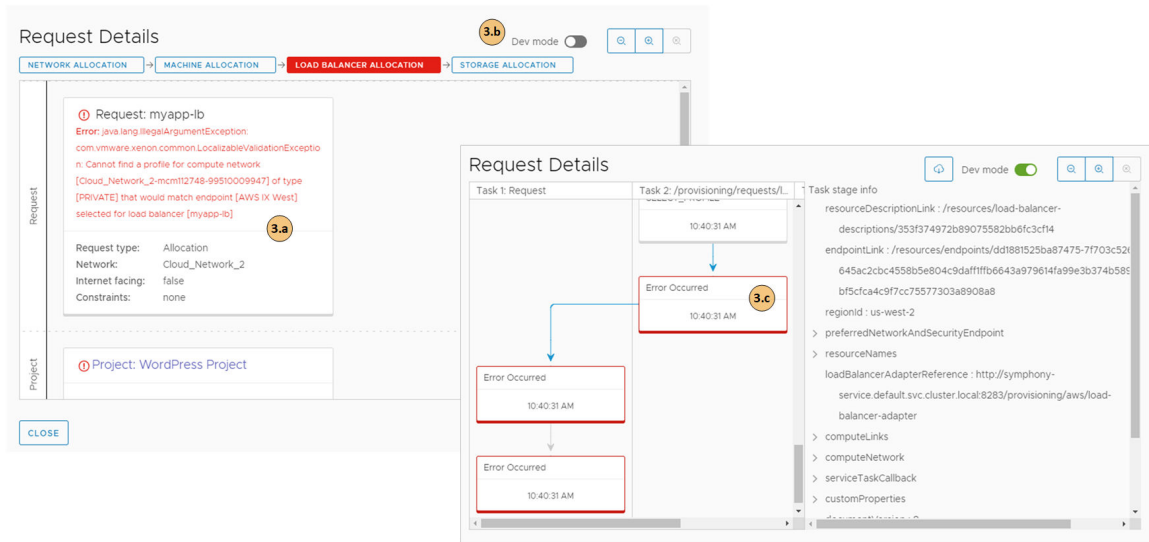
- b Os **Detalhes** fornecem uma versão mais detalhada da mensagem de erro.

- c Se o item solicitado foi um modelo de nuvem do Cloud Assembly, o link à direita da mensagem abre o Cloud Assembly para visualizar os **Detalhes da Solicitação**.

3 Os **Detalhes da Solicitação** fornecem o fluxo de trabalho de provisionamento de componentes com falha para pesquisar o problema.

O histórico de solicitações é retido por 48 horas.

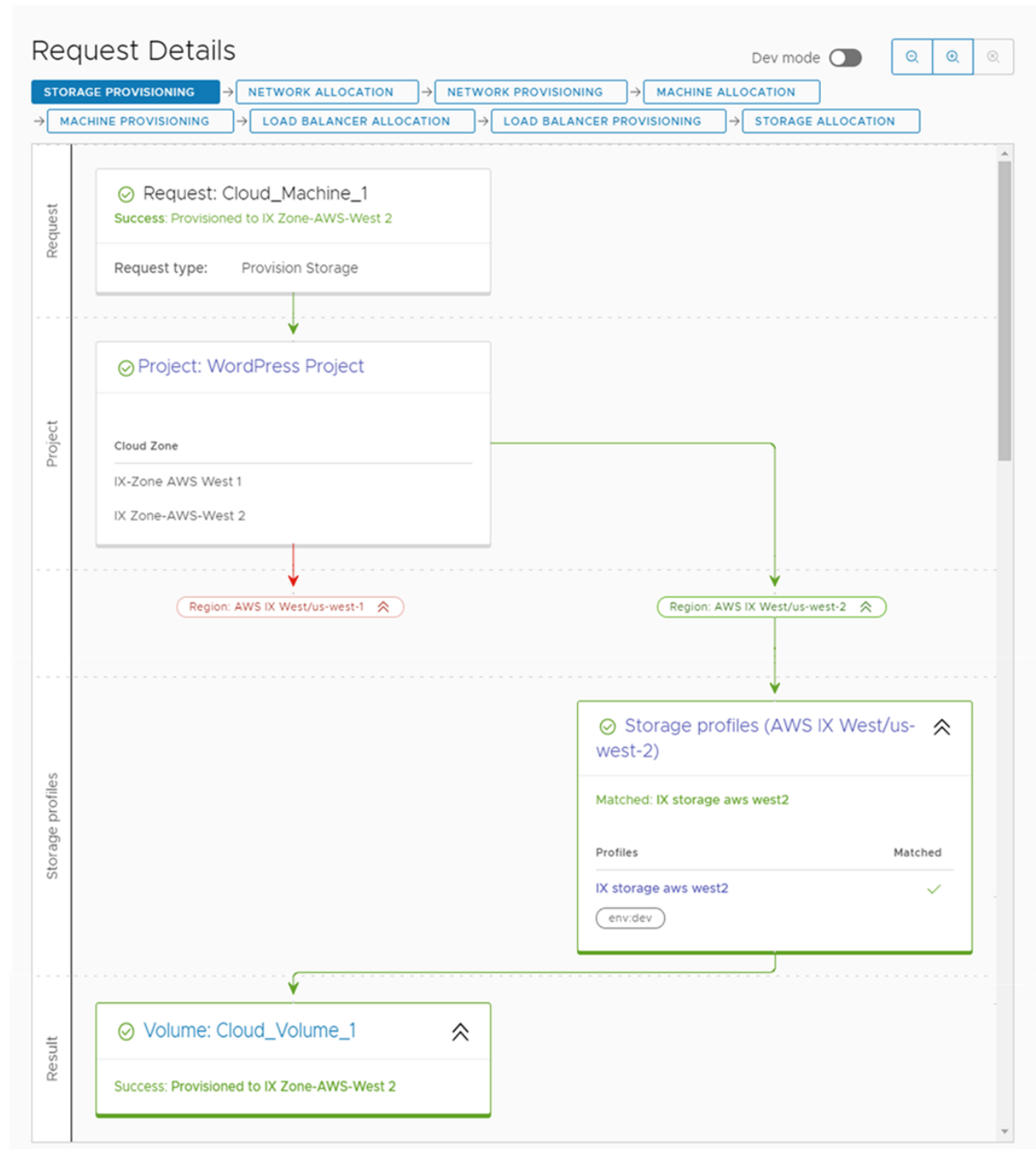
Visualize e filtre o histórico de implantação excluído por até 90 dias após a exclusão



- a Revise a mensagem de erro.
 - b É possível ativar o **Modo Dev** para alternar entre o fluxo de trabalho de provisionamento simples e um fluxograma mais detalhado.
 - c Clique no cartão para revisar o script de implantação.
- 4 Resolva os erros e reimplante o modelo de nuvem.
- Os erros podem estar na construção do modelo ou podem estar relacionados à maneira como a infraestrutura está configurada.

Próximo passo

Quando os erros forem resolvidos e o modelo de nuvem for implantado, é possível ver informações semelhantes ao exemplo a seguir nos Detalhes da Solicitação. Para ver os detalhes da solicitação, selecione **Infraestrutura > Atividade > Solicitações**.



Como gerenciar o ciclo de vida de uma implantação do Cloud Assembly concluída

Depois que uma implantação é provisionada e está em execução, há várias ações que podem ser executadas para gerenciar a implantação. O gerenciamento do ciclo de vida pode incluir ligar ou desligar, redimensionar e excluir uma implantação. Também é possível executar várias ações em componentes individuais para gerenciá-las.

Procedimentos

- 1 Selecione **Recursos > Implantações** e localize sua implantação.
- 2 Para acessar os detalhes da implantação, clique no nome da implantação.

Você usa os detalhes da implantação para compreender como os recursos são implantados e quais mudanças foram feitas. Você também pode ver informações de preços, a integridade atual da implantação e se tem recursos que precisam ser modificados.

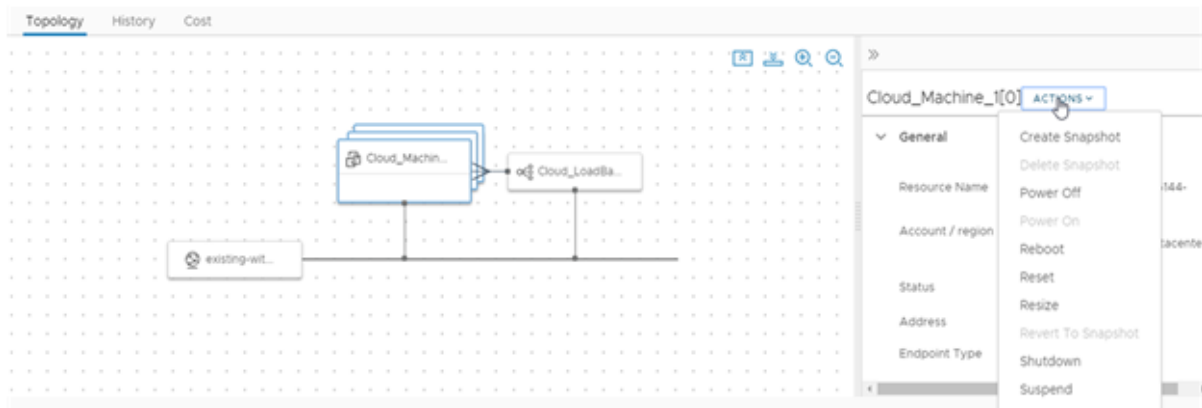
The image displays a sequence of overlapping screenshots from the vRealize Automation Cloud Assembly user interface, illustrating different functional areas:

- Topology View:** Shows a resource graph with a search bar and expandable sections for 'Cloud_vSphere_Machine_1[0]' and 'Cloud_vSphere_Machine_1[1]', each with an 'Attached volumes' section.
- History View:** Displays a 'Create' operation with a 'Successful' status. It includes a table with columns for Timestamp, Status, Resource type, Resource name, and Details, showing events from Mar 2, 2021.
- Price View:** Shows a 'Price analysis' section with 'Overall' and 'Details' tabs. It displays price information (\$0.38) and a bar chart for price over time.
- Monitor View:** Features a 'By Health Status' section and a 'Monitor' tab. It shows resource details for 'Cloud_vSphere_Machine_1-mcm306191-163093649552' and a line graph for CPU usage over time.
- Alerts View:** Displays a list of alerts, including 'Definition_Deployment_VM' and 'AlertDefinition_Deployment_has_cost', with details on their status and impact.
- Optimize View:** Shows a summary of 'Underutilized VMs' (2 Idle VMs, 0 Powered Off VMs) and a detailed table of underutilized VMs with columns for Status, VM name, Allocated CPU, Allocated Memory, and Allocated Storage.

- **Guia Topologia.** Pode-se usar a guia Topologia para compreender a estrutura e os recursos de implantação.
- **Guia Histórico.** A guia Histórico inclui todos os eventos de provisionamento e quaisquer eventos relacionados a ações executadas após a implantação do item solicitado. Se houver algum problema com o processo de provisionamento, os eventos da guia Histórico ajudarão a solucionar as falhas.

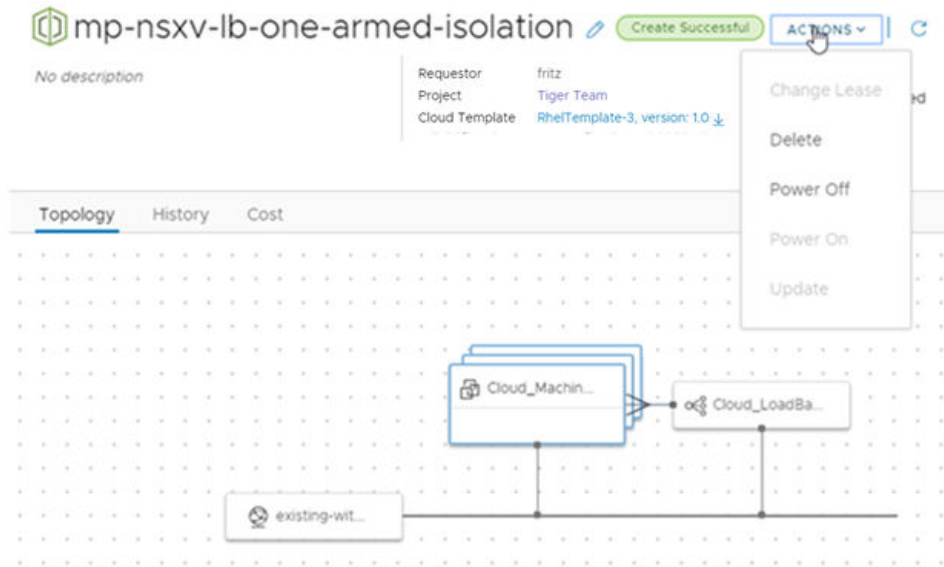
- Guia **Preços**. Você pode usar o cartão de preços para compreender quanto a implantação está custando à sua organização. As informações de preços são baseadas no vRealize Operations Manager ou nas integrações do CloudHealth.
 - Guia **Monitoramento**. Os dados da guia Monitoramento fornece informações sobre a integridade da sua implantação com base nos dados de vRealize Operations Manager.
 - Guia **Alertas**. A guia Alertas fornece alertas ativos sobre os recursos de implantação. Você pode descartar o alerta ou adicionar notas de referência. Os alertas são baseados em dados do vRealize Operations Manager.
 - Guia **Otimizar**. A guia Otimizar fornece informações de utilização sobre sua implantação e oferece sugestões para recuperar ou modificar os recursos para otimizar o consumo de recursos. As informações de otimização se baseiam nos dados de vRealize Operations Manager.
- 3 Se for determinado que uma implantação é muito cara em sua configuração atual e deseja-se redimensionar um componente, selecione o componente na página topologia e, em seguida, selecione **Ações > Redimensionar** na página do componente.

As ações disponíveis dependem do componente, da conta de nuvem e de suas permissões.



- 4 Como parte do ciclo de vida de desenvolvimento, uma de suas implantações não é mais necessária. Para remover os recursos de implantação e recuperação, selecione **Ações > Excluir**.

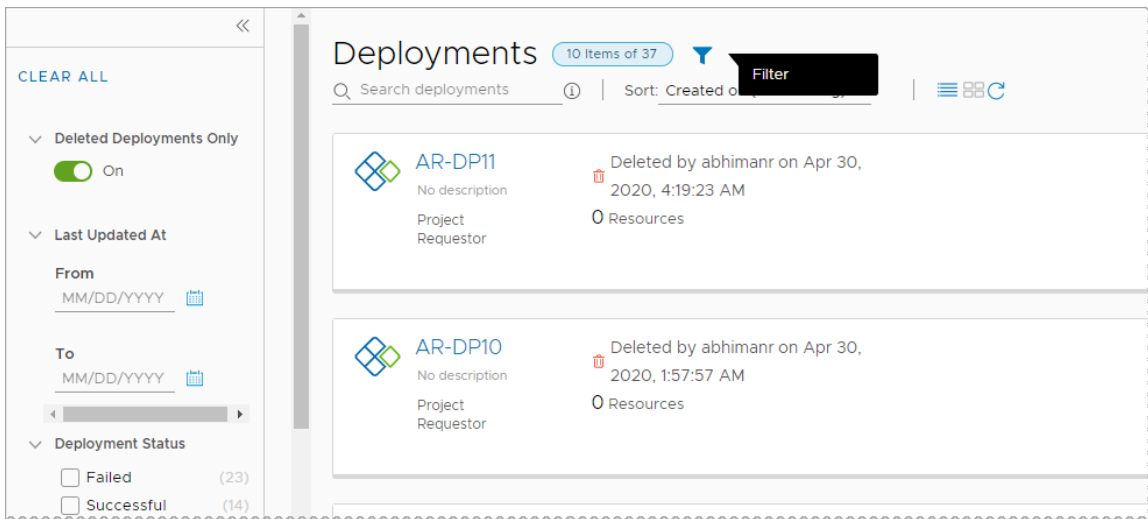
As ações disponíveis dependem do estado da implantação.



- Para exibir as implantações excluídas, clique no filtro na página **Implantações** e ative a alternância **Somente Implantações Excluídas**.

A lista de implantações agora está limitada às que foram excluídas. Talvez seja bom revisar o histórico de uma implantação específica. Por exemplo, para recuperar o nome de uma máquina excluída.

As implantações excluídas são listadas por 90 dias.



Próximo passo

Para saber mais sobre as ações possíveis, consulte [Quais ações posso executar nas implantações do Cloud Assembly](#).

Quais ações posso executar nas implantações do Cloud Assembly

Depois de implantar modelos de nuvem, você pode executar ações no Cloud Assembly para gerenciar os recursos. As ações disponíveis dependem do tipo de recurso e se as ações são suportadas em uma determinada conta de nuvem ou plataforma de integração.

As ações disponíveis também dependem do que o seu administrador autorizou você a executar.

Como administrador ou administrador de projeto, você pode configurar as políticas de Ações de Dia 2 no Service Broker . Consulte [Como conceder direitos para consumidores às políticas de ação de dia 2 do Service Broker](#)

Você também pode ver ações que não estão incluídas na lista. Essas são prováveis ações personalizadas adicionadas pelo administrador. Por exemplo, uma [Como criar uma ação de recurso do Cloud Assembly para aplicar o vMotion a uma máquina virtual](#).

Tabela 7-2. Lista de ações possíveis

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|------------------------------|-------------------------------------|--|---|---|
| Adicionar disco | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Adicione mais discos a máquinas virtuais existentes.</p> <p>Se você adicionar um disco a uma máquina do Azure, esse disco persistente ou não persistente será implantado no grupo de recursos que inclui a máquina.</p> <p>Ao adicionar um disco a uma máquina do Azure, você também pode criptografar esse novo disco usando o conjunto de criptografia de disco do Azure configurado no perfil de armazenamento.</p> <p>Você não pode adicionar um disco a uma máquina do Azure com um disco não gerenciado.</p> <p>Ao adicionar um disco a máquinas vSphere, você pode selecionar o controlador SCSI, cuja ordem foi definida no modelo de nuvem e implantada. Você também pode especificar o número da unidade para o novo disco. Não é possível especificar um número de unidade sem um controlador selecionado. Se você não selecionar um controlador ou fornecer um número de unidade, o novo disco será implantado no primeiro controlador disponível e atribuído em seguida ao próximo número de unidade disponível nesse controlador.</p> <p>"Ao adicionar um disco a uma máquina vSphere para um projeto com limites de armazenamento definidos, o disco adicionado não deverá exceder os limites de armazenamento."</p> <p>Se você usar o VMware Storage DRS (SDRS) e o cluster de repositório de dados estiver configurado no perfil de armazenamento, será possível adicionar discos no SDRS a máquinas vSphere.</p> |
| Aplicar Configuração do Salt | Máquinas | <ul style="list-style-type: none"> ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Instale um subordinado Salt ou atualize a configuração do Salt em uma máquina virtual.</p> <p>A opção Aplicar Configuração do Salt estará disponível se você tiver configurado a integração com o SaltStack Config.</p> <hr/> <p>Observação Antes de usar esse método para instalar o subordinado Salt, existe uma opção mais robusta na qual você inclui o subordinado no modelo de nuvem. O método de modelo inclui um tipo de recurso do SaltStack Config na implantação. Para obter mais informações, consulte Como adicionar o recurso SaltStack Config a modelos.</p> <hr/> <p>Para aplicar uma configuração, você deve selecionar um método de autenticação. A opção Acesso remoto com credenciais existentes usa as credenciais de acesso remoto incluídas na</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|---------------------|--|--|--|---|
| | | | | <p>implantação. Se você tiver alterado as credenciais na máquina após a implantação, a ação poderá falhar. Se você souber as novas credenciais, use o Método de autenticação por senha.</p> <p>A Senha e a Chave privada usam o nome de usuário e a senha ou a chave para validar suas credenciais e, em seguida, conectar-se à máquina virtual via SSH. Se você não fornecer um valor para a ID do Mestre e a ID do Subordinado, o Salt criará os valores para você.</p> |
| Cancelar | <ul style="list-style-type: none"> ■ Implantações ■ Vários tipos de recursos em implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Cancele uma implantação ou uma ação de dia 2 em uma implantação ou um recurso enquanto a solicitação está sendo processada.</p> <p>Você pode cancelar a solicitação no cartão de implantação ou nos detalhes da implantação. Após a cancelamento da solicitação, ela aparecerá como uma solicitação com falha na página Implantações. Use a ação Excluir para liberar todos os recursos implantados e apagar sua lista de implantações.</p> <p>O cancelamento de uma solicitação que você considera estar muito tempo em execução é um método para gerenciar o tempo de implantação. No entanto, é mais eficiente definir o Tempo Limite da Solicitação nos projetos. O tempo limite padrão é de duas horas. Você poderá defini-lo para um período de tempo mais longo se a implantação da carga de trabalho para um projeto exigir mais tempo.</p> |
| Alterar a concessão | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Altere a data e a hora de vencimento da concessão. Quando uma concessão expirar, a implantação será destruída, e os recursos serão recuperados.</p> <p>Políticas de concessão são definidas no Service Broker.</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|----------------------|-------------------------------------|--|--|--|
| Alterar Proprietário | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Altera o proprietário da implantação para o usuário selecionado. O usuário selecionado, como indivíduo ou membro de um grupo, deve ser um administrador ou membro do mesmo projeto que implantou a solicitação.</p> <p>Quando um designer de modelo de nuvem implanta um modelo, esse designer é o solicitante e o proprietário. No entanto, um solicitante pode fazer com que outro membro do projeto seja o proprietário.</p> <p>Você pode usar políticas para controlar o que um proprietário pode fazer com uma implantação, concedendo a ele permissões mais restritivas ou menos restritivas.</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|-----------------|-------------------------------------|---|--|--|
| Alterar Projeto | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ NSX-T ■ NSX-V ■ VMware Cloud Director ■ VMware Cloud Foundation ■ VMware Cloud on AWS ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Use a ação de alteração de projeto para mover uma implantação de um projeto para outro.</p> <p>A ação de alteração de projeto está disponível para implantações com recursos implantados e para implantações com recursos integrados. Essa ação não tem suporte para implantações que contêm recursos simultaneamente integrados e implantados. A ação não está disponível para implantações migradas.</p> <p>Os recursos com suporte incluem os seguintes tipos de recursos e restrições:</p> <ul style="list-style-type: none"> ■ As implantações com recursos implantados podem conter máquinas virtuais, discos, balanceadores de carga, redes, grupos de segurança, grupos do Azure, NATs e gateways. ■ As implantações com recursos integrados podem conter máquinas virtuais, discos e redes. ■ Se você adicionar um tipo de recurso sem suporte a qualquer tipo de implantação, com recursos implantados ou com recursos integrados, não poderá executar a ação de alteração de projeto. Por exemplo, se você adicionar uma configuração do Terraform a uma implantação, a ação de alteração de projeto não estará disponível. <p>Funções, considerações e restrições para implantações com recursos implantados:</p> <ul style="list-style-type: none"> ■ Para alterar o projeto de uma implantação com recursos implantados, o usuário inicial deve ter a seguinte função: <ul style="list-style-type: none"> ■ Administrador de nuvem. ■ Você só pode alterar o projeto quando o projeto de destino contém todas as zonas de nuvem em que as máquinas e os discos da implantação são implantados. A implantação movida fica então sujeita aos limites configurados do projeto de destino, incluindo contagem de instâncias, memória, CPU e armazenamento. Após a movimentação, o uso atual é liberado do projeto de origem. ■ Depois de mover uma implantação ao projeto de destino, ela estará sujeita às políticas do projeto de destino. Por exemplo, concessão, ações de dia 2, cota de recursos e outras políticas. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|------|-------------------------------------|--------------------------------------|-------------------|---|
| | | | | <p>Para mover uma implantação, a concessão de implantação definida pela política de concessão do projeto de destino não pode expirar nas próximas 24 horas.</p> <p>Funções, considerações e restrições para implantações com recursos integrados:</p> <ul style="list-style-type: none"> ■ Para mover uma implantação com recursos integrados, o usuário inicial deve ter pelo menos uma das seguintes funções: <ul style="list-style-type: none"> ■ Administrador de nuvem. ■ Permissão para gerenciar implantações. Essa permissão pode ser definida como uma função personalizada. ■ Administrador do projeto de destino. ■ O membro do projeto de destino e as implantações são compartilhados entre todos os usuários no projeto de destino. ■ Embora seja possível mover recursos integrados para um projeto que não contém as mesmas zonas de nuvem, se o projeto de destino não tiver as mesmas zonas de nuvem, ações futuras de dia 2 envolvendo recursos de região/conta de nuvem que você executar poderão não funcionar. <p>Considerações gerais:</p> <ul style="list-style-type: none"> ■ Se você for um administrador que está movendo a implantação, poderá fazer essa movimentação para um projeto do qual o proprietário não é membro e, portanto, ele perderá o acesso. Você pode adicionar o proprietário ao projeto de destino ou mover a implantação para um projeto do qual ele é membro. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|-------------------------------|-------------------------------------|--------------------------------------|---|--|
| Alterar grupos de segurança | Máquinas | ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Você pode associar e dissociar grupos de segurança com redes de máquina em uma implantação. A ação de alteração se aplica aos grupos de segurança existentes e sob demanda do NSX-V e do NSX-T. Essa ação está disponível apenas para máquinas únicas, não para clusters de máquina.</p> <p>Para associar um grupo de segurança à rede da máquina, o grupo de segurança deve estar presente na implantação.</p> <p>Dissociar um grupo de segurança de todas as redes de todas as máquinas em uma implantação não remove o grupo de segurança da implantação.</p> <p>Essas alterações não afetam os grupos de segurança aplicados como parte dos perfis de rede.</p> <p>Essa ação altera a configuração do grupo de segurança da máquina sem recriar a máquina. Esta é uma alteração não destrutiva.</p> <ul style="list-style-type: none"> ■ Para alterar a configuração do grupo de segurança da máquina, selecione a máquina no painel topologia e, em seguida, clique no menu Ação no painel direito e selecione Alterar grupos de segurança. Agora, você pode adicionar ou remover a associação aos grupos de segurança com as redes de máquina. |
| Conectar-se ao console remoto | Máquinas | ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Descoberto ■ Integração | <p>Abra uma sessão remota na máquina selecionada. Revise os requisitos a seguir para uma conexão bem-sucedida.</p> <ul style="list-style-type: none"> ■ Como consumidor de implantação, certifique-se de que a máquina provisionada esteja ligada. |

Tabela 7-2. Lista de ações possíveis (continuação)

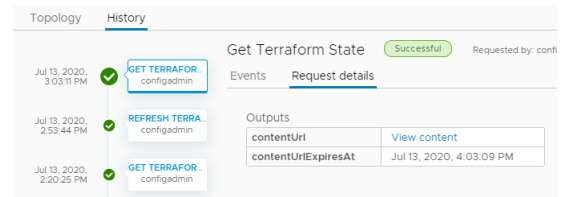
| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|-------------------------|-------------------------------------|--|---|--|
| Criar Snapshot de Disco | Máquinas e discos | <ul style="list-style-type: none"> ■ Microsoft Azure | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Crie um snapshot de um disco de máquina virtual ou um disco de armazenamento.</p> <ul style="list-style-type: none"> ■ Para máquinas, você cria snapshots para discos de máquinas individuais, incluindo o disco de inicialização, discos de imagem e discos de armazenamento. ■ Para discos de armazenamento, você cria snapshots de discos gerenciados independentes, e não de discos não gerenciados. <p>Além de fornecer um nome de snapshot, você também pode fornecer as seguintes informações para o snapshot:</p> <ul style="list-style-type: none"> ■ Snapshot Incremental. Marque a caixa de seleção para criar um snapshot das alterações desde o último snapshot, em vez de um snapshot completo. ■ Grupo de Recursos. Digite o nome do grupo de recursos de destino no qual você deseja criar o snapshot. Por padrão, o snapshot é criado no mesmo grupo de recursos usado pelo disco pai. ■ ID do Conjunto de Criptografia. Selecione a chave de criptografia para o snapshot. Por padrão, o snapshot é criptografado com a mesma chave usada pelo disco pai. ■ Tags. Digite todas as tags que ajudarão você a gerenciar os snapshots no Microsoft Azure. |
| Criar snapshot | Máquinas | <ul style="list-style-type: none"> ■ Google Cloud Platform ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Crie um snapshot da máquina virtual.</p> <p>Se você tiver permissão apenas para dois snapshots no vSphere e esses snapshots já existirem, esse comando não estará disponível até que você exclua um snapshot.</p> |
| Excluir | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Destrói uma implantação.</p> <p>Todos os recursos são excluídos e recuperados.</p> <p>Se uma exclusão falhar, você poderá executar mais uma vez a ação de excluir em uma implantação. Durante a segunda tentativa, é possível selecionar Ignorar Falhas de Exclusão. Se você selecionar essa opção, a implantação será excluída, mas os recursos talvez não sejam recuperados. Você deve verificar os sistemas nos quais a implantação foi provisionada para garantir que todos os recursos sejam removidos. Se não forem, será necessário excluir manualmente os recursos residuais nesses sistemas.</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|--|-------------------------------------|---|---|---|
| | NSX Gateway | <ul style="list-style-type: none"> ■ NSX | <ul style="list-style-type: none"> ■ Implantação ■ Integração | Exclua as regras de encaminhamento de portas NAT de um gateway NSX-T ou NSX-V. |
| | Máquinas e balanceadores de carga | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere ■ VMware NSX | <ul style="list-style-type: none"> ■ Implantação ■ Integração | Remova uma máquina ou balanceador de carga de uma implantação. Essa ação pode resultar em uma implantação inutilizável. |
| | Grupos de segurança | <ul style="list-style-type: none"> ■ NSX-T ■ NSX-V | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Se o grupo de segurança não estiver associado a uma máquina na implantação, o processo o removerá da implantação.</p> <ul style="list-style-type: none"> ■ Se o grupo de segurança for sob demanda, ele será destruído no endpoint. ■ Se o grupo de segurança for compartilhado, a ação falhará. |
| | Clusters Tanzu Kubernetes | <ul style="list-style-type: none"> ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | Remova um cluster Tanzu Kubernetes de uma implantação. |
| Excluir Snapshot de Disco | Máquinas e discos | <ul style="list-style-type: none"> ■ Microsoft Azure | <ul style="list-style-type: none"> ■ Implantação ■ Integração | Exclua um disco da máquina virtual do Azure ou um snapshot de disco gerenciado. Esta ação está disponível quando há pelo menos um snapshot. |
| Excluir instantâneo | Máquinas | <ul style="list-style-type: none"> ■ VMware vSphere ■ Google Cloud Platform | <ul style="list-style-type: none"> ■ Implantação ■ Integração | Exclui um snapshot da máquina virtual. |
| Desativar Diagnóstico de Inicialização | Máquinas | <ul style="list-style-type: none"> ■ Microsoft Azure | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Desative o recurso de depuração de máquina virtual do Azure.</p> <p>A opção Desativar só estará disponível se esse recurso estiver ativado.</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|-------------------------------------|-------------------------------------|--|--|---|
| Editar tags | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Adicione ou modifique tags de recursos que são aplicadas a recursos de implantação individuais. |
| Ativar Diagnóstico de Inicialização | Máquinas | <ul style="list-style-type: none"> ■ Microsoft Azure | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Ative o recurso de depuração de máquina virtual do Azure para diagnosticar falhas de inicialização de máquina virtual. As informações de diagnóstico de inicialização estão disponíveis no console do Azure.</p> <p>A opção Ativar só estará disponível se o recurso não estiver ativado no momento.</p> |
| Obter o estado do Terraform | Configuração do Terraform | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Exiba o arquivo de estado do Terraform.</p> <p>Para visualizar as alterações feitas nas máquinas do Terraform nas plataformas de nuvem em que foram implantadas e atualizar a implantação, primeiro execute a ação Atualizar estado do Terraform e, em seguida, execute a ação Obter o estado do Terraform.</p> <p>Quando o arquivo é exibido em uma caixa de diálogo. O arquivo fica disponível por aproximadamente 1 hora antes que você precise executar uma nova ação de atualização. Você poderá copiá-lo se precisar dele mais tarde.</p> <p>Você também pode visualizar o arquivo na guia Histórico de implantações. Selecione o evento Obter o estado do Terraform na guia Eventos e, em seguida, clique em Detalhes da solicitação. Se o arquivo não tiver expirado, clique em Visualizar conteúdo. Se o arquivo tiver expirado, execute a Atualização e as ações de Obter novamente.</p> |



Você pode executar outra ação de dia 2 nos recursos do Terraform que estão incorporados na configuração. As ações disponíveis dependem do tipo de recurso, da plataforma de nuvem na qual são implantados e se você tem autorização para executar as ações baseadas em uma política de dia 2.

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|---------------|-------------------------------------|--|--|---|
| Desligar | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Descoberto ■ Integrado | Desligue a implantação após a primeira tentativa de desligar os sistemas operacionais convidados. Se o desligamento suave falhar, um desligamento forçado ainda será executado. |
| | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Desligue a máquina após a primeira tentativa de desligar os sistemas operacionais convidados. Se o desligamento suave falhar, o desligamento forçado ainda será executado. |
| Ligar | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Liga a implantação. Se os recursos estavam suspensos, a operação normal será retomada do ponto em que eles foram suspensos. |
| | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Descoberto ■ Integrado | Liga a máquina. Se a máquina estava suspensa, a operação normal será retomada do ponto em que a máquina foi suspensa. |
| Reinicializar | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Reinicia o sistema operacional convidado em uma máquina virtual. Para uma máquina vSphere, o VMware Tools deve ser instalado na máquina para usar esta ação. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|--------------|---|--|---|--|
| Reconfigurar | Balancedores de carga | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware NSX | <ul style="list-style-type: none"> ■ Implementado ■ Integridade | <p>Altere o tamanho do balanceador de carga e seu nível de registro em log.</p> <p>Você também pode adicionar ou remover rotas e alterar o protocolo, a porta, a configuração de integridade e as configurações de pool de membros. Para balanceadores de carga do NSX, você pode ativar ou desativar a verificação de integridade e modificar as opções de integridade. Para o NSX-T, você pode definir a verificação como ativa ou passiva. O NSX-V não oferece suporte a verificações de integridade passivas.</p> |
| | Encaminhamento de portas de gateway NSX | <ul style="list-style-type: none"> ■ NSX-T ■ NSX-V | <ul style="list-style-type: none"> ■ Implementado ■ Integridade | <p>Adicione, edite ou exclua as regras de encaminhamento de portas NAT de um gateway NSX-T ou NSX-V.</p> |
| | Grupos de segurança | <ul style="list-style-type: none"> ■ NSX-T ■ NSX-V ■ VMware Cloud ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implementado ■ Integridade | <p>Adicione, edite ou remova regras de firewall ou restrições com base em se o grupo de segurança é sob demanda ou existente.</p> <ul style="list-style-type: none"> ■ Grupo de segurança sob demanda <p>Adicione, edite ou remova regras de firewall para grupos de segurança sob demanda do NSX-T e do VMware Cloud.</p> <ul style="list-style-type: none"> ■ Para adicionar ou remover uma regra, selecione o grupo de segurança no painel de topologia, clique no menu Ação no painel direito e selecione Reconfigurar. Agora você pode adicionar, editar ou remover as regras. ■ Grupo de segurança existente <p>Adicione, edite ou remova restrições para grupos de segurança existentes do NSX-V, NSX-T e VMware Cloud.</p> <ul style="list-style-type: none"> ■ Para adicionar ou remover uma restrição, selecione o grupo de segurança no painel de topologia, clique no menu Ação no painel direito e selecione Reconfigurar. Agora, você pode adicionar, editar ou remover as restrições. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|---------------------------------|-------------------------------------|--|--|--|
| Atualizar o estado do Terraform | Configuração do Terraform | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Recupere a iteração mais recente do arquivo de estado do Terraform.</p> <p>Para recuperar todas as alterações feitas nas máquinas do Terraform nas plataformas de nuvem em que foram implantadas e atualizar a implantação, primeiro execute a ação Atualizar estado do Terraform.</p> <p>Para exibir o arquivo, execute a ação Obter o estado do Terraform na configuração.</p> <p>Use a guia Histórico de implantações para monitorar o processo de atualização.</p> |
| Remover disco | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Remova discos de máquinas virtuais existentes.</p> <p>Se você executar a ação de dia 2 em uma implantação que é implantada como máquinas e discos vSphere, a contagem de disco será recuperada conforme for aplicada a limites de armazenamento do projeto. Os limites de armazenamento do projeto não se aplicam a discos adicionais que você adicionou após a implantação como uma ação de dia 2.</p> |
| Redefinir | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Força uma máquina virtual a reiniciar sem desligar o sistema operacional convidado. |
| Redimensionar | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ Google Cloud Platform ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Aumenta ou diminui a CPU e a memória de uma máquina virtual. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|--------------------------------------|-------------------------------------|--|---|---|
| Redimensionar disco de inicialização | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Aumente ou diminua o tamanho da mídia do disco de inicialização.</p> <p>Se você executar a ação de dia 2 em uma implantação aplicada como máquinas e discos vSphere e a ação falhar com uma mensagem semelhante a "O armazenamento solicitado é maior que o posicionamento de armazenamento disponível", é provável que isso seja devido aos limites de armazenamento definidos nos seus modelos de VM do vSphere e na biblioteca de conteúdo que definida no projeto. Os limites de armazenamento do projeto não se aplicam a discos adicionais que você adicionou após a implantação como uma ação de dia 2.</p> |
| Redimensionar disco | Disco de armazenamento | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Aumenta o recurso de um disco de armazenamento.</p> <p>Se você executar a ação de dia 2 em uma implantação aplicada como máquinas e discos vSphere e a ação falhar com uma mensagem semelhante a "O armazenamento solicitado é maior que o posicionamento de armazenamento disponível", é provável que isso seja devido aos limites de armazenamento definidos nos seus modelos de VM do vSphere e na biblioteca de conteúdo que definida no projeto. Os limites de armazenamento do projeto não se aplicam a discos adicionais que você adicionou após a implantação como uma ação de dia 2.</p> |
| | Máquinas | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Aumente ou diminua o tamanho dos discos incluídos no modelo de imagem da máquina e de quaisquer discos anexados.</p> |
| Reiniciar | Máquinas | <ul style="list-style-type: none"> ■ Microsoft Azure | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Desliga e reinicia uma máquina em execução.</p> |
| Reverter para snapshot | Máquinas | <ul style="list-style-type: none"> ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integração | <p>Reverte para um snapshot anterior da máquina. É necessário ter um snapshot existente para usar essa ação.</p> |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|-------------------------|-------------------------------------|---|--|---|
| Executar tarefa Puppet | Recursos gerenciados | <ul style="list-style-type: none"> ■ Puppet Enterprise | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Executa a tarefa selecionada nas máquinas da implantação.</p> <p>As tarefas são definidas na sua instância do Puppet. Você deve ser capaz de identificar a tarefa e fornecer os parâmetros de entrada.</p> |
| Escalar Nós de Trabalho | Clusters Tanzu Kubernetes | <ul style="list-style-type: none"> ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Aumente ou diminua o número de máquinas virtuais de nós de trabalhador do Tanzu Kubernetes na sua implantação. |
| Desligar | Máquinas | <ul style="list-style-type: none"> ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação | Desliga o sistema operacional convidado e desligue a máquina. O VMware Tools deve ser instalado na máquina para usar essa ação. |
| Suspender | Máquinas | <ul style="list-style-type: none"> ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Pausa a máquina para que ela não possa ser usada e não consuma outros recursos do sistema além do armazenamento que ela está usando.</p> |
| Atualizar | Implantações | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | <p>Altera a implantação com base nos parâmetros de entrada.</p> <p>Para obter um exemplo, consulte Como mover uma máquina implantada para outra rede.</p> <p>Se a implantação for baseada em recursos do vSphere e a máquina e os discos incluírem a opção de contagem, limites de armazenamento definidos no projeto poderão ser aplicados quando você aumentar a contagem. Se a ação falhar com uma mensagem semelhante a "O armazenamento solicitado é maior que o posicionamento de armazenamento disponível", isso provavelmente é devido aos limites de armazenamento definidos nos seus modelos de VM do vSphere que estão especificados no projeto. Os limites de armazenamento do projeto não se aplicam a discos adicionais que você adicionou após a implantação como uma ação de dia 2.</p> |
| Atualizar tags | Máquinas e discos | <ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere | <ul style="list-style-type: none"> ■ Implantação ■ Integrado | Adicione, modifique ou exclua uma tag aplicada a um recurso individual. |

Tabela 7-2. Lista de ações possíveis (continuação)

| Ação | Aplica-se a estes tipos de recursos | Disponível para estes tipos de nuvem | Origem do recurso | Descrição |
|---------------------------|-------------------------------------|--|---|---|
| Atualizar Versão do Tanzu | Clusters Tanzu Kubernetes | <ul style="list-style-type: none"> VMware vSphere | <ul style="list-style-type: none"> Implantado Integrado | Atualize a versão atual do Kubernetes para uma versão posterior. |
| Cancelar Registro | Máquinas | <ul style="list-style-type: none"> Amazon Web Service Google Cloud Platform Microsoft Azure VMware vSphere | <ul style="list-style-type: none"> Implantado Integrado | <p>A ação de cancelar o registro está disponível apenas para máquinas de implantação integradas. Máquinas não registradas são removidas da implantação, junto com todos os discos anexados. Ao remover os recursos, você pode executar novamente o fluxo de trabalho de integração para a máquina não registrada. Você pode querer integrar o recurso novamente, dessa vez em um novo projeto.</p> <p>Se você fizer qualquer alteração na máquina, por exemplo, adicionar um disco, antes de cancelar o registro da máquina, a ação de cancelar o registro falhará.</p> |

Gerenciando recursos no Cloud Assembly

Como administrador de nuvem ou desenvolvedor de modelos de nuvem do Cloud Assembly, você usa a guia Recursos para gerenciar seus recursos de nuvem. Essa guia funciona como um centro de recursos onde você pode monitorar os recursos nas nuvens, fazer alterações neles e até destruí-los ou excluí-los.

Você pode localizar e gerenciar seus recursos usando diferentes exibições. Você pode filtrar as listas, exibir os detalhes dos recursos e executar ações nos itens individuais. As ações disponíveis dependem do estado do recurso e das políticas de dia 2.

"Se você for administrador do Cloud Assembly, também é possível visualizar e gerenciar máquinas detectadas."

Para exibir seus recursos, selecione **Recursos > Recursos**.

Trabalhando com as listas de recursos

Você pode usar as listas de recursos para gerenciar os seguintes tipos de recursos: máquinas, volumes de armazenamento, redes, balanceadores de carga e grupos de segurança que compõem suas implantações. Na lista de recursos, esses recursos podem ser gerenciados em grupos de tipos de recursos em vez por implantações.

- Todos os Recursos

Inclui todos os recursos descobertos, implantados, migrados e integrados descritos nas seções a seguir.

- Máquinas Virtuais

Máquinas virtuais individuais. As máquinas podem fazer parte de implantações maiores.

- Volumes

Volumes de armazenamento que foram descobertos ou associados a implantações.

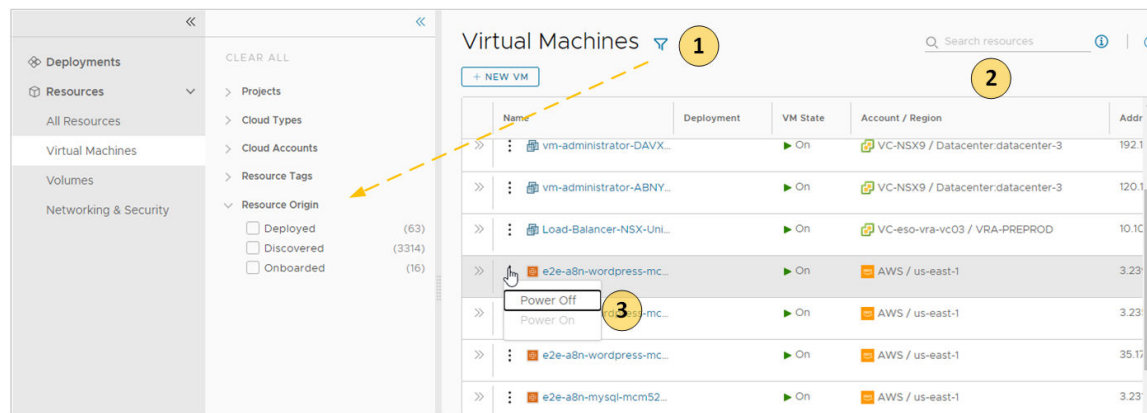
- Rede e segurança

Inclui redes, balanceadores de carga e grupos de segurança.

Semelhante à exibição de lista de implantações, você pode filtrar a lista, selecionar um tipo de recurso, pesquisar, classificar e executar ações.

Se você clicar no nome do recurso, poderá trabalhar com o recurso no contexto dos detalhes do recurso.

Figura 7-3. Lista da página de recursos



1 Filtre sua lista com base em atributos de recursos.

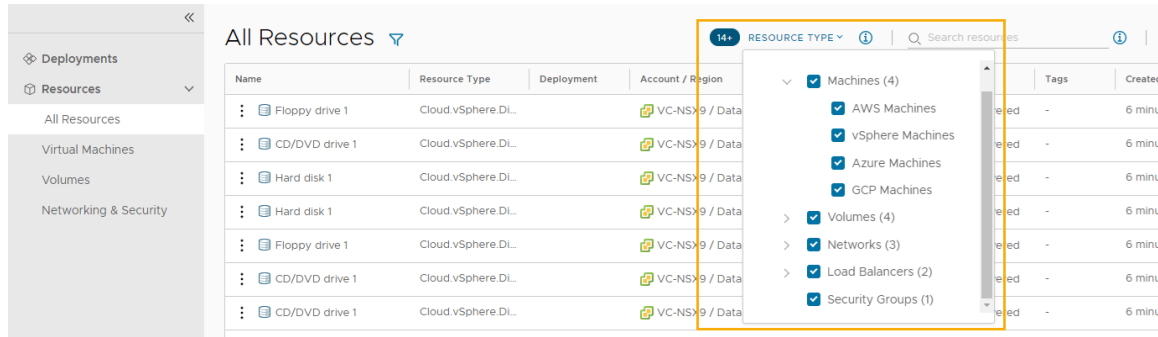
Por exemplo, você pode filtrar com base no projeto, nos tipos de nuvem, na origem ou em outros atributos.

2 Pesquise recursos com base no nome, regiões da conta ou outros valores.

3 Execute as ações de dia 2 disponíveis que são específicas ao tipo de recursos e ao estado do recurso.

Por exemplo, você poderá ligar uma máquina descoberta se ela estiver desligada. Ou você pode redimensionar uma máquina integrada.

Além das opções de pesquisa e filtro em cada página, a página Todos os Recursos inclui um seletor de Tipo de Recurso para você criar um filtro para todos os recursos.



Lista de recursos gerenciados por origem

Você pode usar a guia Recursos para gerenciar os tipos de recursos a seguir.

Tabela 7-3. Origens de recursos

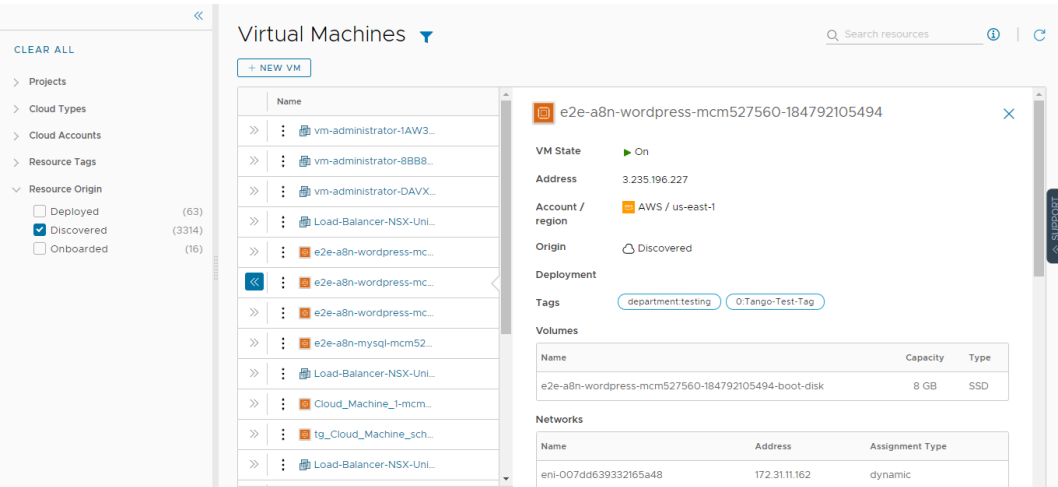
| Recurso gerenciado | Descrição |
|--------------------|--|
| Implantado | As implantações são cargas de trabalho totalmente gerenciadas que são modelos de nuvem implantados ou recursos integrados. Os recursos de carga de trabalho podem incluir máquinas, volumes de armazenamento, redes, balanceadores de carga e grupos de segurança. Você pode gerenciar suas implantações na seção Implantações ou na seção Recursos. |
| Descoberto | Os recursos descobertos são as máquinas, volumes de armazenamento, redes, balanceadores de carga e grupos de segurança que o processo de descoberta identificou para cada região de conta de nuvem que você adicionou. Somente os Administradores do Cloud Assembly podem ver e gerenciar os recursos descobertos na seção Recursos. |
| Migrados | Os recursos migrados são as implantações do 7.x que você migrou para o vRealize Automation. Os recursos migrados podem incluir máquinas, volumes de armazenamento, redes, balanceadores de carga e grupos de segurança. Os recursos migrados são gerenciados como implantações. Você pode gerenciar os recursos migrados na seção Implantações ou na seção Recursos. |
| Integrado | Recursos integrados são recursos descobertos que você coloca em um gerenciamento mais robusto do vRealize Automation. Os recursos integrados são gerenciados como implantações. Você pode gerenciar os recursos integrados na seção Implantações ou na seção Recursos. |

Qual é a exibição de detalhes do recurso

Você pode usar a exibição de detalhes do recurso para obter uma visão mais detalhada do recurso selecionado. Dependendo do recurso, os detalhes podem incluir redes, portas e outras informações coletadas sobre a máquina. A profundidade das informações varia dependendo do tipo de conta de nuvem e da origem.

Para abrir o painel de detalhes, clique no nome do recurso ou nas setas duplas.

Figura 7-4. Painel de detalhes de recursos



Quais ações de dia 2 posso executar nos recursos

As ações de dia 2 disponíveis dependem da origem do recurso, da conta de nuvem, do tipo de recurso e do estado.

Tabela 7-4. Lista de ações por origem

| Origem do Recurso | Ações do dia 2 |
|-------------------|---|
| Implantado | As ações que estão disponíveis para execução nos recursos dependem do tipo de recurso, da conta de nuvem e do estado. Para ver uma lista detalhada, consulte Quais ações posso executar nas implantações do Cloud Assembly . |
| Descoberto | As ações disponíveis para recursos descobertos são limitadas a máquinas virtuais. Dependendo do status, você pode realizar as seguintes ações. <ul style="list-style-type: none">■ Desligar■ Ligar Ação adicional da máquina virtual do vSphere. <ul style="list-style-type: none">■ Conectar-se ao console remoto |

Tabela 7-4. Lista de ações por origem (continuação)

| | |
|-----------|--|
| Migrados | Os recursos migrados têm as mesmas opções de gerenciamento de ação de dia 2 que as implantações. As ações que estão disponíveis para execução nos recursos migrados dependem do tipo de recurso, da conta de nuvem, do status e das políticas do dia 2. Para ver uma lista detalhada, consulte Quais ações posso executar nas implantações do Cloud Assembly . |
| Integrado | Os recursos integrados têm as mesmas opções de gerenciamento de ações de dia 2 que as implantações. As ações que estão disponíveis para execução nos recursos integrados dependem do tipo de recurso, da conta de nuvem e do estado. Para ver uma lista detalhada, consulte Quais ações posso executar nas implantações do Cloud Assembly . |

Como trabalhar com recursos individuais no Cloud Assembly

Como administrador de nuvem ou membro de projeto com recursos para o seu projeto, você pode usar a seção Recursos da guia Recursos para gerenciar seus recursos implantados, integrados e migrados como individuais por tipo.

Esse fluxo de trabalho, que se concentra no gerenciamento de máquinas virtuais, fornece um guia para o gerenciamento do ciclo de vida de recursos de alto nível que você pode aplicar aos outros tipos de recursos.

Localizar recursos de máquina virtual

As máquinas virtuais implantadas, integradas e migradas estão disponíveis na página Todos os Recursos e na página Máquinas Virtuais na guia Recursos. Esse exemplo concentra-se em máquinas virtuais, mas você pode aplicar o mesmo fluxo de trabalho aos outros tipos de recursos.

- 1 Selecione **Recursos > Recursos > Máquinas Virtuais**.
- 2 Localize sua máquina virtual.

Você pode usar os filtros ou a pesquisa para localizar recursos específicos.

| Name | Deployment | VM State | Account / Region | Address | Project | Origin | Tags |
|--------------------------|------------------------------|----------|--|-----------------|-------------------|------------|------|
| vm-administrator-VLDX... | | On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | | | Discovered | - |
| vm-administrator-N6CE... | | On | https://cmbu-w01-vc08.eng.vmware.com / w01-vc08... | 192.167.211.142 | | Discovered | - |
| mcm-20211203215331-0... | Google Cloud Create VM_6f... | On | yingzhi-GCP / us-east1 | 34.74.168.22 | Create VM Proj... | Deployed | - |

Revisar os detalhes da máquina virtual

Os detalhes do recurso fornecem uma visualização rápida das informações da máquina, incluindo redes, propriedades personalizadas e outras informações coletadas.

- 1 Localize a máquina na lista Máquinas Virtuais.

- Clique no nome do recurso ou nas setas duplas na coluna esquerda da tabela.

O painel de detalhes é aberto no lado direito da lista.

The screenshot shows the 'Virtual Machines' section of the vRealize Automation Cloud Assembly interface. On the left, a list of VMs is displayed with columns for Name, Deployment, VM State, Account / Region, Address, Project, Origin, and Tags. The VM 'mcm-20211203215331-0...' is selected. On the right, a detailed view of this VM is shown, including its state (On), address (34.74.168.22), account/region (yingzhi-GCP / us-east1), origin (Deployed), deployment (Google Cloud Create VM_6f6d0315-ddc8-4f5d-9e1e-563c149a836d), tags, volumes (create-vm-new-disk-1-524598563851 and mcm-20211203215331-000020), networks (default), and custom properties (resourceId, zone_overlapping_migrated, project, zone, environmentName, providerId, id).

- Para fechar o painel, clique nas setas duplas ou no nome do recurso.

Executar ações de dia 2 na máquina virtual

Você usa as ações de dia 2 para gerenciar seus recursos. As ações disponíveis dependem do tipo de recurso, do estado do recurso e das políticas de ação de dia 2 aplicadas.

- Localize a máquina na lista Máquinas Virtuais.
- Clique nas reticências verticais para ver as ações disponíveis.
- Clique na ação.

The screenshot shows the 'Virtual Machines' section of the vRealize Automation Cloud Assembly interface. A list of VMs is displayed. The VM 'mcm-20211203215331-0...' is selected. A context menu is open over this VM, showing actions such as Add Disk, Create Snapshot, Delete, Power Off, Resize, Resize Boot Disk, Resize Disk, and Update Tags.

Como trabalhar com o recursos descobertos no Cloud Assembly

Como administrador do Cloud Assembly, use a seção Recursos da guia Recursos para gerenciar suas máquinas descobertas. Somente os administradores podem ver os recursos descobertos nas várias páginas.

Esse fluxo de trabalho concentra-se no gerenciamento de máquinas virtuais descobertas.

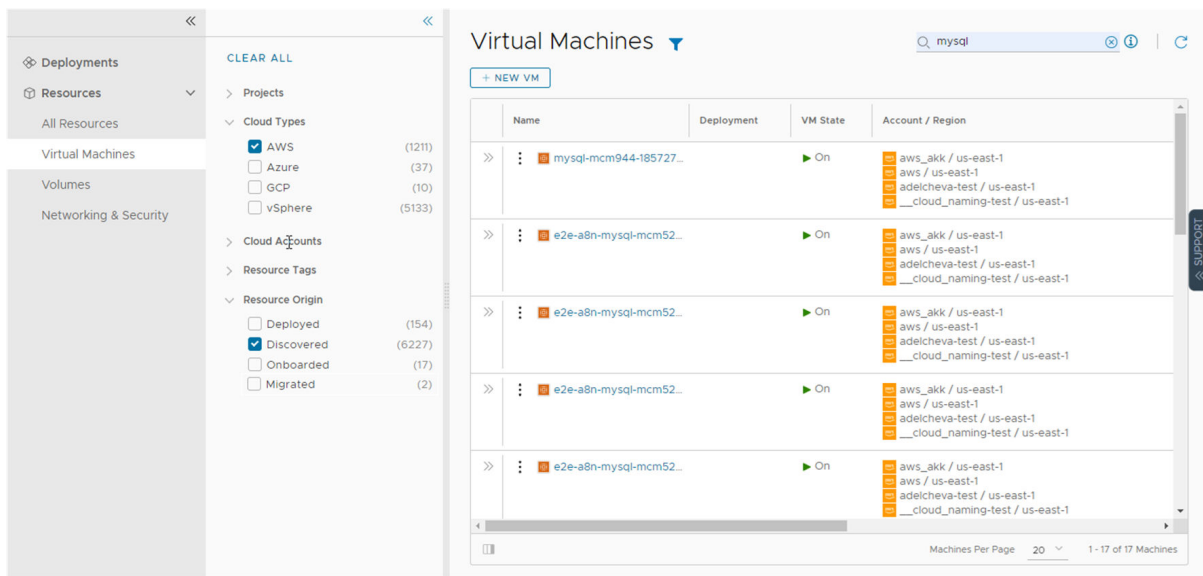
O que fazer primeiro

- Adicione uma conta de nuvem para os recursos que você deseja descobrir. Neste fluxo de trabalho, uma máquina do Amazon Web Services é usada como exemplo. Para adicionar uma conta de nuvem, consulte [Como adicionar contas de nuvem ao Cloud Assembly](#).

Localizar máquinas virtuais descobertas

O recurso descoberto é coletado da região da conta de nuvem e adicionado aos recursos na guia Recurso. Este exemplo concentra-se em máquinas virtuais, mas outros tipos de recursos são coletados, incluindo informações de armazenamento e de rede.

1 Seleccione **Recursos > Recursos > Máquinas Virtuais**.



- 2 Para localizar as máquinas virtuais da AWS, clique no ícone **Filtro** próximo ao rótulo da página
- 3 Na lista de filtros, expanda **Tipos de Nuvem** e selecione **AWS**.

A lista agora está limitada às máquinas virtuais da AWS. Você pode ver tipos implantados, descobertos e outros tipos de origem.

- 4 Na lista de filtros, expanda **Origem do Recurso** e selecione **Descoberto**.

Essa lista agora está limitada às máquinas virtuais da AWS.

- 5 Para localizar uma determinada máquina, você pode usar a opção **Pesquisar recursos** para pesquisar por nome, endereço IP, tags ou valores.

Neste exemplo, **mysql** é o termo de pesquisa.

Revisar detalhes da máquina virtual

Os detalhes do recurso incluem todas as informações coletadas para o recurso. Você pode usar essas informações para compreender o recurso e quaisquer associações com outros recursos.

- 1 Localize a máquina virtual na lista máquina virtual.
- 2 Para exibir os detalhes do recurso, clique no nome da máquina ou clique nas setas duplas na coluna esquerda.

O painel de detalhes é aberto no lado direito da lista.

The screenshot shows the 'Virtual Machines' section of the vRealize Automation Cloud Assembly interface. On the left, a list of virtual machines is displayed with columns for Name, Status, and Actions. The selected VM is 'mysql-mcm1688-174252447070'. The right panel shows the details for this VM, including its state (On), address (44.195.25.253), account/region (aws_akk / us-east-1), origin (cloud_terraform-test / us-east-1), deployment (cloud_naming-test / us-east-1), tags (UserName:fritz, EventTopic:compute.allocation.pre), volumes (mysql-mcm1688-174252447070-boot-disk, 8 GB, SSD), and networks (eni-Oa44e518e9562fdb, 172.31.53.191, dynamic).

| Name | Capacity | Type |
|--------------------------------------|----------|------|
| mysql-mcm1688-174252447070-boot-disk | 8 GB | SSD |

| Name | Address | Assignment Type |
|----------------------|---------------|-----------------|
| eni-Oa44e518e9562fdb | 172.31.53.191 | dynamic |

- 3 Revise os detalhes, incluindo armazenamento, redes, propriedades personalizadas e outras informações coletadas.
- 4 Para fechar o painel, clique nas setas duplas ou clique no nome do recurso.

Executar ações de dia 2 na máquina virtual

Você usa as ações de dia 2 para gerenciar os recursos. As ações atuais de máquinas virtuais descobertas incluem Ligar e Desligar. Se você gerencia uma máquina virtual do vSphere, também poderá executar Conectar-se ao Console Remoto.




- 1 Localize a máquina na lista Máquinas Virtuais.
- 2 Clique nas reticências verticais para ver as ações disponíveis.

As possíveis ações de uma máquina virtual da AWS são Desligar e Ligar. Ligar não está ativo porque a máquina já está ligada.

- 3 Clique em **Desligar** e envie a solicitação.

Virtual Machines mysql

+ NEW VM

| Name | Deployment | VM State | Account / Region | Address | Proje |
|---|------------|----------|---|---------------|-------|
| >>  mysql-mcm944-185727... | | ▶ On | aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1 | 52.87.253.251 | |
| >>  e2e-a8n-mysql-mcm52... | | ▶ On | aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1 | 3.93.34.186 | |
| >>  e2e-a8n-mysql-mcm52... | | ▶ On | aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1 | 44.192.5.36 | |

Power Off — In Progress
(0 / 1 Tasks)

SUPPORT

Quando o processo é concluído, a máquina é desligada. Agora você pode ligá-la novamente.

O que mais posso fazer com a máquina virtual descoberta

Para gerenciar completamente os recursos descobertos, você pode integrá-los. Consulte [O que são planos de integração no Cloud Assembly](#).