

# Guia de instalação, upgrade e gerenciamento do vRealize Suite Lifecycle Manager 8.6

VMware vRealize Suite Lifecycle Manager 8.6



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

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

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

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

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

# Conteúdo

Sobre o Guia de instalação, upgrade e gerenciamento do vRealize Suite Lifecycle Manager 8

## 1 Como instalar o vRealize Suite Lifecycle Manager 9

Requisitos do sistema 9

Portas do vRealize Suite Lifecycle Manager 11

Instalação do VMware vRealize Suite Lifecycle Manager Easy Installer 13

Como executar o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager 14

Como usar o Easy Installer do vRealize Suite Lifecycle Manager para o vRealize Automation e VMware Identity Manager para instalar meus aplicativos 17

Como usar o Easy Installer para o vRealize Automation e o VMware Identity Manager para migrar o vRealize Suite Lifecycle Manager 24

Como executar o vRealize Suite Lifecycle Manager Easy Installer 26

Como faço para usar o Easy Installer para instalar o vRealize Suite Lifecycle Manager 27

Como usar o Easy Installer para migrar o vRealize Suite Lifecycle Manager 28

Fazer login no servidor do vRealize Suite Lifecycle Manager 29

Acessar o dashboard vRealize Suite Lifecycle Manager 30

Notificações no vRealize Suite Lifecycle Manager 30

Configuração do SMTP para notificações de saída por e-mail 31

Criação de webhooks de entrada para canais do Slack e do Teams 32

Configuração de notificações de saída 32

## 2 Configurar o vRealize Suite Lifecycle Manager 34

Configurar as configurações do vRealize Suite Lifecycle Manager 34

Provedor de Autenticação em vRealize Suite Lifecycle Manager 36

Configurar o sistema 36

Configurar Servidores NTP 42

Configurar Servidores DNS 43

Fonte de dados usando configurações SNMP para vRealize Network Insight 43

Substituir certificado para o vRealize Suite Lifecycle Manager 44

Como trabalhar com suporte do produto 45

Configurar certificado no Locker 50

Configurar a licença no Locker 52

Configurar a senha dentro do Locker 53

Gerenciamento de senhas no Locker 53

Adicionar um Centro de dados a vRealize Suite Lifecycle Manager 54

Atribuir uma Função de usuário no vCenter Server 55

vRealize Suite Lifecycle Manager em um ambiente VMware Cloud on AWS 58

Como criar funções para acesso específico	58
Atribuir funções para operações de certificado	58
Gerenciamento de identidade e tenant com o VMware Identity Manager	60
Gerenciar seu diretório no Gerenciamento de Identidade	61
Configurar a definição de atributo do usuário	62
Atribuir funções de usuário com o Gerenciamento de usuário	62
Adicionar o Active Directory sobre LDAP	63
Adicionar o Active Directory com a autenticação integrada do Windows	66
Gerenciamento de tenants no vRealize Suite Lifecycle Manager	69
Como usar a Migração de Tenant	82
<b>3 Criar um ambiente no vRealize Suite Lifecycle Manager</b>	<b>87</b>
Criar um novo ambiente de nuvem privada usando o assistente de instalação	87
Instalar o VMware Identity Manager no vRealize Suite Lifecycle Manager	91
Definir configurações de ambiente para uma nova nuvem privada	92
Instalar os produtos vRealize Suite	93
Aceitar a seleção de EULA e licença	93
Configurar detalhes do certificado	94
Configurar detalhes da infraestrutura	95
Configurar detalhes de rede	97
Configurar os detalhes do produto	98
Configurar produtos do vRealize Suite para instalação	102
Validar detalhes do ambiente de nuvem privada	106
Confirmar as configurações de ambiente e instalação	110
Importar um ambiente existente usando o Assistente de instalação	111
Importar ambiente do VMware Identity Manager	112
Importar ambiente do vRealize Business for Cloud	112
Importar ambiente do vRealize Automation	113
Importar a configuração da pilha de sal autônoma do VMware vRealize	114
Importar ambiente do vRealize Network Insight	115
Importar ambiente do vRealize Operations Manager	116
Importar ambiente do vRealize Log Insight	116
Criar um ambiente de nuvem privada usando um arquivo de configuração	117
Criação de ambientes no vRealize Cloud	118
Definir configurações de ambiente para um novo Cloud Proxy	118
Instalação de produtos Cloud Proxy	119
Configuração de detalhes do produto de proxy de nuvem	120
Integração de assinaturas do vRealize Cloud Universal	121
<b>4 Como gerenciar ambientes no vRealize Suite Lifecycle Manager</b>	<b>122</b>
Operações do Dia 2 para o Ambiente Global no vRealize Suite Lifecycle Manager	122

Redimensionar os recursos de hardware para o VMware Identity Manager	124
Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager	125
Reconfigurar pods internos e sub-redes de serviço	126
Adicionar um produto a um ambiente de nuvem privada existente	127
Adicionar uma Fonte de dados a um Ambiente de nuvem privada existente	127
Operações de dados com suporte pelo vRealize Network Insight	128
Importar fontes de dados para o vRealize Suite Lifecycle Manager	128
Gerenciar uma fonte de dados em um ambiente de nuvem privada já existente	129
Atualizar senhas em massa para a fonte de dados	129
Dimensionar horizontalmente o VMware Identity Manager	130
Verificação de integridade agendada	132
Dimensionar horizontalmente o VMware Identity Manager habilitado para tenant	132
Dimensionar horizontalmente o Conector do Windows	133
Dimensionar horizontalmente produtos do vRealize Suite	134
Dimensionar horizontalmente o vRealize Automation ativado para tenant	136
Expandir verticalmente produtos do vRealize Suite	136
Exportar um arquivo de configuração do ambiente de nuvem privada	138
Download de logs de produtos da nuvem privada	138
Excluir um ambiente	139
Gerenciar produtos vRealize Suite em uma nuvem privada	140
Criação e configuração de um snapshot do produto	141
Sincronização de inventário no vRealize Suite Lifecycle Manager	142
Referências do Produto	143
Alterar sua senha para os produtos vRealize	144
Excluir um produto de um ambiente	145
Adicionar licenças para os produtos do vRealize Suite	147
Configurar o monitoramento de integridade da pilha de gerenciamento do vRealize Suite	148
Status de integridade no vRealize Suite Lifecycle Manager	149
Exibir o dashboard da Visão Geral da Integridade do SDDC no VMware vRealize Operations Manager	150
Ativar ou desativar a verificação de integridade de produtos no vRealize Suite Lifecycle Manager	150
Como adicionar e gerenciar conteúdo do Marketplace	151
Encontrar e baixar conteúdo do Marketplace	151
Exibir e atualizar conteúdo baixado do Marketplace	152
Instalar um conteúdo baixado do Marketplace	153
Excluir conteúdo baixado do Marketplace	154
<b>5 Como gerenciar o ciclo de vida do conteúdo no vRealize Suite Lifecycle Manager</b>	
<b>155</b>	
Como trabalhar com endpoints de conteúdo	157
Adicionar um vRealize Orchestrator endpoint de conteúdo	159

Adicionar um endpoint de conteúdo do vRealize Automation	160
Adicionar um endpoint de nuvem do vRealize Automation	162
Adicionar um endpoint de controle de origem	162
Adicionar um endpoint de conteúdo do vCenter Server	164
Adicionar um endpoint do vRealize Operations Manager	165
Excluir um endpoint de conteúdo	166
Editar um endpoint de conteúdo	167
Gerenciar conteúdo	167
Adicionar conteúdo	169
Excluir diversos conteúdos	171
Trabalhar com conteúdo capturado	171
Ações de conteúdo	172
Tipos de conteúdo disponíveis para os produtos	172
Como pesquisar conteúdo	176
Conteúdo do teste	177
Controle de origem com o gerenciamento do ciclo de vida de conteúdo vRealize Suite Lifecycle Manager	180
Implementar um pacote de conteúdo	186
Pacote de vários lançamentos de conteúdo	186
Excluir um pacote de conteúdo	188
Problemas de conteúdo que podem ser encontrados	189
Controle de origens de acesso	189
Como gerenciar endpoints de servidores de controle de origem	190
Adicionar um endpoint do servidor de controle de origem	190
Excluir um endpoint do servidor de controle de origem	191
Como trabalhar com as configurações de conteúdo	192
Configurar Stub de Pipeline	193
Mapear a configuração do proxy	194
Configurações de pipelines de conteúdo	194
Pipelines de Conteúdo	196

## 6 Como atualizar produtos do vRealize Suite Lifecycle Manager e vRealize Suite 198

Fazer upgrade do vRealize Suite Lifecycle Manager 8.x	198
Suporte para versões adicionais do produto	200
Atualizar o VMware Identity Manager	200
Migrar o conector do Windows	202
Fazer upgrade do vRealize Automation 8.x com o vRealize Suite Lifecycle Manager	203
Funcionalidade de upgrade do vRealize Automation	205
Atualizar um produto do vRealize Suite	207
Atualizar produtos já existentes usando o verificador de pré-atualização	209
Atualizar vRealize Operations Manager	211

Atualizar o vRealize Automation 7.x	212
Atualizar vRealize Network Insight	213
Atualizar vRealize Log Insight	214
Atualizar vRealize Business for Cloud	215
Atualizar a configuração do vRealize Automation Salt Stack	216
<b>7 Executar um plano de recuperação de desastres para o vRealize Suite Lifecycle Manager</b>	<b>217</b>
<b>8 Gerenciamento de licenças do vRealize Cloud no vRealize Suite Lifecycle Manager</b>	<b>219</b>
Gerenciar licenças do vRealize Cloud no Locker	219
Fazendo download do relatório de uso para licenças do vRealize Cloud	221
Ativação de licenças de assinatura do vRealize Cloud Universal	221
Operações do Dia 2 para o vRealize Cloud Universal	222
Operações de Dia 2 para licenças do vRealize Cloud	222
<b>9 Solução de problemas com o vRealize Suite Lifecycle Manager</b>	<b>224</b>
Falha inesperada ao ligar a grande máquina virtual do vRealize Operations Manager devido às limitações de recursos	226
Há falha na implantação do ambiente ou agrupamento em cluster do vRealize Log Insight e no Registro do VMware Identity Manager	226
Alterações no servidor DNS	227
Detalhes de IP incorretos durante a implantação do vRealize Suite Lifecycle Manager	228
Os mapeamentos binários não estão preenchidos	228
A captura de conteúdo falha com o campo seguro	229
Reparar erros usando arquivos de log	229
Falha na captura do blueprint	229
Falha na implantação do perfil do componente	230
Atualizar o nome de host do vRealize Suite Lifecycle Manager	230
Recurso não encontrado no Gerenciamento de Diretórios	231
A UI do vRealize Automation não exibe novas chaves de licença	232
Falha na captura, teste ou liberação de conteúdo do vRealize Orchestrator	232
Estado sem resposta de operações relacionadas a licenças no vRealize Automation 7.6	233
Falha na importação ou sincronização de inventário de produto do vRealize Suite	233
Falha nas operações do Dia 2 do VMware Identity Manager quando a senha raiz expira	234
Ativar rotação de log para logs de pgpool nos arquivos do Postgres agrupado em cluster do VMware Identity Manager	234
Interrupção do cluster do VMware Identity Manager postgres devido à perda de IP delegado	235
Falha na importação do vRealize Automation para o vRealize Suite Lifecycle Manager	236
O vRealize Suite Lifecycle Manager exibe a versão mais antiga após um upgrade	237
Licenças desconectadas como operação do Dia 2 na interface de usuário do Cloud Universal não estão listadas para reconexão	237

# Sobre o Guia de instalação, upgrade e gerenciamento do vRealize Suite Lifecycle Manager

O Guia de instalação e gerenciamento do *vRealize Suite Lifecycle Manager* fornece instruções para instalar o VMware vRealize Suite Lifecycle Manager e usar o vRealize Suite Lifecycle Manager para instalar e gerenciar produtos do vRealize Suite.

## Público-alvo

Essas informações destinam-se a qualquer pessoa que queira usar o vRealize Suite Lifecycle Manager para implantar e gerenciar os produtos do vRealize Suite para monitorar e gerenciar um centro de dados definido por software (SDDC). As informações são escritas para administradores de máquina virtual experientes que estão familiarizados com aplicativos de gerenciamento empresarial e operações de centro de dados.

## Participando do Programa de Aperfeiçoamento da Experiência do Cliente do vRealize Suite Lifecycle Manager

Este produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. O CEIP oferece informações à VMware que a permitem melhorar seus produtos e serviços, corrigir problemas e lhe recomendar como implantar e utilizar nossos produtos da melhor forma.

Os detalhes sobre os dados recolhidos pelo CEIP e os fins para os quais eles são utilizados pela VMware são estabelecidos no Centro de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

Para participar ou sair do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP), consulte [Definir as configurações do ambiente para uma nova nuvem privada](#)

# Como instalar o vRealize Suite Lifecycle Manager

1

O vRealize Suite Lifecycle Manager ajuda a instalar os produtos do vRealize Suite em tempo menor do que na instalação individual dos produtos. Você também pode gerenciar e fazer upgrade de seus produtos vRealize Suite por meio do vRealize Suite Lifecycle Manager.

- [Requisitos do sistema](#)

Os seguintes requisitos de hardware e sistema operacional são necessários para o vRealize Suite Lifecycle Manager.

- [Portas do vRealize Suite Lifecycle Manager](#)

Esta seção fornece uma lista de portas usadas pelo vRealize Suite Lifecycle Manager para a comunicação do produto e da integração.

- [Instalação do VMware vRealize Suite Lifecycle Manager Easy Installer](#)

Você pode usar um dos nossos instaladores para instalar os produtos necessários do vRealize Suite.

- [Fazer login no servidor do vRealize Suite Lifecycle Manager](#)

Faça login na UI do vRealize Suite Lifecycle Manager para criar e gerenciar ambientes de nuvem com o vRealize Suite Lifecycle Manager.

- [Acessar o dashboard vRealize Suite Lifecycle Manager](#)

O vRealize Suite Lifecycle Manager inclui um painel que funciona como um painel único composto por toda a funcionalidade como aplicativo.

- [Notificações no vRealize Suite Lifecycle Manager](#)

Você pode exibir as atualizações disponíveis para os produtos no meio ambiente e a integridade geral do vRealize Suite Lifecycle Manager em Notificações.

## Requisitos do sistema

Os seguintes requisitos de hardware e sistema operacional são necessários para o vRealize Suite Lifecycle Manager.

Requisitos	vRealize Suite Lifecycle Manager
Requisitos mínimos de software	<ul style="list-style-type: none"> <li>■ vCenter Server 6.0</li> <li>■ ESXi versão 6.0</li> </ul>
Requisitos mínimos de hardware	<ul style="list-style-type: none"> <li>■ 6 GB de memória</li> <li>■ 78 GB de armazenamento - Provisão espessa</li> </ul>
Virtual CPU	2

## Produtos do vRealize compatíveis para instalação, dimensionamento horizontal e upgrade do Greenfield

O vRealize Suite Lifecycle Manager é compatível com os seguintes produtos do vRealize Suite:

- vRealize Automation
- vRealize Automation Salt Stack Config: Autônoma
- vRealize Automation Salt Stack Config:- integrado ao vRA
- vRealize Business for Cloud
- vRealize Operations Manager
- vRealize Log Insight
- vRealize Network Insight
- VMware Identity Manager

A [Matriz de interoperabilidade de produto da VMware](#) fornece detalhes sobre as versões de produtos compatíveis e a matriz de compatibilidade do vRealize Suite Lifecycle Manager com os produtos do vRealize Suite.

Para obter mais informações sobre o vRealize Suite, consulte a [Visão geral do vRealize Suite](#). Você pode integrar uma versão de produto do vRealize que oferece suporte à importação no vRealize Suite Lifecycle Manager e, em seguida, pode atualizar o mesmo para versões de produtos compatíveis por meio do vRealize Suite Lifecycle Manager.

## Versões do vRealize compatíveis com produtos importados do vRealize Suite Lifecycle Manager

O vRealize Suite Lifecycle Manager é compatível com as seguintes versões do produto e produtos do vRealize.

Produto	Versões compatíveis
vRealize Automation	7.2, 7.3.0, 7.3.1, 7.4, 7.5.0, 7.6.0, 8.0.0, 8.0.1, 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.4.1, 8.5, 8.5.1 e 8.6.0 O vRealize Automation 8.4.1 é compatível com o vRealize Suite Lifecycle Manager 8.4.1. O vRealize Automation 8.4.2 é compatível com o vRealize Suite Lifecycle Manager 8.4.1 Patch 1. O vRealize Automation 8.5.0 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, Pacote 3 de suporte do produto. O vRealize Automation 8.5.1 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, Pacote 4 de suporte do produto.
vRealize Automation Salt Stack Config: Autônoma	8.4.0, 8.4.1, 8.5, 8.5.1 e 8.6.0 O vRealize Automation Salt Stack Config 8.4.2 é compatível com o vRealize Suite Lifecycle Manager 8.4.1 Patch 1.
vRealize Automation SaltStack Config: vRA-Integrated	O vRealize Automation Salt Stack Config 8.5.0 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, Pacote 3 de suporte do produto. O vRealize Automation 8.5.1 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, Pacote 4 de suporte do produto.
vRealize Business for Cloud	7.2, 7.3.0, 7.3.1, 7.4, 7.5.0 e 7.6.0
vRealize Operations Manager	6.3, 6.4, 6.5.0, 6.6.0, 6.6.1, 6.7.0, 7.0.0, 7.5.0, 8.0.0, 8.0.1, 8.1.0, 8.1.1, 8.2.0, 8.3.0, 8.4.0, 8.5.0 e 8.6.0 O vRealize Operations Manager 8.5.0 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, pacote 2 de suporte do produto.
vRealize Log Insight	4.5.1, 4.6.0, 4.6.1, 4.7.0, 4.7.1, 4.8.0, 8.0.0, 8.1.0, 8.1.1, 8.2.0, 8.3.0, 8.4.0, 8.4.1, 8.5.0, 8.6.0 O vRealize Log Insight 8.4.1 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, pacote 1 de suporte do produto.
VMware Identity Manager	3.3.1 e posterior.
vRealize Network Insight	4.0, 4.1, 4.1.1, 4.2.0, 5.0, 5.1.0, 5.2.0, 5.3.0, 6.0.0, 6.1.0, 6.2.0, 6.3.0 e 6.4.0 O vRealize Network Insight 6.3.0 é compatível com o vRealize Suite Lifecycle Manager 8.4.1, Pacote 2 de suporte do produto.

Para a interoperabilidade de produtos, consulte [Matriz de Interoperabilidade](#). Para obter mais informações sobre o vRealize Suite, consulte [Visão Geral do vRealize Suite](#).

## Navegadores compatíveis

- Google Chrome
- Internet Explorer
- Mozilla Firefox

## Portas do vRealize Suite Lifecycle Manager

Esta seção fornece uma lista de portas usadas pelo vRealize Suite Lifecycle Manager para a comunicação do produto e da integração.

**Tabela 1-1. Portas e endpoints necessários para integração e comunicação com serviços do VMware na nuvem**

Serviço	Porta TCP	URL
My VMware	443	<a href="https://apigw.vmware.com">https://apigw.vmware.com</a>
Nuvem Marketplace	443	<a href="https://gtw.marketplace.cloud.vmware.com">https://gtw.marketplace.cloud.vmware.com</a>
Atualizações	443	<a href="https://vapp-updates.vmware.com">https://vapp-updates.vmware.com</a>
Compatibilidade	443	<a href="https://simservice.vmware.com">https://simservice.vmware.com</a>
Repositório de atualização de patches e políticas	443	<a href="https://vrealize-updates.vmware.com">https://vrealize-updates.vmware.com</a>
VMware Cloud	443	<a href="https://console.cloud.vmware.com">https://console.cloud.vmware.com</a>
API do VMware Cloud	443	<a href="https://api.mgmt.cloud.vmware.com">https://api.mgmt.cloud.vmware.com</a>
Interface de programação de aplicativos de assinaturas	443	<a href="https://vconnect.vmware.com">https://vconnect.vmware.com</a>

Nomes de host da interface de programação de aplicativos do My VMware	Nomes de host da interface de programação de aplicativos do Market Place	URLs de host da interface de programação de aplicativos do Market Place
apigw.vmware.com	marketplace.vmware.com	<a href="https://gtw.marketplace.cloud.vmware.com">https://gtw.marketplace.cloud.vmware.com</a>
download2.vmware.com download3.vmware.com	drd6c1w7be.execute-api.us-west-1.amazonaws.com (*.amazonaws.com)	<ul style="list-style-type: none"> <li>■ <a href="https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com">https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com</a></li> <li>■ <a href="https://cspmarketplaceproductiondownloadable.s3.us-west-2.amazonaws.com">https://cspmarketplaceproductiondownloadable.s3.us-west-2.amazonaws.com</a> e <a href="https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com">https://cspmarketplacemainbuck.s3.us-west-2.amazonaws.com</a></li> </ul>

\*.akamaiedge.net

**Observação**

- vRealize Suite Lifecycle Manager sempre inicia a comunicação para recuperar ou enviar dados para os serviços VMware na nuvem. Você pode configurar sua rede para permitir o tráfego de saída e bloquear o tráfego de entrada para a porta especificada sem afetar os recursos do vRealize Suite Lifecycle Manager que se integram aos serviços VMware na nuvem.
- Certifique-se de que todos os downloads ou URLs do host da interface de programação de aplicativos que são redirecionados do Market Place sejam permitidos.

**Tabela 1-2. Portas necessárias para integração e comunicação com os produtos VMware no local**

Produto ou Integração	Número da Porta TCP
Dispositivo do vRealize Automation	8008, 5480, 443, 22
Nós de servidor IaaS do vRealize Automation	443

**Tabela 1-2. Portas necessárias para integração e comunicação com os produtos VMware no local (continuação)**

Produto ou Integração	Número da Porta TCP
Proxy do vRealize Automation	443
Dispositivos do Servidor/Coletor do vRealize Business for Cloud	5480, 443, 22
Dispositivos de cluster de técnicas de análise do vRealize Operations Manager	443, 22
Dispositivos do coletor remoto do vRealize Operations Manager	443, 22
Dispositivos do vRealize Log Insight	443, 9543, 16520, 22
vRealize Network Insight	443, 22
Dispositivos Identity Manager	8443, 443, 9999, 9898, 9000, 9694 (use-os para um cluster)
Dispositivos do vRealize Orchestrator	<ul style="list-style-type: none"> <li>■ 8281 - somente versão vRealize Orchestrator 7.x.</li> <li>■ 443 - Começando com o vRealize Orchestrator 8.x.</li> </ul>
Instâncias do vCenter Server	443
Instâncias do ESXi Host	443
Host de gerenciamento de conteúdo (GitLab)	443

**Observação** Para o vRealize Suite Lifecycle Manager 8.x e posterior, o protocolo ICMP deve ser habilitado entre o vRealize Suite Lifecycle Manager e os produtos que estão sendo gerenciados.

**Observação** Para obter mais informações sobre portas, consulte o *Guia de reforço de segurança do vRealize Suite Lifecycle Manager 8.x* e a ferramenta Portas e protocolo do [VMware](#).

## Instalação do VMware vRealize Suite Lifecycle Manager Easy Installer

Você pode usar um dos nossos instaladores para instalar os produtos necessários do vRealize Suite.

- **VMware vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager:** este instalador ajuda a instalar o vRealize Suite Lifecycle Manager, o vRealize Automation e o VMware Identity Manager (também conhecido como VMware Workspace ONE Access). O pacote OVA desse pacote contém os binários do vRealize Suite Lifecycle Manager, vRealize Automation e VMware Identity Manager.
- **VMware vRealize Suite Lifecycle Manager Easy Installer:** este instalador ajuda a instalar somente o vRealize Suite Lifecycle Manager. Esse pacote contém o pacote OVA somente do vRealize Suite Lifecycle Manager.

Você pode baixar o arquivo executável de um desses instaladores na página de download do My VMware.

## Como executar o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager

O vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager pode ser baixado na página de downloads My VMware.

### Procedimentos

- 1 Baixe o arquivo executável do vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager na página de downloads My VMware.
- 2 Após baixar o arquivo, monte o arquivo `vra-lcm-installer.iso`.
- 3 Navegue até a pasta `vrlcm-ui-installer` dentro do CD-ROM.
- 4 A pasta contém três subpastas para três sistemas operacionais. Com base no sistema operacional, navegue até a pasta do sistema operacional correspondente na pasta `vrlcm-ui-installer`.
- 5 Clique no arquivo de instalação na pasta.

Sistema operacional	Caminho do arquivo
Windows	<code>lcm-installer\vrlcm-ui-installer\win32</code>
Linux	<ol style="list-style-type: none"> <li>a Faça login na VM do Linux.</li> <li>b Execute <code>apt-get install p7zip-full</code>.</li> <li>c Execute <code>7z x vra-lcm-installer.iso</code>.</li> <li>d Execute <code>chmod +x vrlcm-ui-installer/lin64/installer</code></li> <li>e Execute <code>chmod +x ./vrlcm-ovftool/lin64/ovftool*</code></li> <li>f Execute instalação apta do libnss3 (necessário somente se o componente libnss3 não estiver instalado.)</li> <li>g Execute <code>vrlcm-ui-installer/lin64/installer</code>.</li> </ol>
Mac	<code>vrlcm-ui-installer/mac/Installer</code>

A interface de usuário do vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager é específica para o sistema operacional. Verifique se você está usando o caminho de pasta da IU válido para executar o instalador.

### Resultados

Você não pode instalar seus aplicativos usando o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager.

Se o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager falhar ao ser iniciado e você vir esta mensagem de erro "Ocorreu um problema durante a instalação. Verifique os logs do instalador e tente novamente", será porque:

- Um host foi reinicializado durante a instalação. Selecione o Host para retornar a um estado com integridade.
- O repositório de dados estava 100% cheio durante a instalação. Limpe a memória do repositório de dados e tente iniciar novamente o Easy Installer.
- Não foi possível conectar o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager ao host ESXI. Adicione o vCenter Server de destino e todas as entradas DNS FQDN dos servidores ESXI associados ao cluster ao arquivo do host do sistema: C:\Windows\System32\drivers\etc\hosts. Para Linux e Mac, /etc/hosts.

## Instalar e configurar o vRealize Identity Manager

É possível instalar uma nova instância do vRealize Identity Manager ou importar uma instância existente do ao configurar o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e vRealize Identity Manager.

Se quiser personalizar a configuração do VMware Identity Manager, que pode incluir a implantação do VMware Identity Manager em modo padrão ou de cluster, modo personalizado de rede e armazenamento, poderá ignorar a instalação do VMware Identity Manager. Se tiver ignorado, ainda será solicitado a configurar o VMware Identity Manager na interface do usuário do vRealize Suite Lifecycle Manager. Com o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager, você importa um VMware Identity Manager existente para o vRealize Suite Lifecycle Manager ou é possível implantar uma nova instância do VMware Identity Manager. Para obter mais informações sobre o redimensionamento de hardware para o VMware Identity Manager, consulte [Redimensionamento de hardware](#).

### Pré-requisitos

Verifique se você tem um endereço IP estático antes de iniciar a configuração.

### Procedimentos

- 1 Para instalar uma nova instância, selecione **Instalar novo vIDM**.
- 2 Insira as caixas de texto necessárias sob **Nome da Máquina Virtual**, **Endereço de IP**, **Nome de Host** e **Administração de Configuração Padrão**.

---

**Observação** O vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager cria o usuário administrador de configuração padrão como um usuário local no VMware Identity Manager e o mesmo usuário é utilizado para integrar produtos ao VMware Identity Manager.

---

- 3** Para importar uma instância já existente, selecione **Importar vIDM já existente**.
- Insira o **Nome do Host**, **Senha de administração**, **Senha Administração do Sistema**, **Senha Usuário SSH**, **Senha Raiz**, **Administrador de Configuração Padrão**, e a **Senha de Configuração Padrão**.
  - Selecione a **Sincronização dos membros do grupo para o Diretório quando o usuário quiser sincronizar o membro do grupo** ao adicionar um grupo para a configuração global do VMware Identity Manager.

Com vRealize Easy Installer para vRealize Automation e VMware Identity Manager 8.6	Versão compatível do VMware Identity Manager	Descrição
Nova instalação do vRealize Suite Lifecycle Manager	Somente 3.3.5	
Importar o vRealize Suite Lifecycle Manager	3.3.1, 3.3.2, 3.3.4 ou 3.3.5	
Implantar o vRealize Automation	3.3.2	<b>Observação</b> Se você importar o VMware Identity Manager 3.3.1 e instalar o vRealize Automation 8.2 ou posterior, a instalação falhará.

**Observação** O VMware Identity Manager será compatível se o cenário for um dos seguintes:

- Instância de cluster ou única com banco de dados Postgres incorporado.
- VMware Identity Manager 3.3.2 e 3.3.3 com o tipo determinado de implantação.

**Observação** O VMware Identity Manager não será compatível se o cenário for um dos seguintes:

- Instância de cluster ou única com banco de dados externo (Postgres/MSSQL e assim por diante).
- Instância de cluster ou única com conectores adicionais (conectores Windows e externos) diferentes dos incorporados.
- Versões anteriores do VMware Identity Manager. (3.3.0 e versão anterior)

**Observação** Se a versão mais antiga vRealize Suite Lifecycle Manager não tiver VMware Identity Manager, ela poderá ser instalada ou importada. O ciclo de vida do VMware Identity Manager e as funcionalidades estendidas do Dia 2 não serão compatíveis com o vRealize Suite Lifecycle Manager se o VMware Identity Manager importado não tiver fator forma compatível:

O suporte para upgrade de uma versão mais antiga do VMware Identity Manager (3.3.0 e anteriores) para a mais recente só está disponível se for uma única instância ou um nó do vRealize Identity Manager com banco de dados postgres incorporado.

Caso contrário, você pode fazer upgrade fora do vRealize Suite Lifecycle Manager. Após o upgrade, ele poderá ser importado novamente a qualquer momento acionando a sincronização de inventário no vRealize Suite Lifecycle Manager.

**4 Clique em Avançar.**

Se não puder implantar o vRealize Suite Lifecycle Manager, o VMware Identity Manager ou o vRealize Automation no vCenter Server VMC usando o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager, use o vCenter Server com privilégio de administrador para implantar produtos.

## Como usar o Easy Installer do vRealize Suite Lifecycle Manager para o vRealize Automation e VMware Identity Manager para instalar meus aplicativos

Você pode instalar vRealize Suite Lifecycle Manager, VMware Identity Manager e vRealize Automation usando o Easy Installer do vRealize Suite Lifecycle Manager para o vRealize Automation e o VMware Identity Manager.

### Instalar e configurar produtos

É possível implantar e configurar o vRealize Suite Lifecycle Manager usando o Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation e VMware Identity Manager quando uma implantação for concluída.

O Lifecycle Manager pode ser instalado e configurado usando-se o Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation e VMware Identity Manager. Você pode consultar *Instalação do vRealize Automation usando o Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation e VMware Identity Manager*.

### Pré-requisitos

- Verifique se um vCenter Server está disponível para implantação do Lifecycle Manager e produtos.
- Um IPv4 estático com FQDN preciso é usado para uma implantação do Lifecycle Manager.
- Para evitar portas internas indesejadas externas após a reinicialização do dispositivo virtual do vRealize Suite Lifecycle Manager, faça login no dispositivo virtual do vRealize Suite Lifecycle Manager através do SSH e execute o comando `rm -rf /etc/bootstrap/everyboot.d/10-start-services`, após implantar o dispositivo virtual do vRealize Suite Lifecycle Manager a partir do Easy installer.

## Procedimentos

- 1 Implante o Lifecycle Manager usando o Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation e VMware Identity Manager.

**Observação** Por padrão, você pode encontrar:

- default\_datacenter (nome do centro de dados fornecido no Easy Installer)
- default\_vCenter (nome do vCenter fornecido no Easy Installer)
- Servidores DNS e servidores NTP
- Extensão do disco de dados (tamanho de disco fornecido no Easy Installer)
- ambiente global. (VMware Identity Manager - Com base na seleção do produto)
- ambiente de vRealize Automation de trabalho (com base na seleção do produto)
- Senhas de acesso do VMware Identity Manager e vRealize Automation no locker
- Mapeamento de origem para vRealize Automation e VMware Identity Manager

- 2 Para implantar um novo produto, depois de fazer login no vRealize Suite Lifecycle Manager, clique em **Lifecycle Operations** no **Dashboard - Meus Serviços**.
- 3 Clique no **Datacenter** e navegue até **ADICIONAR DATACENTER**.
- 4 Adicione um **vCenter Server** ao Centro de Dados.
- 5 Crie um certificado válido no **Locker** do vRealize Suite Lifecycle Manager.
- 6 Adicione as chaves de licença necessárias para utilização futura no Locker do vRealize Suite Lifecycle Manager.
- 7 Aumente o espaço em disco do dispositivo do Lifecycle Manager para acomodar binários de produtos e outros componentes necessários a serem usados no futuro.
- 8 (Opcional) Defina as configurações de proxy no Lifecycle Manager para uma conectividade de rede interna.

## Instalando o vRealize Suite Lifecycle Manager com o Easy Installer para o vRealize Automation e o VMware Identity Manager

Você pode instalar o vRealize Suite Lifecycle Manager usando o Easy Installer no vRealize Suite Lifecycle Manager para o vRealize Automation e o VMware Identity Manager.



Assista ao vRealize Suite Lifecycle Manager vídeo Instalação com o Easy Installer.

## Pré-requisitos

Você deve atender a estes pré-requisitos antes de poder instalar o vRealize Suite Lifecycle Manager:

- Certifique-se de ter um vCenter Server configurado e acesso às credenciais.

- Certifique-se de que você tenha os detalhes de configuração de rede do vRealize Automation
- Certifique-se de conhecer os detalhes de implantação do Lifecycle VA

#### Procedimentos

- 1 Clique em **Instalar** na janela **vRealize Easy Installer**.
- 2 Clique em **Avançar** após ler a introdução.
- 3 Aceite o Contrato de Licença e clique em **Avançar**. Leia o **Programa de aperfeiçoamento da experiência do cliente** e marque a caixa de seleção para participar do programa.
- 4 Para especificar os detalhes do vCenter Server, insira esses detalhes na guia Destino de Implantação do Dispositivo.
  - a Insira o **Nome do Host do vCenter Server**.
  - b Insira o número da **Porta HTTPs**.
  - c Digite o **Nome de usuário do vCenter Server** e a **Senha**.
- 5 Clique em **Avançar** e você será solicitado a solicitar um Aviso de Certificado, clique em **Aceitar** para prosseguir.
- 6 Você deve especificar uma localização para implantar dispositivos virtuais.
  - a Expanda a árvore do vCenter Server.
  - b Expanda para qualquer centro de dados e mapeie a sua implantação para uma pasta de VM específica.
- 7 Especifique um cluster de recursos na guia Selecionar um Recurso de Processamento.
  - a Expanda a árvore do centro de dados para uma localização de recurso apropriada e clique em **Avançar**.
- 8 Na guia Selecionar um Local de Armazenamento, selecione um repositório de dados para armazenar a implantação e clique em **Avançar**.
- 9 Nas guias Configuração de Rede e Configuração de Senha, configure a **Rede** e a **Configuração da senha** inserindo os campos necessários e clicando em **Avançar**.
  - a Para uma VM do vRealize Suite Lifecycle Manager, insira o **Servidor NTP** para o dispositivo e clique em **Avançar**.

As configurações de rede fornecidas para todos os produtos são uma entrada única para suas definições de configuração. A senha fornecida também é comum para todos os produtos e você não precisa inserir a senha novamente durante a instalação dos produtos.

A senha deve ter no mínimo uma maiúscula, uma minúscula, um número e um caractere especial. Os caracteres especiais podem ser !@#\$%^&\*(). Dois pontos (:) não é suportado na senha para vRealize Automation 8.0 e 8.0.1.

- 10 Configurar as definições de configuração do vRealize Suite Lifecycle Manager,
- a Insira um **Nome da Máquina Virtual, Endereço de IP, e Nome de Host**.
  - b Forneça informações de configuração. Insira nos campos **Nome do Centro de Dados, Nome do vCenter e Aumentar o Espaço em Disco**.
  - c Ative ou desative a **Conformidade do modo FIPS**, conforme necessário.
  - d Clique em **Avançar**.

#### Próximo passo

Agora você pode começar a instalação do vRealize Identity Manager.

### Instalar o VMware Identity Manager

Você pode instalar uma nova instância do VMware Identity Manager ou importar uma instância existente do quando está configurando o vRealize Suite Lifecycle Manager Easy Installer para o vRealize Automation e o VMware Identity Manager.

#### Observação

- Sem instalar ou importar um VMware Identity Manager, você não pode acessar nenhum outro ambiente do vRealize Suite Lifecycle Manager.
- Se você for instalar o vRealize Automation, certifique-se de implantar o VMware Identity Manager com o tamanho recomendado para o vRealize Automation.
- Consulte o [vRealize Suite Lifecycle Manager Easy Installer para o vRealize Automation](#) e a [documentação do VMware Identity Manager](#) para os requisitos de software e hardware para implantar o VMware Identity Manager.

#### Pré-requisitos

- Verifique se você tem um endereço IP estático e os detalhes do Active Directory antes de iniciar a configuração.
- Verifique se um平衡ador de carga externo está instalado com um certificado válido e se os requisitos foram atendidos. Para obter informações específicas de balanceamento de carga para o VMware Identity Manager, consulte a documentação do [Balanceamento de carga do VMware Identity Manager](#).

#### Procedimentos

- 1 Para instalar uma nova instância , selecione o **Instalar vIDM**.
  - a Insira as caixas de texto necessárias sob **Nome da Máquina Virtual, Endereço de IP, Nome de Host e Administração de Configuração Padrão**.

- 2 Para importar uma instância existente, selecione **Importar vIDM já Existente**.
  - a Digite o **Nome do host**, a **Senha de administrador**, a **Senha de administrador do sistema**, a **senha de usuário do SSH**, **Senha raiz**, o **Administrador da configuração padrão** e a **Senha do Administrador da configuração padrão**.

**Observação** Esse é um usuário local que você cria no tenant padrão no VMware Identity Manager e fornece o acesso de administrador no tenant padrão. O mesmo usuário é usado para toda integração de produto do VMware Identity Manager e a função de administrador é atribuída no produto correspondente. Por exemplo, quando o vRealize Automation 8.x está sendo registrado no VMware Identity Manager, esse usuário de configuração padrão torna-se o administrador da organização e recebe as funções apropriadas. Depois que o vRealize Automation 8.x for implantado, o usuário de configuração será o usuário inicial de quem fez o login. Com outros produtos, quando integrados ao VMware Identity Manager, o mesmo usuário recebe uma função de administrador do produto. Mais um caso de uso de SSO em que o administrador de configuração padrão tem acesso a todos os produtos implantados.

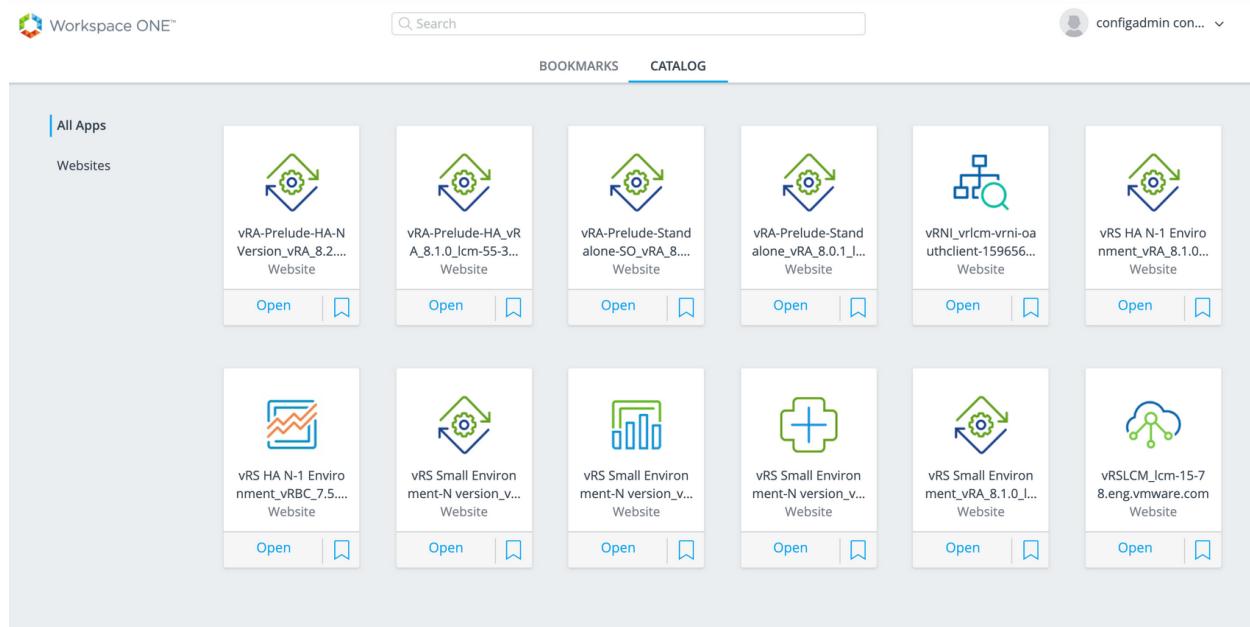
- 3 Clique em **Avançar**.

### Aplicativos de catálogo para produtos vRealize Suite

Você pode implantar um aplicativo de catálogo para acessar produtos vRealize Suite, que são gerenciados no VMware Workspace ONE Access (anteriormente chamado de VMware Identity Manager).

Ao instalar os produtos vRealize Suite no , o integrará o produto desejado ao (opcional) para VMware vRealize Suite Lifecycle Manager criar um aplicativo de catálogo no VMware Workspace ONE Access VMware Identity Manager. Com um single sign-on no VMware Workspace ONE Access, exiba a lista de catálogos que são criados para os produtos vRealize Suite . Você pode optar por abrir qualquer produto do catálogo com o recurso de single sign-on do catálogo .

Os vRealize Suite com suporte para o uso de aplicativos de catálogo são vRealize Automation, vRealize Log Insight, vRealize Network Insight, vRealize Operations Manager, vRealize Business for Cloud e vRealize Suite Lifecycle Manager.



### Observação

- vRealize Automation Ao instalar um único nó vRealize Automation versão 8.x, o aplicativo de catálogo o direcionará para o nome do host primário .
- Ao instalar um vRealize Automation agrupado em cluster versão 8.x, o aplicativo de catálogo o direcionará para o nome do host do vRealize Automation nome do host Balanceador de carga.
- Ao dimensionar horizontalmente um único nó vRealize Automation 8.x para uma configuração de agrupamento em cluster, o aplicativo de catálogo direciona você para o nome de host do Balanceador de Carga do vRealize Automation adicionado recentemente.

### Instalar e configurar o vRealize Automation usando o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager

O Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation VMware Identity Manager oferece uma funcionalidade para instalar o vRealize Automation com etapas mínimas.

O instalador fornece opções mínimas ou uma implantação em cluster antes de iniciar a configuração do vRealize Automation. Não há suporte para instalação manual de componentes OVA ou ISO do vRealize Automation.

**Observação** Agora, o nó mestre é chamado de nó primário. O nó de réplica mestre agora é chamado de nó de réplica primário.

### Pré-requisitos

- Verifique se você tem as credenciais primárias do vRealize Automation antes de instalar o vRealize Automation. O vRealize Automation 8.4 requer um VMware Identity Manager externo 3.3.2 ou posterior.

- Verifique se um平衡ador de carga externo está instalado e se os requisitos foram atendidos. Para obter mais informações, consulte [Balanceamento de carga do vRealize Automation](#).

## Procedimentos

- 1 Digite o **Nome do Ambiente** do vRealize Automation.
  - 2 Na licença do vRealize Automation, digite a chave de licença.
  - 3 Depois de definir as configurações do VMware Identity Manager, você pode optar por instalar o vRealize Automation.
  - 4 Para uma implantação padrão com um nó primário, execute as seguintes etapas.
    - a Digite o **Nome da Máquina Virtual**, o **Endereço IP** e o **Nome do Host FQDN** do vRealize Automation.
    - b Forneça informações de configuração. Insira nos campos **Nome do Centro de Dados**, **Nome do vCenter** e **Aumentar o Espaço em Disco**. Para obter mais informações, consulte o [Easy Installer do vRealize Suite Lifecycle Manager para vRealize Automation e VMware Identity Manager](#).
    - c Ative ou desative a **Conformidade do Modo FIPS**, conforme necessário.
    - d Pule para a Etapa 6.
  - 5 Para uma implantação de cluster com três nós, digite o **endereço IP do balanceador de carga** e o **nome do host**.
  - 6 Para uma implantação de cluster, crie um nó primário usando a etapa 4 como orientação.
  - 7 Para uma implantação de cluster, crie nós secundários, insira as caixas de texto necessárias e continue.
  - 8 Em Configuração Avançada do vRealize Automation, você pode escolher a opção **Usar Padrão** para ativar os valores padrão para pods internos e configuração de serviços no formato CIDR ou usar a opção **Usar Personalizado** para inserir os valores para o Intervalo de IP do Cluster K8S e Intervalo de IP do Serviço K8S no formato CIDR.
  - 9 Clique em **Avançar**.
  - 10 Leia a página Resumo com os dados inseridos e clique em **Enviar**.
- Depois de enviar os detalhes, o instalador leva cerca de 30 minutos para instalar o Lifecycle Manager, copiar binários e iniciar o processo de instalação. Você pode ativar o recurso vários tenants para o vRealize Automation, consulte [Gerenciamento de tenants no vRealize Suite Lifecycle Manager](#).

## Como usar o Easy Installer para o vRealize Automation e o VMware Identity Manager para migrar o vRealize Suite Lifecycle Manager

Este tópico discute como Easy Installer do vRealize Suite Lifecycle Manager para o vRealize Automation e o VMware Identity Manager ajuda a migrar as versões mais antigas do vRealize Suite Lifecycle Manager para as versões mais recentes.

### Como migrar a versão 2.x para o vRealize Suite Lifecycle Manager 8.x

É possível migrar as versões anteriores do Lifecycle Manager para as versões mais recentes.

Você pode migrar o vRealize Suite Lifecycle Manager 2.1 para a versão 8.x ou posterior. A migração também requer entradas, como nome de host, o nome de usuário, a senha e senha SSH do vRealize Suite Lifecycle Manager legado. Para obter mais informações, assista ao vídeo Migração do vRealize Suite Lifecycle Manager com o Easy Installer:



Migração do vRealize Suite Lifecycle Manager com o Easy Installer  
([https://vmwaretv.vmware.com/media/t/1\\_couul29d](https://vmwaretv.vmware.com/media/t/1_couul29d))

#### Pré-requisitos

- Verifique se você tem o vRealize Suite Lifecycle Manager versão 2.1 ou posterior.
- O vRealize Suite Lifecycle Manager legado deve ter o SSH habilitado para o usuário raiz.

#### Procedimentos

- 1 No assistente **Easy Installer**, clique em **Migrar**.
- 2 Insira os detalhes do vCenter no qual o novo vRealize Suite Lifecycle Manager 8.x está instalado.
- 3 Selecione o centro de dados no **vCenter Server**, o **Recurso de cálculo** e o **Armazenamento**.
- 4 Digite os detalhes de configuração de rede.
- 5 Em **Configuração da senha**, insira a senha que pode ser definida como a senha de administração e raiz do vRealize Suite Lifecycle Manager.
- 6 Se quiser implantar o Identity Manager, insira a senha para **admin**, **sshuser** e **credencial raiz**.
- 7 Insira o **Nome da VM**, o **Nome do host** e os **Detalhes de IP** do vRealize Suite Lifecycle Manager 8.x.
- 8 Insira o **Nome do host**, o **Nome do usuário** e a **Senha** do vRealize Suite Lifecycle Manager legado.

**9 Selecione Nova Instalação do Identity Manager ou Importar Identity Manager já Existente.**

Se você optou por instalar o Novo Identity Manager, ele será implantado no mesmo vCenter Server mencionado na etapa 2. Se você importar um Identity Manager existente, verifique se ele já está registrado na VM legada do vRealize Suite Lifecycle Manager e se o SSH do Identity Manager está habilitado para o usuário raiz.

---

**Observação** Uma nova instalação do vRealize Suite Lifecycle Manager 8.x apenas oferece suporte ao VMware Identity Manager 3.3.4. As versões anteriores do VMware Identity Manager terão suporte somente para uma instância do vRealize Suite Lifecycle Manager existente que esteja sendo migrada para o vRealize Suite Lifecycle Manager 8.x e versão posterior. O suporte para upgrade de uma versão anterior do VMware Identity Manager para a mais recente apenas estará disponível se estiver em conformidade com os critérios compatíveis do vRealize Suite Lifecycle Manager. As versões anteriores do vRealize Suite Lifecycle Manager 8.x permitem que apenas uma instância do VMware Identity Manager seja implementada com o conector e o banco de dados postgresql incorporados. O upgrade do VMware Identity Manager dentro do vRealize Suite Lifecycle Manager 8.x para as versões mais recentes terá suporte se estiver em conformidade com os critérios mencionados. Caso contrário, o upgrade deverá ser feito fora do vRealize Suite Lifecycle Manager. Após a atualização, uma reimpressão pode ser feita a qualquer momento acionando a Sincronização de Inventário no vRealize Suite Lifecycle Manager 8.x.

---

**10 Clique em Enviar.**

- 11 Quando a migração for concluída com êxito, clique no URL do vRealize Suite Lifecycle Manager ou na solicitação de migração para exibir o progresso, fazendo login no `admin@local` com a senha fornecida na etapa 5.**
- 12 Todos os ambientes com centros de dados, vCenter Servers, Configurações (como NTP, DNS e assim por diante), endpoints de conteúdo que são gerenciados Lifecycle Manager mais antigos são migrados e os ambientes são importados para a versão mais recente.**

### Resultados

Como parte da migração, crie um ambiente global com base na instalação ou importação ao importar o vRealize Suite Lifecycle Manager VMware Identity Manager legado para o vRealize Suite Lifecycle Manager 8.x. Se houver uma falha no ambiente global, ela pode ser devido à senha de usuário SSH ausente no vRealize Suite Lifecycle Manager legado. Insira os detalhes da senha SSH selecionando a senha correta ao tentar novamente e envie as alterações para criar um ambiente global. Depois que um ambiente global for criado, você poderá retomar a operação de migração.

Com a migração, você pode criar ambientes, configurações, certificados e assim por diante. É possível verificar o status da migração em Status da solicitação.

---

**Observação** Se você importar um VMware Identity Manager existente e a senha do administrador for diferente do usuário SSH para o VMware Identity Manager, a solicitação de ambiente global falhará. Nesse caso, adicione a senha SSH no aplicativo Locker manualmente e repita a solicitação com essa senha.

---

## Como executar o vRealize Suite Lifecycle Manager Easy Installer

Você pode baixar o arquivo executável na página de download do My VMware.

### Procedimentos

- 1 Baixe o arquivo executável do Easy Installer do vRealize Suite Lifecycle Manager na página de download do My VMware.
- 2 Após baixar o arquivo, monte o arquivo lcm-installer.iso.
- 3 Navegue até a pasta vrlcm-ui-installer do CD-ROM.
- 4 A pasta contém três subpastas para três sistemas operacionais. Com base no sistema operacional, navegue até a pasta do sistema operacional correspondente na pasta vrlcm-ui-installer.
- 5 Clique no arquivo de instalação na pasta.

Sistema Operacional	Caminho do arquivo
Windows	lcm-installer\vrlcm-ui-installer\win32
Linux	<ol style="list-style-type: none"> <li>a Faça login na VM do Linux.</li> <li>b Execute apt-get install p7zip-full.</li> <li>c Execute 7z x vra-lcm-installer.iso.</li> <li>d Execute chmod +x vrlcm-ui-installer/lin64/installer</li> <li>e Execute instalação apta do libnss3 (necessário somente se o componente libnss3 não estiver instalado.)</li> <li>f Execute vrlcm-ui-installer/lin64/installer.</li> </ol>
Mac	vrlcm-ui-installer/mac/Installer

- 6 A UI do Easy Installer do vRealize Suite Lifecycle Manager é específica para o sistema operacional. Verifique se você está usando o caminho de pasta da IU válido para executar o instalador.

### Resultados

Agora você pode instalar o vRealize Suite Lifecycle Manager usando o Easy Installer do vRealize Suite Lifecycle Manager.

## Como faço para usar o Easy Installer para instalar o vRealize Suite Lifecycle Manager

Você pode instalar o vRealize Suite Lifecycle Manager usando o Easy Installer do vRealize Suite Lifecycle Manager.

### Pré-requisitos

- Certifique-se de ter um vCenter Server configurado e acesso às credenciais.
- Certifique-se de conhecer os detalhes de implantação do Lifecycle VA.

### Procedimentos

- 1 Clique em **Instalar** na janela do Easy Installer do vRealize Suite Lifecycle Manager.
- 2 Clique em **Avançar** após ler a introdução.
- 3 Aceite o contrato de licença de usuário final e clique em Avançar. Leia o Programa de aperfeiçoamento da experiência do cliente e marque a caixa de seleção para ingressar no programa.
- 4 Para especificar os detalhes do vCenter Server, insira esses detalhes na guia Destino de Implantação do Dispositivo.
  - a Insira o **Nome do Host do vCenter Server**.
  - b Digite o **número da porta HTTPs**.
  - c Digite o **nome de usuário** e a **senha do vCenter Server**.
- 5 Clique em **Avançar** e você será solicitado a solicitar um Aviso de Certificado, clique em **Aceitar** para prosseguir.
- 6 Você deve especificar um local de armazenamento para implementar dispositivos virtuais.
  - a Expanda a árvore do vCenter Server.
  - b Expanda para qualquer centro de dados e mapeie a sua implantação para uma pasta de VM específica.
- 7 Especifique um cluster de recursos na guia Selecionar um Recurso de Processamento.
  - a Expanda a árvore do centro de dados para uma localização de recurso apropriada e clique em **Avançar**.
- 8 Na guia Selecionar um Local de Armazenamento, selecione um repositório de dados para armazenar a implantação e clique em **Avançar**.
- 9 Nas guias Configuração de rede e Configuração de senha, defina a configuração de rede e senha inserindo os campos obrigatórios e clicando em **Avançar**.
  - a Para uma VM do vRealize Suite Lifecycle Manager, digite o **servidor NTP** do dispositivo e clique em **Avançar**.

As configurações de rede fornecidas para todos os produtos são uma entrada única para suas definições de configuração. A senha fornecida também é comum para todos os produtos e você não precisa inserir a senha novamente durante a instalação dos produtos.

A senha deve ter no mínimo uma maiúscula, uma minúscula, um número e um caractere especial. Os caracteres especiais podem ser !@#\$%^&\*(). Dois pontos(:) não são aceitos na senha.

#### 10 Defina as configurações do vRealize Suite Lifecycle Manager.

- a Insira um **Nome da Máquina Virtual, Endereço de IP, e Nome de Host**.
- b Forneça informações de configuração. Preencha os campos **Nome do Centro de Dados, Nome do vCenter e Aumentar o Espaço em Disco**.
- c Ative ou desative a conformidade do modo FIPS, conforme necessário.
- d Clique em **Avançar**.
- e Verifique os detalhes na página Resumo e clique em **Enviar**.

## Como usar o Easy Installer para migrar o vRealize Suite Lifecycle Manager

Você pode usar o vRealize Suite Lifecycle Manager Easy Installer para migrar de versões mais antigas do vRealize Suite Lifecycle Manager.

### Pré-requisitos

- Verifique se você tem o vRealize Suite Lifecycle Manager versão 2.1 ou posterior.
- O vRealize Suite Lifecycle Manager legado deve ter o SSH habilitado para o usuário raiz.

### Procedimentos

- 1 No vRealize Suite Lifecycle Manager Easy Installer, clique em **Migrar**.
- 2 Digite os detalhes do vCenter em que o novo vRealize Suite Lifecycle Manager 8.4 está instalado.
- 3 Selecione o centro de dados no **vCenter Server, o Recurso de cálculo e o Armazenamento**.
- 4 Digite os detalhes de configuração de rede.
- 5 Em **configuração de senha** digite a senha que pode ser definida como a senha da raiz e administrador do vRealize Suite Lifecycle Manager.
- 6 Digite o **Nome da VM, Nome do host** e os **Detalhes do IP** do vRealize Suite Lifecycle Manager.
- 7 Digite o nome do **Nome do host, Nome de usuário e Senha** do vRealize Suite Lifecycle Manager legado.
- 8 Clique em **Enviar**.

- 9 Quando a migração for bem-sucedida, clique na URL do vRealize Suite Lifecycle Manager ou na solicitação de migração para exibir o progresso fazendo login com **admin@local** com a senha fornecida na etapa 5.
- 10 Todos os ambientes com centros de dados, vCenter Servers, Configurações (como NTP, DNS e assim por diante), endpoints de conteúdo que são gerenciados Lifecycle Manager mais antigos são migrados e os ambientes são importados para a versão mais recente.

**Observação** Durante a migração, instalação ou importação, o VMware Identity Manager é opcional. Selecione a barra de alternância **Ignorar a instalação do VMware Identity Manager e importar para onde o VMware Identity Manager integrado ao vRLCM legado não seria importado** para ativar essa opção.

## Fazer login no servidor do vRealize Suite Lifecycle Manager

Faça login na UI do vRealize Suite Lifecycle Manager para criar e gerenciar ambientes de nuvem com o vRealize Suite Lifecycle Manager.

### Pré-requisitos

Implante o dispositivo do vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 Use um navegador Web compatível (Chrome, IE ou Mozilla FireFox) para se conectar ao dispositivo do vRealize Suite Lifecycle Manager usando o endereço IP ou o nome do host do dispositivo.

**https://endereço IP/vrlcm**

**Observação** Você também pode acessar o vRealize Suite Lifecycle Manager usando a URL **https://endereço IP**. A URL **http://endereço IP** não é redirecionada com êxito para o vRealize Suite Lifecycle Manager.

- 2 Digite o nome de usuário do administrador

**admin@local**

- 3 Digite a senha de administrador padrão.

A senha do administrador será a senha padrão fornecida no Easy Installer durante a implantação vRealize Suite Lifecycle Manager.

- 4 Clique em **Fazer Login**.

### Próximo passo

Se você estiver fazendo login no vRealize Suite Lifecycle Manager pela primeira vez, defina a senha do vRealize Suite Lifecycle Manager **root**. Se você quiser redefinir a senha, vá para a guia **Configurações** para fazer a alteração.

Defina uma nova senha de administrador e outras configurações do vRealize Suite Lifecycle Manager, como as configurações de SSH.

## Acessar o dashboard vRealize Suite Lifecycle Manager

O vRealize Suite Lifecycle Manager inclui um painel que funciona como um painel único composto por toda a funcionalidade como aplicativo.

O dashboard é composto pelos aplicativos:

### **Lifecycle Operations**

Use este aplicativo no dashboard para acessar o vRealize Suite Lifecycle Manager para gerenciar as operações do Dia 0 ao Dia N dos vRealize Suite Produtos, incluindo o vRealize Network Insight.

### **Locker**

Use esse aplicativo para gerenciar certificados, licenças e senhas. Você pode criar e importar certificados, incluindo o CSR. Você também pode validar antes de aplicar ou substituir os certificados.

### **Gerenciamento de Identidade e Tenants**

Você pode gerenciar diretórios e tenants ativos e atribuir funções a usuários ou grupos.

### **Gerenciamento de conteúdo**

Você pode usar este aplicativo para acessar o ciclo de vida de conteúdo no vRealize Suite Lifecycle Manager para gerenciar o conteúdo do centro de dados definido por software (SDDC), incluindo captura, teste e liberação para vários ambientes e recursos de controle de origem por meio da integração do GitLab ou do bit bucket. Você pode capturar vários conteúdos de um controle de origem e verificar-lhos em outro controle de origem ou em uma ramificação diferente.

### **Marketplace**

Use o vRealize Suite Lifecycle Manager para adicionar e gerenciar conteúdo a partir do Marketplace.

### **vRealize Cloud**

Você pode usar este aplicativo para gerenciar suas assinaturas e proxies do Cloud.

## **Notificações no vRealize Suite Lifecycle Manager**

Você pode exibir as atualizações disponíveis para os produtos no meio ambiente e a integridade geral do vRealize Suite Lifecycle Manager em Notificações.

Os seguintes tipos de notificação estão disponíveis no vRealize Suite Lifecycle Manager:

- Integridade da licença

- Integridade do certificado
- Upgrade do produto
- Patch do produto
- Upgrade automático do vRealize Suite Lifecycle Manager
- Patch automático do vRealize Suite Lifecycle Manager
- Pacote de suporte do produto do vRealize Suite Lifecycle Manager
- Notificações do VCF
- Notificações de integridade para produtos do vRealize Suite
- Notificação de integridade do Identity Manager

Para exibir notificações, navegue até **Página Inicial** e clique no ícone de **Sino**. Para listar todas as notificações, clique no ícone de lista **Exibir** no canto direito da janela **Notificação**.

---

**Observação** O vRealize Suite Lifecycle Manager deve estar conectado à Internet para receber notificações da origem online.

---

## Configuração do SMTP para notificações de saída por e-mail

O servidor SMTP é necessário para enviar e-mails. Portanto, você deve configurar o servidor SMTP antes de configurar as notificações de saída.

### Procedimentos

- 1 Navegue até **Configurações** pelo dashboard Operações de ciclo de vida.
- 2 Selecione **SMTP** em Servidor e Contas.
- 3 Digite o ID de e-mail do remetente em Detalhes de configuração do SMTP.
- 4 Digite o **Nome do host SMTP/Endereço IP** e, em seguida, selecione **Criptografia** na lista.
- 5 Selecione o **Número da porta SMTP**.
- 6 Se selecionar o botão de alternância **Requer autenticação**, você deverá fornecer os detalhes da autenticação. Selecione o sinal de mais (+) ou o símbolo de chave para adicionar os detalhes da senha.
- 7 Selecione uma opção nas Credenciais SMTP disponíveis.
- 8 Clique em **Salvar**.
- 9 Após a configuração bem-sucedida do SMTP, clique em **ENVIAR E-MAIL DE TESTE** para validar se o servidor SMTP configurado está correto. Digite seu ID de e-mail para começar a receber notificações por e-mail.

### Próximo passo

Você pode configurar as notificações de saída por e-mail.

## Criação de webhooks de entrada para canais do Slack e do Teams

Ao criar um webhook de entrada, você recebe uma URL exclusiva. Você deve adicionar essa URL exclusiva na página Notificações de saída para receber alertas e notificações de saída.

### Procedimentos

- 1 Para criar um webhook de entrada no Teams, vá para o canal no qual deseja adicionar o webhook e selecione as reticências (...) em **Mais opções**.
- 2 Clique em **Conectores** no menu suspenso.
- 3 Procure o webhook de entrada e selecione **Adicionar**.
- 4 Selecione **Configurar** e forneça um nome. Você também pode carregar uma imagem para o webhook, se necessário.
- 5 Uma URL exclusiva que mapeia ao canal é gerada. Copie e salve a URL do webhook e clique em **Concluído**.
- 6 Para criar um webhook de entrada no Slack, crie seu aplicativo Slack e, em seguida, selecione o recurso **Webhooks de entrada**.
- 7 Selecione o botão de alternância **Ativar webhooks de entrada**.
- 8 Clique em **Adicionar novo webhook ao espaço de trabalho** e clique em **Autorizar**.
- 9 Uma URL de webhook exclusiva para uso é gerada.

## Configuração de notificações de saída

As notificações de saída foram introduzidas para ajudar você a configurar os canais de ID de e-mail, Slack e Teams. Após configurar Notificações de saída, você deve começar a receber notificações em seu ID de e-mail registrado ou integrações compatíveis com o Slack e o Teams. Você também pode visualizar o status de integridade dos produtos do vRealize Suite e detalhes da licença. As notificações de saída são críticas ou consolidadas. Você receberá alertas instantâneos para notificações críticas. Você pode optar por alertas diários, semanais ou mensais para notificações consolidadas. Notificações consolidadas fornecem uma lista de atualizações críticas, moderadas e outras relevantes.

### Pré-requisitos

- Certifique-se de que o servidor SMTP esteja configurado antes de configurar as notificações de saída por e-mail.
- Crie webhooks de entrada para os canais do Slack e do Teams.

### Procedimentos

- 1 Navegue até **Configurações** pelo dashboard Operações de ciclo de vida.
- 2 Selecione **Notificações de saída** em Administração do sistema.
- 3 Digite o **Nome de integração** e selecione **Frequência**.

- 4 Digite a URL dos **Webhooks** criada para os canais do Slack e do Teams e digite os IDs de e-mail do destinatário.
- 5 Marque as caixas de seleção aplicáveis para Gatilhos de notificação.
- 6 Clique em **Salvar**.

# Configurar o vRealize Suite Lifecycle Manager

2

Depois de instalar vRealize Suite Lifecycle Manager, você pode realizar determinadas tarefas pós-instalação, como definir as configurações, licenças e senhas na UI do vRealize Suite Lifecycle Manager.

Este capítulo inclui os seguintes tópicos:

- Configurar as configurações do vRealize Suite Lifecycle Manager
- Configurar certificado no Locker
- Configurar a licença no Locker
- Configurar a senha dentro do Locker
- Adicionar um Centro de dados a vRealize Suite Lifecycle Manager
- Como criar funções para acesso específico
- Gerenciamento de identidade e tenant com o VMware Identity Manager

## Configurar as configurações do vRealize Suite Lifecycle Manager

Você pode acessar Lifecycle Operations no dashboard Meu Serviço. Você pode modificar as configurações do sistema para o vRealize Suite Lifecycle Manager, como senhas e configurações de SSH em Lifecycle Operations.

Na primeira vez que visualizar a página de configurações, deverá fornecer dados para todas as configurações disponíveis para salvar qualquer configuração. Apenas um administrador de usuário tem acesso aos Aplicativos de Administrador do Sistema. A página de configurações do contém os seguintes aplicativos.

Administração do sistema	Servidores e Contas
Detalhes do sistema	Servidores NTP
Registros	SNMP
Patches do sistema	DNS
Pacote de suporte de produtos	My VMware

Administração do sistema	Servidores e Contas
Upgrade do sistema	Mapeamento Binário
Configurações de horário	SMTP
Alteração de Senha	
Proxy	
Alteração de certificado	
Provedor de autenticação	
Notificações de Saída	

**Observação** Agora, o valor de tempo limite de inatividade da sessão de UI é configurável. Se você estiver inativo por um determinado período, poderá selecionar o tempo máximo em minutos antes de fazer o logout da sessão.

- [Provedor de Autenticação em vRealize Suite Lifecycle Manager](#)

Você pode exibir os detalhes do provedor de autenticação na guia **Configurações** do vRealize Suite Lifecycle Manager.

- [Configurar o sistema](#)

Configure seu sistema após a instalação do dispositivo do vRealize Suite Lifecycle Manager.

- [Configurar Servidores NTP](#)

Adicione os servidores NTP em vRealize Suite Lifecycle Manager para que eles possam ser referenciados durante a implantação vRealize Suite produtos. Os servidores NTP adicionados ao vRealize Suite Lifecycle Manager podem ser usados para definir o sistema que está com o vRealize Suite Lifecycle Manager. Os servidores NTP também podem ser usados como entrada para o esquema de implantação do produto vRealize Suite.

- [Configurar Servidores DNS](#)

Configure seus servidores DNS para configurar o dispositivo do vRealize Suite Lifecycle Manager para resolver os nomes de host e IPs do servidor de nome de domínio.

- [Fonte de dados usando configurações SNMP para vRealize Network Insight](#)

O vRealize Suite Lifecycle Manager dá suporte ao vRealize Network Insight. O vRealize Network Insight consiste em fontes de dados, que são reconhecidas pelo dispositivo vRealize Suite Lifecycle Manager usuário.

- [Substituir certificado para o vRealize Suite Lifecycle Manager](#)

Se você usar o certificado personalizado para o vRealize Suite Lifecycle Manager em vez do certificado padrão autoassinado, substituirá o certificado do vRealize Suite Lifecycle Manager.

- [Como trabalhar com suporte do produto](#)

Depois de configurar as informações de sistema do vRealize Suite Lifecycle Manager, você pode verificar e aplicar atualizações ou patches que estão disponíveis em seu ambiente já existente.

## Provedor de Autenticação em vRealize Suite Lifecycle Manager

Você pode exibir os detalhes do provedor de autenticação na guia **Configurações** do vRealize Suite Lifecycle Manager.

A seção Informações do provedor de autenticação exibe o tipo do provedor de autenticação existente, o endpoint do provedor de autenticação, o FQDN registrado do aplicativo, o ID de cliente e o nome do aplicativo de catálogo.

A seção Ação do provedor de autenticação oferece recursos para sincronizar e registrar novamente. Quando você altera ou atualiza o nome do host ou FQDN do vRealize Suite Lifecycle Manager, o provedor de autenticação deve sincronizar com o nome do host. O botão de **Sincronizar** garante que o nome do host atual ou FQDN do vRealize Suite Lifecycle Manager seja sincronizado com o VMware Identity Manager. Após a sincronização, você poderá verificar a URL de destino e o URI de redirecionamento na guia **Catálogo** do VMware Identity Manager.

O botão **REGISTRAR NOVAMENTE** permite registrar novamente o vRealize Suite Lifecycle Manager com o VMware Identity Manager ao criar novos clientes e aplicativos de catálogo OAuth. A ação de registrar novamente ocorre quando VMware Identity Manager está presente no globalenvironment do vRealize Suite Lifecycle Manager.

Ao atualizar o vRealize Suite Lifecycle Manager 8.1 e versões anteriores, a ID do aplicativo de catálogo para atualizar o aplicativo de catálogo existente não é salva e, portanto, é criado um aplicativo de catálogo duplicado. O novo nome do host e a ID do aplicativo de catálogo são salvos no inventário, que é usado para as operações subsequentes.

## Configurar o sistema

Configure seu sistema após a instalação do dispositivo do vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 No dashboard My Services dashboard, clique em **Operações de ciclo de vida** e, em seguida, clique em **Configurações**.
  - 2 Para aumentar o espaço em disco para o vRealize Suite Lifecycle Manager, navegue até **Detalhes do sistema**, clique em **Aumentar armazenamento**.
    - a Digite o **nome do host do vCenter**, o **Nome do usuário** e a **Senha** pela primeira vez.
    - b Digite o Tamanho do Disco em GB e clique em **Aumentar**.
- Não é possível editar os campos de Informações da Rede.

- 3 Para reiniciar o servidor, clique em **Reiniciar o sistema**.
  - a Para agendar uma reinicialização semanal do servidor, alterne o **Programar uma reinicialização** e selecione o dia da semana e o horário para a reinicialização semanal.
- 4 Clique em **Salvar**.

## Ativar ou desativar o SSH no vRealize Suite Lifecycle Manager

Você pode ativar o SSH para fins de solução de problemas.

Como melhor prática, desative o SSH em um ambiente de produção e ative-o somente para resolver problemas que não podem ser resolvidos por outros meios. Deixe-o ativado somente quando for necessário para uma finalidade específica e em conformidade com as políticas de segurança da sua organização. Se o gerenciamento de conteúdo estiver ativado, o SSH será ativado automaticamente e não poderá ser desativado. Forçar a desativação do SSH causa falha na funcionalidade de Gerenciamento do Ciclo de Vida do Conteúdo.

### Procedimentos

- 1 No dashboard do vRealize Suite Lifecycle Manager, clique em Lifecycle Operations e **Configurações**.
- 2 Clique em **Detalhes do sistema**, em Informações de Rede, digite o Nome do **Host**, o Endereço IP **o**, Tipo de Endereço IP, a **Máscara de rede** e os **campos de Gateway**.
- 3 Digite o **DNS preferencial** e o **DNS alternativo**.

**Observação** O SSH é ativado por padrão.

- 4 Clique em **SALVAR**.

## Trabalhar com os logs do vRealize Suite Lifecycle Manager

É possível configurar os arquivos de log do vRealize Suite Lifecycle Manager e baixar os arquivos de log para solução de problemas. Os logs do vRealize Suite Lifecycle Manager são inseridos em `vmware_vrlcm.log` e `/blackstone-spring.log`

### Gerar Pacote de Log no vRealize Suite Lifecycle Manager

Você pode configurar o nível de informações do vRealize Suite Lifecycle Manager coleta nos arquivos de log e o número de arquivos de log para o vRealize Suite Lifecycle Manager.

Na interface de usuário do vRealize Suite Lifecycle Manager, execute as seguintes etapas.

- 1 Selecione **Operações de Ciclo de Vida**, selecione **Configurações** e navegue até **Administração do Sistema > Logs**.
- 2 Para criar um pacote de log do vRealize Suite Lifecycle Manager, clique em **GERAR PACOTE DE LOG**.
- 3 Para baixar os logs, clique em **BAIXAR OS LOGS**.

Na interface de linha de comando, execute as seguintes etapas.

- 1 Conecte o Secure Shell (SSH) ao vRealize Suite Lifecycle Manager VA usando credenciais raiz.
- 2 Crie um diretório de pacote de log do vRealize Suite Lifecycle Manager usando o comando  
`mkdir -p /data/lcm-logbundle`.
- 3 Gere um diretório de pacote de log do vRealize Suite Lifecycle Manager usando o comando  
`/var/lib/vlcm-common/vlcm-support -w /data/lcm-logbundle`.
- 4 Baixe `/data/lcm-logbundle/<file-name>` com cópia segura.

### Configurar o agente do Log Insight

O vRealize Suite Lifecycle Manager 8.0.0 e posteriores oferece suporte para vRealize Log Insight análise do log. O pacote de conteúdo no vRealize Log Insight para vRealize Suite Lifecycle Manager é compatível com a versão 8.0.1 (Patch 1) e posteriores. O agente do vRealize Log Insight é pré-instalado no dispositivo virtual do vRealize Suite Lifecycle Manager. Você pode configurar o dispositivo do vRealize Suite Lifecycle Manager para encaminhar `cfapi` logs e eventos do sistema para a instância do vRealize Log Insight. Para usar os painéis e widgets do pacote de conteúdo do vRealize Suite Lifecycle Manager, a configuração deve ser feita somente em `cfapi`.

#### Pré-requisitos

Verifique se você já tem os detalhes do servidor do vRealize Log Insight antes de definir as propriedades do agente do Log Insight.

## Procedimentos

- 1 Faça login no dispositivo virtual do vRealize Suite Lifecycle Manager.
  - a Abra um navegador da Web, acesse <https://vRSLCMIP/vrlcm> e faça login com suas credenciais de usuário.
  - b Clique em Lifecycle Operations e, na **Página inicial**, clique em **Configurações de > Logs > em Configuração do agente do Log Insight**.
  - c Atualize os seguintes parâmetros na seção da IU do vRealize Suite Lifecycle Manager e salve suas alterações.

```
[server]
hostname= vRealize Log Insight hostname proto=cfapi port=9000 SSL=no
```

Quando o servidor do vRealize Log Insight não estiver configurado para aceitar uma conexão SSL, a ativação do SSL para agentes do Log Insight no vRealize Suite Lifecycle Manager é opcional.

Ou

```
hostname=vRealize Log Insight hostname proto=cfapi port=9543 SSL=yes
```

Quando o servidor do vRealize Log Insight estiver configurado para aceitar uma conexão SSL, os agentes do Log Insight devem ser configurados para usar a conexão SSL no vRealize Suite Lifecycle Manager.

Ou

```
hostname=vRealize Log Insight hostname proto=syslog port=514
SSL Server Certificates
```

Defina as regras de como o cliente do Log Insight lida com a validação do certificado do servidor do Log Insight. Os certificados recebidos pelo agente do Log Insight são armazenados localmente na máquina do host do agente.

```
Accept Any
Accept Any Trusted
Common Name: (Self-signed server certificate is accepted if its Common Name matches
this value)
Certificates acceptance rules:
```

**Observação** Os agentes do Log Insight que receberem um novo certificado autoassinado com a mesma chave pública do certificado autoassinado existente armazenado localmente aceitarão o novo certificado. Por exemplo, um certificado autoassinado pode ser gerado novamente com uma chave privada já existente, mas com uma nova data de expiração.

Se o agente tiver um certificado autoassinado armazenado localmente e receber um certificado assinado pela CA válido, o agente aceitará silenciosamente o certificado assinado pela CA.

Os agentes que possuem um certificado assinado pela CA rejeitarão certificados autoassinados. O agente aceita certificados autoassinados somente quando ele se conecta inicialmente ao servidor do Log Insight.

Se um agente com um certificado assinado pela CA localmente receber um certificado válido assinado por outra CA confiável, ele será rejeitado por padrão. Você pode selecionar Aceitar Qualquer um Confiável para aceitar o certificado.

---

Tempo de reconexão: 30 min (tempo em minutos para forçar a reconexão com o servidor. Esta opção atenua os problemas causados pelas conexões TCP de longa duração).

Tamanho máximo do buffer: 200 (limite máximo de uso do armazenamento local (dados+logs) em MBs. Intervalo válido: 100-2.000 MB. Padrão: 200 MB).

- 2 Configure o grupo de agentes do Linux na IU de administração do Log Insight.
  - a Abra um navegador da Web e vá para <https://vRealize Log Insight hostname/IP>.
  - b Faça login com as credenciais - **Nome de usuário** como administrador e **Senha** como `vrl1_admin_password`.
  - c Clique no ícone do menu suspenso Configuração e selecione **Administração**.

---

**Observação** O pacote de conteúdo não vem pré-instalado no vRealize Log Insight. Você deve instalar o pacote baixando-o do Marketplace e, em seguida, configurar os agentes.

- d Em **Gerenciamento**, clique em **Agentes**.
- e No menu suspenso na parte superior, selecione **vRealize Lifecycle Management 8.0.1** na seção **Modelos disponíveis**.
- f Clique em **Copiar modelo**.
- g Após copiar o modelo, forneça Ipv4 ou FQDN do vRealize Suite Lifecycle Manager e salve a configuração.
- h Quando a configuração for concluída, os vRealize Suite Lifecycle Manager eventos ou logs do começam a fluir no vRealize Log Insight e os widgets relevantes exibem os dados.

## Configuração de horário no vRealize Suite Lifecycle Manager

Você pode definir as configurações de horário e adicionar o servidor NTP ou usar um tempo de host para o vRealize Suite Lifecycle Manager.

- 1 Para alterar as configurações de horário, navegue até o painel Meus serviços, clique em **Operações de Ciclo de Vida** e clique em **Configurações**.
- 2 Clique em **Configurações de Horário**.
- 3 Para o Modo de Sincronização de Horário Aplicável, selecione **Usar Servidor de Horário (NTP)** ou **Usar Horário do Host**.
  - a Para adicionar um servidor, clique em **Adicionar Novo Servidor** e insira o nome e o endereço FQDN do servidor.
  - b Para editar, clique no ícone Editar na lista de servidores NTP. Não é possível editar o FQDN/Endereço IP, é possível editar somente o nome do servidor NTP.

Para obter mais informações sobre o servidor NTP, consulte [Configurar Servidores NTP](#).

## Supporte ao Federal Information Processing Standard 140-2

FIPS 140-2 é um padrão dos governos dos EUA e Canadense que especifica requisitos de segurança para módulos criptográficos. O VMware vRealize Suite Lifecycle Manager versão 8.2 e posteriores são compatíveis com o Federal Information Processing Standard (FIPS) 140-2.

A conformidade com o FIPS é um modo de opt-in novo e seguro a ser aderente às iniciativas de Prontidão corporativa (Enterprise Readiness Initiatives – ERI) no vRealize Suite Lifecycle Manager da VMware. Para saber mais sobre o suporte ao FIPS 140- 2 nos produtos da VMware, consulte [Políticas de segurança e certificações do FIPS](#).

### Ativar ou desativar a conformidade do modo FIPS no vRealize Suite Lifecycle Manager

Você pode ativar a conformidade do modo FIPS usando o Easy Installer durante a instalação do vRealize Suite Lifecycle Manager ou selecionando a opção como uma operação de Dia 2 na página de Configurações. Para saber mais sobre a conformidade do modo FIPS usando o Easy Installer, consulte a *Documentação do vRealize Automation*.

### Procedimentos

- 1 No dashboard Meu Serviço, selecione Lifecycle Operations e, em seguida, selecione a página de Configurações.
- 2 Em Administração do Sistema, clique em **Detalhes do Sistema**.

- 3 Ative ou desative a caixa de seleção Conformidade do modo FIPS, conforme necessário. Clique em **Atualizar**. O vRealize Suite Lifecycle Manager é reiniciado quando você ativa ou desativa a conformidade do modo FIPS.

**Observação** Quando você ativa a Conformidade do modo FIPS, o vRealize Suite Lifecycle Manager não faz o upgrade para a próxima versão. Você deve desativar a Conformidade do modo FIPS, fazer o upgrade do vRealize Suite Lifecycle Manager e, em seguida, reabilitar a Conformidade do modo FIPS.

## Configurar Servidores NTP

Adicione os servidores NTP em vRealize Suite Lifecycle Manager para que eles possam ser referenciados durante a implantação vRealize Suite produtos. Os servidores NTP adicionados ao vRealize Suite Lifecycle Manager podem ser usados para definir o sistema que está com o vRealize Suite Lifecycle Manager. Os servidores NTP também podem ser usados como entrada para o esquema de implantação do produto vRealize Suite.

### Pré-requisitos

Verifique se os servidores NTP estão funcionando.

### Procedimentos

- 1 No dashboard Lifecycle Operations, navegue até **Configurar > servidores NTP**.
- 2 Para adicionar um servidor NTP, clique em **Adicionar Servidor NTP**.
- 3 Digite um **Nome** e **FQDN/Endereço IP** válido do servidor NTP.
- 4 Clique em **Adicionar**.

**Observação** A partir do vRealize Suite Lifecycle Manager 8.2, os servidores NTP podem ser definidos para o vRealize Automation 8.2 e versões mais recentes.

## Definir configurações de NTP após a implantação

vRealize Suite Lifecycle Manager no momento não permite ajustar as configurações de NTP para o dispositivo virtual durante a implantação do OVA. Esta seção abrange informações sobre sincronização precisa de horário com a infraestrutura e os produtos do conjunto que ela implanta e gerencia.

### Pré-requisitos

Verifique se o serviço SSH no dispositivo vRealize Suite Lifecycle Manager está ativado.

## Procedimentos

- 1 Faça login no vRealize Suite Lifecycle Manager usando o cliente Secure Shell (SSH).
  - a Abra uma conexão SSH para o FQDN ou o endereço IP do dispositivo virtual.
  - b Faça login usando as seguintes credenciais, com **Configuração** como valor, **Nome de usuário** como raiz e **Senha** como root\_password para o usuário.
- 2 Configure a origem de NTP para o dispositivo virtual.
  - a Abra o arquivo /etc/systemd/timesyncd.conf para editar, como vi.
  - b Remova o comentário da configuração do NTP, adicione as configurações de NTP e salve as alterações. Por exemplo, NTP=ntp.sfo01.rainpole.local ntp.sp01.rainpole.local
- 3 Ative o serviço `systemd-timesyncd` e verifique o status.
  - a Execute o comando `timedatectl set-ntp true` para ativar a sincronização de horário da rede.
  - b Execute o `systemctl restart systemd-timesyncd` para ativar a sincronização do NTP
  - c Execute o `timedatectl status` para verificar o status do serviço.
- 4 Faça logout da sessão inserindo **Logout**.

## Configurar Servidores DNS

Configure seus servidores DNS para configurar o dispositivo do vRealize Suite Lifecycle Manager para resolver os nomes de host e IPs do servidor de nome de domínio.

### Pré-requisitos

Verifique se tem um servidor DNS existente.

### Procedimentos

- 1 No dashboard Meus Serviços, clique em **Lifecycle Operations**.
- 2 Clique em **Configurações** e navegue até **Servidores e Protocolos > DNS**.
- 3 Clique em **Adicionar Servidor DNS**
- 4 Digite um **Nome de servidor DNS** e um **Endereço IP**.
- 5 Clique em **Adicionar**.

## Fonte de dados usando configurações SNMP para vRealize Network Insight

O vRealize Suite Lifecycle Manager dá suporte ao vRealize Network Insight. O vRealize Network Insight consiste em fontes de dados, que são reconhecidas pelo dispositivo vRealize Suite Lifecycle Manager usuário.

Você pode registrar as configurações SNMP, que são relevantes para o vRealize Network Insight. Clique em **Adicionar Configuração** para adicionar SNMP tanto para o tipo 2c quanto para o tipo 3. O SNMP configurado é então usado enquanto você adiciona uma fonte de dados do vRealize Network Insight para Roteadores e Switches.

---

**Observação** A partir da versão 4.0 e posteriores do vRealize Network Insight, um novo tamanho de bloco é introduzido no vRealize Suite Lifecycle Manager, extragrande para a plataforma e para o nó do coletor. Quando existem três nós em um ambiente agrupado em cluster, o tamanho do bloco deve ser extragrande. Todos os nós de plataforma em um ambiente agrupado em cluster devem ter o mesmo tamanho de bloco, grande ou extragrande. Mas não é possível ter os tamanhos grande e extragrande no mesmo cluster.

Se um ambiente agrupado em cluster for implantado com tamanho de bloco grande e se você quiser adicionar mais um nós de plataforma, terá que aumentar manualmente a CPU e o tamanho da RAM do vCenter Server. Em seguida, poderá importar o ambiente e dimensioná-lo horizontalmente com um tamanho de bloco extragrande.

---

## Adicionar Configuração de SNMP

Você pode adicionar a configuração de SNMP.

### Procedimentos

- 1 Navegue pelo dashboard do **Lifecycle Operations** e vá até **Configurações de > SNMP**.
- 2 Clique em **Adicionar Configuração**.
- 3 Para selecionar a **versão do SNMP**, selecione **v2C** ou **v3**.
  - a Se você selecionou v3, digite o **Nome do usuário** e o **Nome do contexto**.
  - b Ao selecionar o tipo de Autenticação, você receberá uma solicitação para digitar a **Senha de autenticação** e o **tipo de Privacidade**.
- 4 Clique em **Adicionar**.

## Substituir certificado para o vRealize Suite Lifecycle Manager

Se você usar o certificado personalizado para o vRealize Suite Lifecycle Manager em vez do certificado padrão autoassinado, substituirá o certificado do vRealize Suite Lifecycle Manager.

### Pré-requisitos

- Um certificado codificado em X509 PEM base-64 e uma chave privada. Certifique-se de que a chave privada não esteja criptografada.
- Uma máquina com acesso SSH ao vRealize Suite Lifecycle Manager e um software como PuTTY e um software SCP como o WinSCP instalado nela.

### Procedimentos

- 1 Renomeie o certificado para server.crt e a chave privada para server.key.

- 2 Abra uma conexão Secure Shell com o dispositivo vRealize Suite Lifecycle Manager como usuário raiz.
- 3 Copie os arquivos de certificado `server.crt` e `server.key` na pasta `/opt/vmware/vlcm/cert`. Você pode usar um software SCP como o WinSCP no Windows. Certifique-se de fazer backup dos arquivos originais antes de os copiar.
- 4 Depois de copiar os certificados, reinicie os serviços de proxy do vRealize Suite Lifecycle Manager para atualizar o certificado do dispositivo.
  - a Reinicie os serviços do sistema executando o seguinte comando na sessão SSH: `sudo systemctl restart nginx`.
  - b Verifique o status dos serviços do sistema executando o seguinte comando na sessão SSH: `sudo systemctl status nginx`.
- 5 Depois de reiniciar os serviços, verifique se o certificado está atualizado no dispositivo, abra um navegador e acesse `https://<lcm-server-host>`.
- 6 Verifique se o novo certificado está visível no navegador.

## Como trabalhar com suporte do produto

Depois de configurar as informações de sistema do vRealize Suite Lifecycle Manager, você pode verificar e aplicar atualizações ou patches que estão disponíveis em seu ambiente já existente.

### Configurar binários de produto

Você pode selecionar um Binário de produto para usar cada produto do vRealize Suite.

Você pode fazer download de binários fora do Lifecycle Manager e disponibilizá-los no caminho NFS.

#### Pré-requisitos

Para usar um binário de produto baixado de My VMware, verifique se você está registrado no My VMware e registrado nos serviços My VMware com o vRealize Suite Lifecycle Manager. Consulte [Registrar-se no My VMware](#).

#### Procedimentos

- 1 Em Meus serviços, navegue até Operações de ciclo de vida.
- 2 Clique em **Configurações** e navegue até **Mapeamento de binário > Binários de produto**.
- 3 Clique em **Adicionar binários**.
- 4 Selecione o tipo de Localização.
  - Local - você pode mapear os binários para a cópia do vRealize Suite Lifecycle Manager baixada localmente.
  - NFS - você pode mapear para um binário de produto baixado com produtos dependentes da localização do binário de produto.

- Downloads de My VMware - você pode mapear para o binário de produto baixado de My VMware.
- ISO do Windows - você pode mapear o binário do ISO necessário para a implantação do Windows a partir do Lifecycle Manager.

**Observação** Os mapeamentos automáticos de OVA do produto são mapeados com base na soma de verificação dos arquivos binários. Quando você seleciona todos os arquivos OVA no compartilhamento NFS e tenta mapear os binários de produto, leva muito tempo para mapear e o disco de dados pode ser encher mais rapidamente. O NFS representa o local onde os arquivos OVA são copiados na unidade compartilhada NFS. O usuário deve fornecer a localização do NFS no formato, NFS-IP:<nfs hostname/ip>:<folder path>/x/y/z. Por exemplo, 10.11.12.134:/caminho/para/pasta.

- 5 Digite a localização do binário de produto a ser usado na caixa de texto **Localização básica** e clique em **Detectar**.
- 6 Para fornecer o ISO do Windows, selecione o tipo de localização como **ISO do Windows** e digite os **Detalhes de mapeamento do ISO do Windows**.
- 7 Selecione o arquivo do binário de produto na lista **Binário de produto**.

**Observação** Por padrão, todos os downloads de My VMware a partir do vRealize Suite são mapeados automaticamente sem intervenção do usuário. Se você já baixou os binários de produto usando integração do vRealize Suite My VMware, mas o mapeamento não existe na lista em Binário de produto, é possível selecionar a opção Downloads do VMware na janela Adicionar binários de produto. Para copiar manualmente os arquivos OVA do dispositivo virtual do vRealize Suite, é possível selecionar a opção **Local** na janela Adicionar binários de produto e fornecer o local que reside no próprio dispositivo do vRealize Suite. Para qualquer um dos cenários, ao clicar em **Detectar**, os binários relevantes são listados na tabela da janela.

- 8 Clique em **Adicionar**.
- 9 Com o vRealize Suite Lifecycle Manager versão 2.0 e posteriores, você também pode visualizar a lista de **Patches** disponíveis para Produtos.
  - a Clique em **Verificar patches on-line**.
  - b Para carregar patches, clique em **CARREGAR**.

**Observação** Agora você pode excluir os binários de produto não compatíveis que não estão em uso. Para excluir os binários, clique em **Excluir binários não compatíveis**, selecione os binários e clique em **Excluir tudo**.

## Como aplicar patches para produtos por meio do vRealize Suite Lifecycle Manager

Você pode pesquisar e baixar patches disponíveis para produtos com suporte no vRealize Suite Lifecycle Manager.

Você pode realizar as seguintes ações usando patches do ícone de notificações:

- Você pode exibir implantações de produtos que possuem os patches.
- Você pode exibir logs de patches.
- Você pode exibir o status de aplicação de patches.

---

**Observação** A partir do vRealize Suite Lifecycle Manager 8.2, se você selecionar o vRealize Automation 8.x para aplicação de patches, uma opção de pré-verificação estará disponível para validação.

---

### Instalar um patch para produtos através do vRealize Suite Lifecycle Manager

Você pode visualizar e clicar no patch relacionado no serviço de Notificação. Em seguida, você será direcionado para a página do ambiente onde poderá visualizar um conjunto detalhado de informações referentes a todos os patches.

#### Procedimentos

- 1 Clique em Lifecycle Operations, navegue para **Configurações > Mapeamento binário**.
  - 2 Clique em **Binários de patch**.
  - 3 Para mapear um patch offline, baixe o patch do portal do [My VMware](#) e coloque-o na pasta de dados no dispositivo vRealize Suite Lifecycle Manager e mapeie o patch offline usando a opção de pasta local na IU do vRealize Suite Lifecycle Manager.
  - 4 Para verificar se há patches disponíveis na Internet, clique em **VERIFICAR PATCHES ONLINE**.
  - 5 Acione a instalação de patch no cartão de produto na página do ambiente.
  - 6 Selecione o patch na lista de patches baixados.
- Os patches devem ser baixados da página Binários do produto. Somente os patches baixados estão listados aqui.
- 7 Clique em **Avançar**.
  - 8 **Revise e instale** o patch disponível e clique em **Concluir**.

O progresso da solicitação de instalação do patch pode ser rastreado em **Solicitações**.

- 9 Para visualizar o histórico de patches, clique em **Histórico de > patches**.

- 10 Para exibir o histórico de patches no cartão do ambiente, clique em **Histórico de patches**

O histórico de patches do produto do vRealize Log Insight não tem conteúdo, mesmo quando os patches do vRealize Log Insight são aplicados com êxito. Isso é causado por causa da versão secundária do vRealize Log Insight após a instalação do patch. Por exemplo, se o patch 1 for aplicado para o vRealize Log Insight 4.6.0, a versão do vRealize Log Insight será alterada para o vRealize Log Insight 4.6.1, e o cartão do produto será atualizada para 4.6.1 e nenhum histórico de patches será visível. Instalar patch no vRealize Suite Lifecycle Manager só é aceito nas seguintes versões dos produtos.

- vRealize Automation 7.5 e posterior.

- vRealize Operations Manager 7.0 e posterior.
- vRealize Business for Cloud 7.5 e posterior.
- vRealize Log Insight 4.7 e posterior.
- vRealize Network Insight 3.9 e posterior.

## Configurar os binários de produtos com patch

Com o patch 8.1, você pode baixar e mapear o pacote OVA que já está com patch em um ambiente do vRealize Automation. Essa operação é útil quando você deseja dimensionar horizontalmente um ambiente com patch. A partir do vRealize Suite Lifecycle Manager versão 8.6.1, os binários de patch do vRealize Log Insight também são compatíveis.

### Pré-requisitos

Certifique-se de que o pacote OVA correspondente ao produto corrigido seja baixado do Portal My VMware para o dispositivo do vRealize Suite Lifecycle Manager e colocado na pasta de dados. Por exemplo: /data/patchovabundles/. Para obter mais informações sobre como baixar os pacotes OVA, clique em portal [My VMware](#). Você também pode ver o procedimento detalhado para o vRealize Automation em [KB 79105](#).

### Procedimentos

1 Clique em Lifecycle Operations para **Configurações de > Mapeamentos binários**.

2 Clique em **Binários de produtos com patch**.

3 Para baixar os patches, clique no link fornecido na UI.

Você será direcionado para a página do My VMware onde poderá baixar o patch ou o pacote OVA necessário.

4 Clique em **ADICIONAR UM BINÁRIO COM PATCH**.

a Digite a **Localização de origem** e clique em **Descobrir**.

A localização de origem é o caminho do diretório no dispositivo do vRealize Suite Lifecycle Manager no qual os arquivos do pacote OVA são recuperados.

b Selecione o pacote OVA necessário na lista e clique em **ADICIONAR**.

5 Para excluir um patch de produto, clique no ícone Excluir no patch selecionado.

## Registrar-se no My VMware

Você pode se registrar no My VMware para acessar licenças, baixar binários de produtos e consumir conteúdo do Marketplace.

Insira seu nome de usuário e senha do My VMware para permitir que o vRealize Suite Lifecycle Manager baixe o binário do produto via My VMware. Você também pode entrar usando o servidor proxy em Configurações do My VMware. A definição das configurações do My VMware é opcional quando você não tem conectividade com a Internet.

## Pré-requisitos

Verifique se os detalhes da conta que estão sendo inseridos têm os seguintes direitos.

- Direito para o vRealize Suite 2017, ou posterior, ou vCloud Suite 2017, ou posterior, com permissões de download e exibição de licença para baixar produtos do vRealize Suite.
- Direito para o vRealize Network Insight ou o NSX Data Center Enterprise Plus com permissões de download e exibição de licença para baixar o vRealize Network Insight.

O usuário configurado do My VMware deve ter permissões para baixar e exibir licenças. Baixe o pacote de suporte do *VMware Solution Marketplace*.

## Procedimentos

- 1 Navegue até **Servidores e Contas** e clique em **My VMware**.
- 2 Clique em **ADICIONAR CONTA MY VMWARE**.
- 3 Insira seu nome de usuário e senha do My VMware e clique em **Enviar**.

Após o registro, você poderá baixar todos os binários necessários.

---

**Observação** Para baixar o binário do produto, clique na seta de download em **Ações**. Se a sua rede exigir configurações de proxy para acessar sites externos, você poderá fornecer esses detalhes na seção Configurar Proxy. Para obter mais informações sobre como definir as configurações de proxy, consulte [Definir as configurações de proxy](#).

---

## Definir as configurações de proxy

Se estiver usando um servidor proxy na sua rede, deverá configurar o servidor proxy vRealize Suite Lifecycle Manager.

O Proxy Normal (com ou sem Credencial) e o Proxy com configuração do AD têm suporte do vRealize Suite Lifecycle Manager.

## Pré-requisitos

Você deve ter instalado e configurado um servidor proxy em sua rede antes de usá-lo no vRealize Suite Lifecycle Manager e o IP do servidor proxy deve ter um nome de host que é resolvível a partir console do dispositivo do vRealize Suite Lifecycle Manager.

---

## Observação

- Se não conseguir configurar o proxy no vRealize Suite Lifecycle Manager, certifique-se de que o ICMP está permitido do vRealize Suite Lifecycle Manager para o host de proxy e de que haja entradas DNS diretas e inversas para o host proxy.
- Se o servidor proxy não tiver um nome de host resolvível, o procedimento para adicionar o proxy falhará.

---

## Procedimentos

- 1 Navegue até Lifecycle Operations e clique em **Proxy**.

- 2 Clique em **Proxy**.
- 3 Alterne para **Configurar proxy** para usar um servidor proxy para vRealize Suite Lifecycle Manager ou desmarque-o para remover um servidor proxy existente.  
vRealize Suite Lifecycle Manager não salva as configurações do servidor proxy quando o proxy é desativado.
- 4 Se você estiver habilitando o proxy, digite o **Servidor**, a **Porta**, o **Nome de usuário** e a **Credencial**.
- 5 Clique em **Salvar**.  
Se o vRealize Suite Lifecycle Manager já estiver configurado para usar um servidor proxy, os detalhes do proxy serão exibidos.

## Configurar certificado no Locker

Você pode gerar um novo certificado para os produtos que são implantados no vRealize Suite Lifecycle Manager.

### Pré-requisitos

- Os certificados que estão prestes a expirar em menos de 15 dias não podem ser importados.
- Para gerenciar o certificado para um ambiente importado, adicione o certificado ao vRealize Suite Lifecycle Manager e execute a sincronização de inventário para que o certificado seja mapeado para o ambiente importado. Depois disso, os assistentes de substituição do certificado e dimensionamento horizontal ficarão cientes do certificado existente.

### Procedimentos

- 1 Para adicionar um certificado, vá para **Lifecycle Manager > Locker**.

**2** Você pode selecionar Gerar certificado ou Importar certificado.

Opção	Descrição
<b>Gerar</b>	<ul style="list-style-type: none"> <li>a Insira as caixas de texto necessárias.</li> <li>b Selecione o comprimento da chave.</li> <li>c Digite o Domínio/Nome do host do servidor válido. Você também pode incluir o certificado curinga. Por exemplo, você pode inserir *.sql.local.</li> <li>d Digite o <b>FQDN</b> ou <b>endereço IP</b>.</li> <li>e Clique em <b>Gerar</b>.</li> </ul>
<b>Importar certificado</b>	<ul style="list-style-type: none"> <li>a Digite um nome de certificado válido.</li> <li>b Na caixa de texto Frase-chave, digite o &lt;Cert-Password&gt; (se aplicável).</li> <li>c Clique em <b>Navegar arquivo</b> e navegue até o arquivo PEM salvo.</li> <li>d Quando você carrega um arquivo PEM, os detalhes da chave privada e da cadeia de certificados são preenchidos automaticamente.</li> <li>e Digite manualmente os detalhes da chave privada e da cadeia de certificados.</li> <li>f Clique em <b>Importar</b>.</li> </ul> <p>Os requisitos do arquivo PEM são:</p> <ul style="list-style-type: none"> <li>■ A cadeia de certificados e a chave devem estar no mesmo arquivo.</li> <li>■ O arquivo PEM importado pode ter a chave de 2.048 bits ou a chave de 4.096 bits.</li> <li>■ Se o certificado do arquivo PEM estiver criptografado, a frase-chave deve ser fornecida durante a importação do certificado para o vRealize Suite Lifecycle Manager.</li> </ul>
<b>Gerar CSR</b>	<ul style="list-style-type: none"> <li>a Insira as caixas de texto necessárias.</li> <li>b Selecione o comprimento da chave.</li> <li>c Digite um nome de domínio válido. Você também pode incluir o certificado curinga. Por exemplo, você pode inserir *.sql.local.</li> <li>d Digite o endereço IP no qual você está atribuindo o certificado.</li> </ul> <p><b>Observação</b> Gerar CSR baixa um arquivo PEM. Esse arquivo pode ser encaminhado para a autoridade de certificação para assinatura e pode ser realizado como um certificado confiável. O arquivo pem baixado terá a chave privada e a cadeia de solicitações de certificados. Tenha cuidado e compartilhe apenas a parte CSR do arquivo pem, mas não a chave para a assinatura do certificado.</p>

- 3** Clique em **Gerar**.
- 4** Você pode clicar no certificado do inventário do para visualizar os detalhes e seus ambientes associados aos produtos deles.
- 5** Para baixar ou substituir o certificado, clique nas reticências verticais no certificado.

### Resultados

O vRealize Suite Lifecycle Manager gera um novo certificado para o domínio específico fornecido pelo usuário.

# Configurar a licença no Locker

O Locker é um aplicativo como o Lifecycle Manager que ajuda a gerenciar o certificado, as senhas e as licenças em um único painel. Você pode configurar licenças no nível do Locker.

## Pré-requisitos

Verifique se uma licença já está disponível.

## Procedimentos

- 1 Navegue até o dashboard **Lifecycle Operations** e clique em **Locker**.
- 2 À esquerda, clique no ícone **Licença**.
- 3 Para adicionar uma licença, clique em **ADICIONAR**.
- 4 Digite o alias na caixa de texto **Alias da licença**.
- 5 Digite a **Chave de licença** e clique em **Validar**.
- 6 Depois de validar a precisão da licença, clique em **Adicionar**.

A partir do vRealize Suite Lifecycle Manager 8.4.0, as licenças do vRealize Cloud podem ser adicionadas diretamente ao locker do vRealize Suite Lifecycle Manager na interface do usuário.

- 7 Para atualizar uma licença existente, clique em qualquer licença na tabela de licenças.
  - a Clique nas reticências verticais e clique em **Atualizar**.
  - b Leia o resumo da licença atual e clique em **Avançar**.
  - c Selecione um ambiente na tabela de referências e clique em **Avançar**.
  - d Selecione uma licença no menu suspenso e clique em **Concluir**.
- 8 Para excluir uma licença, clique nas reticências verticais e clique em **Excluir**.
  - a Se o Lifecycle Manager tiver uma ou mais contas do My VMware configuradas, as chaves de licença correspondentes serão sincronizadas automaticamente. Para sincronizar licenças da conta do My VMware, clique em **ATUALIZAR**. No entanto, se você tiver adicionado manualmente a mesma chave de licença ao Locker, a entrada correspondente da conta do My VMware não poderá ser capturada.
  - b Quando qualquer produto é importado para o vRealize Suite Lifecycle Manager, as chaves de licença presentes no produto também são capturadas e armazenadas no Locker em Licenças. Se a mesma chave de licença já estiver presente, ela não poderá ser importada.
  - c Se qualquer produto estiver associado a uma licença no vRealize Suite Lifecycle Manager, a entrada da licença não poderá ser excluída do Locker.
  - d O vRealize Suite Lifecycle Manager não restringe a aplicação de várias licenças a qualquer produto. No entanto, o comportamento do produto permite definir apenas uma chave de licença como ativa a qualquer momento.

- e A exclusão da licença do locker do vRealize Suite Lifecycle Manager não remove a chave de licença do produto em si.
- 9 As chaves de licença podem ser aplicadas a produtos gerenciados pelo vRealize Suite Lifecycle Manager em **Ambientes > Página inicial** em Lifecycle Operations. Selecione um produto em qualquer ambiente gerenciado do Lifecycle Operations, clique nas reticências horizontais no nome do produto, selecione **Adicionar Licença** e siga as etapas.

## Configurar a senha dentro do Locker

O Locker no vRealize Suite Lifecycle Manager armazena todas as senhas que são usadas no vRealize Suite Lifecycle Manager. Adicione as senhas para adicionar vCenter Server, implantações de produto, importação de produtos, My VMware, e atualização da senha do produto. Você pode configurar uma senha no nível do locker e ser recuperada da UI.

### Procedimentos

- 1 Navegue até Lifecycle Operations, no dashboard Meus serviços, clique em **Locker**.
- 2 No painel esquerdo, clique no ícone de chave.
- 3 Para adicionar uma Senha, clique em **ADICIONAR**.
- 4 Digite o **Alias da senha** e a **Senha**.
- 5 Para confirmar, digite novamente a Senha, digite a **Descrição da senha** e um **Nome de usuário** válido.

---

**Observação** A caixa de texto de nome de usuário é obrigatória para adicionar ao vCenter Server vRealize Suite Lifecycle Manager.

---

- 6 Clique em **Adicionar**.

## Gerenciamento de senhas no Locker

A partir do vRealize Suite Lifecycle Manager 8.2, você pode gerenciar senhas que são armazenadas no nível do Locker para servidores vCenter, produtos e My VMware.

É possível adicionar uma nova senha na página Senhas do Locker. Clique em **Adicionar** e insira os detalhes do alias e da senha para adicionar uma nova senha.

Para senhas existentes na página Senhas, clique nas reticências (...) e selecione uma das seguintes opções:

Funcionalidade	Descrição
Exibir Senha	Se for um usuário administrador, você poderá visualizar a senha selecionada em texto sem formatação após autenticar a senha raiz SSH do vRealize Suite Lifecycle Manager. A senha de exibição não está disponível para usuários do VMware Identity Manager.
Copiar ID	Você pode copiar o ID da senha e reutilizar a senha. Por exemplo, ao exportar o JSON para implementação de um produto, você pode copiar e reutilizar o ID de senha existente.
Editar Senha	Você pode editar uma senha que não tem referência a uma senha existente. Por exemplo, se você usar uma senha em um ambiente, como o vCenter Server ou o MyVMware, a opção de edição para essa senha estará desativada.
Excluir Senha	Você pode excluir uma senha que não é mais usada e não tem referências. Por exemplo, se você usar uma senha em um ambiente, como o vCenter Server ou o MyVMware, a opção de exclusão para essa senha estará desabilitada.

Se você selecionar uma senha existente, poderá exibir seus detalhes e suas referências. A guia **Detalhes** exibe o identificador de senha, o nome de usuário e a descrição da senha, bem como as datas de criação e última atualização da senha selecionada. A guia **Referências** exibe as referências para ambientes no nível do produto e do nó, senhas do vCenter em centros de dados e outras senhas que são usadas na guia **Configurações**.

Você também pode atualizar uma senha para produtos, nós, MyVMware, proxy e servidores vCenter. Para atualizar a senha, clique nas reticências verticais (:) da senha selecionada.

### Observação

- Quando você atualiza uma senha que é gerenciada pelo vRealize Suite Lifecycle Manager, como produtos, nós ou o usuário raiz, essa senha é atualizada na página Senhas e no inventário do vRealize Suite Lifecycle Manager.
- Quando você atualiza uma senha para o vCenter, o MyVMware, o proxy ou administradores de configuração do VMware Identity Manager, a senha é atualizada apenas no inventário do vRealize Suite Lifecycle Manager.

## Adicionar um Centro de dados a vRealize Suite Lifecycle Manager

Você pode adicionar um centro de dados a vRealize Suite Lifecycle Manager para fazer o backup de seus ambientes em nuvem privada.

## Procedimentos

- 1 No painel esquerdo, clique em **Centros de dados** e clique em **Centros de dados**.

Você pode ver todos os centros de dados e os produtos associados a eles. Você também pode clicar nos ícones de produto que o direcionarão para a página de exibição de detalhes do produto específico.
- 2 Clique em **+ Adicionar Centro de dados**.
- 3 Digite o **Nome do Centro de dados** e forneça uma **Localização** mesmo que a localização não esteja disponível no menu suspenso.
- 4 Clique em **Adicionar**.
- 5 Para excluir um centro de dados, selecione o ícone Excluir.

---

**Observação** Se houver quaisquer solicitações INICIADAS, EM ANDAMENTO ou CONCLUÍDAS para um ambiente, não será possível excluir um centro de dados. Se ele tiver uma solicitação COM FALHA, ou uma solicitação relacionada ao vCenter, a solicitação será arquivada.

---

## Próximo passo

Adicione um vCenter ao centro de dados. Consulte [Adicionar um vCenter a um Centro de dados](#).

## Atribuir uma Função de usuário no vCenter Server

Crie uma função de usuário no Cliente do vSphere com privilégios necessários para o vRealize Suite Lifecycle Manager. A mesma função pode ser atribuída ao usuário que pode adicionar um vCenter Server ao vRealize Suite Lifecycle Manager.

### Pré-requisitos

Verifique se você tem privilégios administrativos para adicionar uma função a um usuário ou a um grupo de usuários. Você deve ter privilégios administrativos para usar o vCenter Server.

Se você estiver usando o vCenter implantado no SDDC do VMC, deverá usar a função CloudAdmin disponível. Para obter mais informações sobre o VMC no vCenter, consulte a documentação do [VMware Cloud on AWS](#). Quando você implanta um VMC no vCenter, poderá usar a função CloudAdmin padrão. Para saber mais sobre os privilégios de administrador de nuvem, consulte a documentação de [privilégios do CloudAdmin](#).

## Procedimentos

- 1 Faça login no vCenter Server usando o Cliente do vSphere.
- 2 Na página inicial do Cliente do vSphere clique em **Funções** em Administração.
- 3 Crie uma função para todas as interações do sistema entre o vRealize Suite Lifecycle Manager e o vCenter Server.
- 4 Clone **Somente leitura** e forneça um nome para a função.

- 5 Na caixa de diálogo **Criar função**, configure a função usando as seguintes definições de configuração e clique em **Avançar**.

Configuração	Valor
<b>Nome da função</b>	vRealize Suite Lifecycle Manager
<b>Privilégio</b>	<ul style="list-style-type: none"> <li>■ Reppositório de dados           <ul style="list-style-type: none"> <li>■ Você pode selecionar Todos os privilégios.</li> </ul> </li> <li>■ Host.Local           <ul style="list-style-type: none"> <li>■ Operações - Adicionar host ao vCenter</li> <li>■ Operações - Criar Máquina virtual</li> <li>■ Operações - Excluir Máquina virtual</li> <li>■ Operações - Reconfigurar Máquina virtual</li> <li>■ Inventário - Modificar - Cluster</li> </ul> </li> <li>■ Rede           <ul style="list-style-type: none"> <li>■ Atribuir rede</li> </ul> </li> <li>■ Recurso           <ul style="list-style-type: none"> <li>■ Atribuir vApp ao pool de recursos</li> <li>■ Atribuir Máquina virtual ao pool de recursos</li> </ul> </li> <li>■ vApp           <ul style="list-style-type: none"> <li>■ Você pode selecionar Todos os privilégios.</li> </ul> </li> <li>■ Máquinas virtuais           <ul style="list-style-type: none"> <li>■ Você pode selecionar Todos os privilégios.</li> </ul> </li> <li>■ Biblioteca de conteúdo           <ul style="list-style-type: none"> <li>■ Você pode selecionar Todos os privilégios.</li> </ul> </li> </ul>

Essa função herda os privilégios System Anonymous, System View e System Read.

**Observação** Você deve ter permissões para criar uma biblioteca de conteúdo. A biblioteca de conteúdo usa um repositório de dados para armazenar todos os modelos, portanto, você precisa de permissão para acessar, ler e gravar no mesmo repositório de dados. Portanto, todos os privilégios no repositório de dados e na biblioteca de conteúdo são necessários.

- 6 Forneça um nome para a nova função e clique em **Concluir**.  
 7 Selecione **Permissões Globais** em Administração e clique em **Gerenciar**.  
 8 Para adicionar permissões, clique no sinal de mais.  
 9 Selecione o usuário e a função que criou e clique em **OK**.

## Adicionar um vCenter Server a um centro de dados do vRealize Suite Lifecycle Manager

Adicione um vCenter Server a um centro de dados antes de usar esse vCenter Server para criar um ambiente de nuvem privada.

### Pré-requisitos

Certifique-se de ter o nome de domínio completo, o nome de usuário e a senha do vCenter Server.

## Procedimentos

- 1 No painel esquerdo, clique em **Centros de Dados**.
- 2 Para adicionar um vCenter, na página **Datacenters**, clique em **+ Adicionar vCenter**.
- 3 Digite o **Nome do vCenter** e **FQDN do vCenter**.
- 4 Clique em **Selecionar Credenciais do vCenter**.
  - a Você pode procurar credenciais existentes do vCenter ou adicionar novas credenciais usando o sinal +.
  - b Clique no sinal + no canto direito para atribuir uma senha para a credencial do vCenter selecionada.
  - c Digite os detalhes da Senha e clique em **Adicionar**.
- 5 Digite o **Nome de usuário do vCenter** para o vCenter Server.

Você deve ter os privilégios necessários do vCenter.
- 6 Selecione o **Tipo do vCenter**.
  - Gerenciamento: todos os produtos VMware SDDC Suite são gerenciados por este tipo de vCenter.
  - Carga de trabalho: todas as VMs de carga ou relacionadas a negócios são gerenciadas por este tipo de vCenter.
  - Gerenciamento consolidado e carga de Trabalho: é um tipo do vCenter no qual os produtos VMware SDDC Suite e as VMs de carga são gerenciados juntos.

A seleção de Tipo de vCenter é atualmente usada apenas para a classificação; a configuração não tem funcionalidade do produto associada.
- 7 Clique em **Validar** e **Salvar** as alterações.
- 8 Para importar os vCenter Servers, clique em **Importar**.
  - a Selecione o arquivo .CSV e clique em **Importar**. Você pode carregar apenas um arquivo de cada vez para a importação em massa de VCs em um centro de dados selecionado.
  - b Clique em **Enviar**.

## Próximo passo

Vá à página **Solicitações** para ver o status dessa solicitação. Quando o status for **concluído**, você pode usar esse vCenter Server para criar ambientes. Para obter mais informações sobre os privilégios de usuário do vCenter, consulte [Atribuir uma Função de usuário no vCenter Server](#)

## Remover o vCenter Server do centro de dados do vRealize Suite Lifecycle Manager

Você pode excluir um vCenter Server do centro de dados do vRealize Suite Lifecycle Manager que não é utilizado pelo ambiente.

## Pré-requisitos

Certifique-se de que o vCenter não tenha uma referência, como um nome de domínio totalmente qualificado ou um nome de usuário associado a um ambiente. Se o vCenter estiver associado a um ambiente, a opção de exclusão será desativada para o vCenter.

## Procedimentos

- 1 Na página Centro de Dados, selecione o vCenter e clique em **Excluir vCenter**.
- 2 Clique em **Excluir** para remover o vCenter selecionado.

## vRealize Suite Lifecycle Manager em um ambiente VMware Cloud on AWS

O vRealize Suite Lifecycle Manager é compatível com o VMware Cloud (VMC) no ambiente AWS. O VMC on AWS é uma oferta de nuvem privada integrada desenvolvida pela VMware e pela Amazon Web Services (AWS). O vRealize Suite Lifecycle Manager é compatível com as versões M11 e M12 do VMC.

Você pode instalar o vRealize Suite Lifecycle Manager em um ambiente VMC usando o Easy Installer. Para obter mais informações, consulte a documentação [Easy Installer](#). Configure uma máquina virtual no vCenter de um Centro de Dados Definido por Software (SDDC) do VMC para iniciar o Easy Installer. Para criar o SDDC de nuvem usando o VMC on AWS e para conectar o SDDC ao centro de dados do seu produto, consulte a documentação [Como começar com o VMware Cloud on AWS](#). Depois de ter implantado com êxito o vRealize Suite Lifecycle Manager no VMC, você também pode instalar outros produtos do VMware vRealize Suite, como o VMware Identity Manager e o vRealize Automation no ambiente VMC para realizar as operações do Dia 2.

Em um ambiente VMC, você deve adicionar o vCenter do SDDC somente como um endpoint. Não é recomendável adicionar qualquer vCenter externo ao SDDC. Ao implantar um vCenter do VMC, certifique-se de que você tenha privilégios de administrador de nuvem. Para saber mais sobre os privilégios de administrador de nuvem, consulte a documentação de [privilégios do CloudAdmin](#).

## Como criar funções para acesso específico

No vRealize Suite Lifecycle Manager, você pode delegar as operações de substituição de certificados a qualquer usuário de forma consistente nos produtos do conjunto da VMware.

Com essa acessibilidade, você também pode permitir que usuários não administradores executem ações como substituir o certificado.

## Atribuir funções para operações de certificado

Com esta seção, você pode criar um administrador de certificado que seja um usuário ou um grupo com uma função específica atribuída. Esses usuários ou grupos de usuários podem ter certos privilégios para acessar o certificado para qualquer produto vRealize.

## Pré-requisitos

- Verifique se há usuários ou grupos de usuários disponíveis e se eles não têm funções anteriores mapeadas.

## Procedimentos

- 1 Em Lifecycle Operations, clique em **Gerenciamento de usuários**.
- 2 Navegue até Gerenciamento de usuários, clique em **ADICIONAR USUÁRIO/GRUPO**.
- 3 Digite um nome de usuário ou grupo e a lista de usuários é preenchida automaticamente.  
Se um usuário já tiver uma função mapeada do usuário selecionado, selecione outro usuário.
- 4 Clique em **Avançar**.
- 5 Selecione a função **Certificado de Administrador** e clique em **Avançar**.
- 6 Clique em **Enviar**.
- 7 Faça logout de vRealize Suite Lifecycle Manager e faça login como um usuário VMware Identity Manager para acessar os serviços como um administrador atribuído.

## Alterar Certificado para vRealize Suite Lifecycle Manager

Como administrador vRealize Suite Lifecycle Manager, você pode alterar seu certificado para a instância do vRealize Suite Lifecycle Manager.

## Pré-requisitos

Verifique se tem um certificado do vRealize Suite Lifecycle Manager existente disponível.

## Procedimentos

- 1 No dashboard Meus Serviços, clique em Lifecycle Operations.
- 2 Navegue até Configurações do e clique em **Alterar Certificado**.  
Você pode visualizar os detalhes do certificado usados pelo vRealize Suite Lifecycle Manager.
- 3 Para substituir o certificado, clique em **SUBSTITUIR CERTIFICADO**.
  - a Leia o resumo do certificado atual e clique em **Avançar**.
  - b Selecione um certificado do menu suspenso e clique em **Avançar**.
  - c Clique em **Executar Pré-verificação** para validar os detalhes do certificado e clique em **Concluir**.
- 4 Depois de clicar em Concluir, você pode visualizar o progresso da alteração do certificado na página **Detalhes da solicitação**.

## Gerenciamento de identidade e tenant com o VMware Identity Manager

No Gerenciamento de Usuários ou de Identidade, você pode mapear os usuários presentes VMware Identity Manager para as funções disponíveis no vRealize Suite Lifecycle Manager. Configurar o VMware Identity Manager é um processo obrigatório antes de instalar qualquer produto do conjunto. Se você não tiver instalado durante a instalação do vRealize Suite Lifecycle Manager, ainda receberá a solicitação para configurá-lo e, em seguida, prossiga.

A implantação de um Identity Manager por meio do vRealize Suite Lifecycle Manager é por meio de um único nó ou de um cluster com um banco de dados PostgreSQL interno incorporado no dispositivo e não suporta um banco de dados externo, como o Microsoft SQL. O vRealize Suite Lifecycle Manager suporta o dimensionamento horizontal do VMware Identity Manager. Para obter mais informações, consulte [Dimensionar horizontalmente o VMware Identity Manager](#).

Depois de implantar um ambiente global com êxito, em Serviço de Identidade e gerenciamento de tenants, você pode ver.

- Gerenciamento de diretórios
- Gerenciamento de usuários
- Gerenciamento de tenants

A seguir estão as funções disponíveis.

- Administrador de nuvem do LCM
- Desenvolvedor de conteúdo
- Gerente de liberação de conteúdo
- Administrador de certificados

Embora o Administrador de nuvem do vRealize Suite Lifecycle Manager tenha acesso ao serviço de Lifecycle Operations, apenas alguns serviços na guia Configurações, como **Configuração de servidor de NTP, SNMP, DNS, My VMware e Mapeamento binário** são acessados. Somente o **administrador de LCM**, o `admin@local` tem o privilégio de acessar todas as configurações no serviço do Lifecycle Operations. O usuário padrão `admin@local` é o único administrador de aplicativos que pode acessar o serviço de **Gerenciamento de usuários**, no qual o **Gerenciamento de diretórios** e o **Identity Management** são manipulados.

---

**Observação** Com a migração de versões anteriores do vRealize Suite Lifecycle Manager para a versão atual do vRealize Suite Lifecycle Manager, as funções de Administrador do LCM e Administrador do LCM Cloud convergem para o Administrador do LCM Cloud. Todos os usuários que faziam parte do administrador do LCM nas versões anteriores do vRealize Suite Lifecycle Manager agora se tornarão Administradores do LCM Cloud do vRealize Suite Lifecycle Manager.

Adicionar o VMware Identity Manager é uma etapa opcional e torna-se possível ao configurar o VMware Identity Manager com Single Sign-On no vRealize Suite Lifecycle Manager e seus produtos.

---

**Observação** Quando o VMware Identity Manager é usado com o vRealize Suite Lifecycle Manager, apenas o **Active Directory sobre LDAP** e o **Active Directory com IWA** são usados para sincronizar usuários e grupos com o serviço do VMware Identity Manager. O Active Directory sobre LDAP e o Active Directory com IWA são a única integração de diretório com suporte.

---

## Gerenciar seu diretório no Gerenciamento de Identidade

Com o Gerenciamento de Diretórios, você pode integrar seu diretório empresarial ao VMware Identity Manager para sincronizar usuários e grupos com o serviço VMware Identity Manager. A partir do vRealize Suite Lifecycle Manager 8.0, é possível criar, ler, atualizar e excluir diretórios no VMware Identity Manager. Todas as atualizações feitas na configuração de diretório do vRealize Suite Lifecycle Manager 8.0 serão refletidas no VMware Identity Manager.

Opções disponíveis no gerenciamento de diretórios.

- **Diretórios:** é possível criar e gerenciar Active Directories no vRealize Suite Lifecycle Manager. Você pode criar um ou mais diretórios e sincronizá-los com seus diretórios empresariais. Com a função Exibir diretório, você pode verificar logs de sincronização e alertas de sincronização, além de exibir os metadados básicos do diretório. A função Editar Diretório permite uma atualização dos atributos mapeados, usuários e DNs de grupo. É possível excluir uma configuração de diretório do vRealize Suite Lifecycle Manager.
- **Definições de atributos de usuários:** a página Atributos de Usuários lista os atributos de usuários padrão que são sincronizados no diretório, e você pode adicionar outros atributos a serem mapeados para atributos do Active Directory.

---

**Observação** O Gerenciamento de Diretório é controlado pelo usuário administrador do vRealize Suite Lifecycle Manager: admin@local. O Gerenciamento de Diretório estará disponível no vRealize Suite Lifecycle Manager 8.0 somente se a versão do VMware Identity Manager disponível no ambiente global for superior ou igual a 3.3.0.

---

## Diretórios compatíveis

- Active Directory sobre LDAP: crie esse tipo de diretório se você pretende se conectar a um único ambiente de domínio do Active Directory
- Active Directory, autenticação integrada do Windows: crie esse tipo de diretório se você pretende se conectar a um ambiente de vários domínios ou florestas do Active Directory.
- LDAP seguro

---

**Observação** Para uma versão 3.3.5 do VMware Identity Manager ativada para FIPS, a senha de associação deve ser de catorze caracteres.

---

Para configurar o diretório empresarial, execute as seguintes tarefas.

- Crie um diretório do mesmo tipo que o seu diretório empresarial e especifique os detalhes da conexão.
- Mapeie os atributos do VMware Identity Manager para os atributos usados no Active Directory ou no diretório LDAP.
- Especifique os usuários e os grupos a serem sincronizados.
- Sincronize usuários e grupos.

Depois de integrar seu diretório empresarial e executar a sincronização inicial, você poderá atualizar a configuração e sincronizar a qualquer momento.

## Configurar a definição de atributo do usuário

Quando configurar o diretório para sincronizar com o Active Directory, especifique os atributos do usuário. Antes de configurar o diretório, você pode especificar quais atributos padrão são obrigatórios e, se necessário, podem ser adicionados atributos adicionais para mapear os atributos do Active Directory.

Alterar os atributos padrão de um obrigatório para não obrigatório e marcar um atributo como obrigatório só poderão ser feitos se não houver diretórios criados. Depois que os diretórios forem criados e sincronizados, eles não poderão ser alterados. Você pode marcar os atributos obrigatórios e não obrigatórios antes de adicionar qualquer diretório na página de diretórios. Quando adicionar novos atributos personalizados depois que os diretórios são criados, para mapeá-los, você precisa editar o diretório e atualizar o mapeamento de atributo de diretório. A alteração será efetivada da próxima vez que o diretório for sincronizado com o Active Directory.

## Atribuir funções de usuário com o Gerenciamento de usuário

Você pode mapear uma função de usuário em relação a usuários e grupos presentes no VMware Identity Manager. Na página Gerenciamento de usuário, o usuário ou um grupo pode ser selecionado e um mapeamento pode ser editado. Você pode excluir um mapeamento de função, se necessário. Se um grupo tiver uma função e se você fizer parte do grupo e fizer login no vRealize Suite Lifecycle Manager, poderá assumir as mesmas funções desse grupo. Se você tiver mapeamento individual, pode ser a consolidação da função do usuário e das funções atribuídas ao grupo.

### Pré-requisitos

Verifique se você tem algum dos grupos de usuários para o vRealize Suite Lifecycle Manager.

Função	Descrição da função	Adicionar URL de usuário/grupos
Administrador de nuvem do LCM	Administrador de nuvem para o vRealize Suite Lifecycle Manager	ug-vrslcm-admins@rainpole.local
Gerente de liberação de conteúdo	Gerente de liberação de conteúdo	ug-vrslcm-content-admins@rainpole.local

Função	Descrição da função	Adicionar URL de usuário/grupos
Desenvolvedor de conteúdo	Desenvolvedor de conteúdo	ug-vrslcm-content-developers@rainpole.local
Administrador de certificados	Desenvolvedor para executar operações de certificado	ug-vrslcm-certificate-admins@rainpole.local

#### Procedimentos

- 1 Clique em **Gerenciamento de Identidade e Tenants** no dashboard Meus Serviços.
- 2 No lado esquerdo, navegue e clique em **Gerenciamento de usuário**.
- 3 Para adicionar um usuário ou um grupo, clique em **+ADICIONAR USUÁRIO/GRUPO**.
- 4 Para selecionar um usuário na lista preenchida na tabela, digite um usuário existente ou um grupo e clique em **Avançar**.  
Se um usuário ou grupo já tiver um mapeamento, um aviso será exibido e você será solicitado a editar o mapeamento de função em vez de criá-lo novamente.
- 5 Selecione uma função para o usuário recém-criado e clique em **Avançar**.
- 6 Leia o resumo e clique em **Enviar**.

## Adicionar o Active Directory sobre LDAP

Você pode criar este tipo de diretório se pretender se conectar a um único ambiente de domínio do Active Directory. Para o Active Directory em um tipo de diretório LDAP, o conector se vincula ao Active Directory usando uma autenticação de vinculação simples.

#### Pré-requisitos

- Liste os grupos e usuários do Active Directory a serem sincronizados a partir do Active Directory.
- Verifique se você especificou os atributos padrão necessários e adicione atributos adicionais na definição de Atributos do usuário.
- Verifique se você tem as credenciais de usuário necessárias para adicionar um diretório.

#### Procedimentos

- 1 Clique em **Gerenciamento de Identidade e Tenants** no dashboard Meus Serviços.
- 2 Navegue até a guia Gerenciamento de Diretórios e clique em **Diretórios**.
- 3 Clique em **Adicionar diretório** e selecione **Adicionar Active Directory sobre LDAP**.

#### 4 Na guia **Detalhes do diretório**:

Campos	Descrição
<b>Informações do Diretório</b>	Digite um nome de diretório válido.
<b>Sincronização e Autenticação do Diretório</b>	<p>Selecione o conector a ser sincronizado com o Active Directory. O conector é um componente de serviço do VMware Identity Manager que sincroniza dados de usuários e de grupos entre o Active Directory e o VMware Identity Manager serviço.</p> <p>Quando usado como um provedor de identidade, ele também autentica os usuários. Cada nó do dispositivo do VMware Identity Manager contém um componente do conector padrão. Quando necessário, um conector dedicado também pode ser implantado através de um ambiente global.</p>
<b>Autenticação ativada</b>	<p>Se você quiser que o conector realize a autenticação, selecione <b>Sim</b>. Você pode indicar se o conector selecionado também realiza a autenticação. Se você estiver usando um provedor de identidade de terceiros para autenticar usuários, clique em <b>Não</b>.</p>
<b>Atributo de Pesquisa de Diretório</b>	Selecione um atributo de conta no menu suspenso que contém um nome de usuário.
<b>Localização de Servidor</b>	<p>Marque a caixa de seleção <b>Diretório compatível com localização de serviço DNS</b>.</p> <ul style="list-style-type: none"> <li>■ Se o Active Directory exigir acesso por SSL/TLS, marque a caixa de seleção <b>Diretório requer que todas as conexões usem STARTTLS ou SSL</b> na seção <b>Certificados</b> e copie e cole os controladores de domínio intermediários (se usados) e certificados de CA raiz na caixa de texto <b>Certificado SSL</b>. Digite primeiro o certificado de CA intermediária e, em seguida, o certificado de CA raiz. Verifique se cada certificado está no formato PEM e inclui as linhas BEGIN CERTIFICATE e END CERTIFICATE. Se os controladores de domínio tiverem certificados de várias Autoridades de certificação raiz e intermediária, digite todas as cadeias de certificado de CA raiz intermediária, uma após a outra. Se o Active Directory exigir acesso por SSL/TLS e você não fornecer os certificados, não será possível criar o diretório.</li> <li>■ Se você não quiser usar a Localização de serviço DNS, verifique se o <b>Directory oferece suporte à localização de serviço DNS</b> não está selecionado e digite o número da porta e o nome do host do servidor do Active Directory.</li> </ul>

Campos	Descrição
<b>Certificados</b>	Se o Active Directory exigir acesso por SSL/TLS marque a caixa de seleção <b>Diretório requer que todas as conexões usem SSL</b> na seção <b>Certificados</b> e copie e cole o certificado intermediário (se usado) e a CA raiz do controlador de domínio na caixa de texto <b>Certificado SSL</b> . Digite primeiro o certificado de CA intermediária e, em seguida, o certificado de CA raiz. Verifique se o certificado está no formato PEM e inclui as linhas BEGIN CERTIFICATE e END CERTIFICATE. Se o Active Directory exigir acesso por SSL/TLS e você não fornecer o certificado, não será possível criar o diretório.
<b>Detalhes do usuário do bind</b>	<ul style="list-style-type: none"> <li>■ Base DN - Digite o DN para iniciar as pesquisas de conta. Por exemplo, OU=myUnit,DC=myCorp, DC=com. A Base DN é usada para autenticação. Somente os usuários sob o DN Base podem se autenticar. Certifique-se de que os DNs do grupo e os DNs do usuário que você especificar posteriormente para sincronização estão nessa Base DN.</li> <li>■ Vincular DN do usuário - digite os detalhes da conta. Por exemplo, CN=binduser,OU=myUnit,DC=myCorp, DC=com. Use uma conta de usuário da vinculação com uma senha que não expire.</li> <li>■ Vincular senha: clique em <b>Testar Conexão</b> para verificar se o diretório consegue se conectar ao Active Directory.</li> </ul>

**5** Clique em **Criar e Avançar**.

Para o Active Directory sobre LDAP, os domínios são listados com uma marca de seleção.

**6** Na guia **Detalhes da seleção do domínio**, selecione o domínio e clique em **Avançar**.

**7** Para mapear o atributo de diretório para o Active Directory, na guia **Mapear atributo**, selecione o atributo necessário e clique em **Salvar e Avançar**.

**8** Na guia **Seleção do grupo**, para sincronizar do Active Directory com o diretório do VMware Identity Manager especifique os detalhes do DN do grupo e clique em **Avançar**.

Você também pode selecionar todos os grupos do Active Directory que já estão disponíveis na lista para sincronização com o diretório.

a Para selecionar grupos, clique em **Adicionar nome distinto do grupo** e especifique um ou mais DNs do grupo. Selecione os grupos sob eles. Especifique os DNs do grupo que estão na Base DN que você especificou na caixa de texto "Base DN" na página Adicionar diretório. Se um DN do grupo estiver fora da Base DN, os usuários desse DN serão sincronizados, mas não poderão fazer login.

b Clique em **Encontrar grupos**. A coluna **Ações** lista o número de grupos encontrados no DN. Para selecionar todos os grupos no DN, clique em **Selecionar todos** ou clique no número e selecione os grupos específicos a sincronizar. Quando você sincroniza um grupo, todos os usuários que não possuem Usuários de Domínio como grupo primário no Active Directory não são sincronizados.

c Selecione a opção **Sincronizar membros do grupo aninhado**.

**9** Na guia **Seleção do usuário**, digite os detalhes do DN do usuário e clique em **Avançar**.

Administradores do conjunto é um nome de usuário no Active Directory que atua como um usuário administrador para os produtos implantados do conjunto, registros e tabela AD.

**10 Selecione a opção Sincronizar Membros do Grupo Aninhado e digite Administradores do Conjunto.**

Quando esta opção está ativada, todos os usuários que pertencem diretamente ao grupo selecionado e todos os usuários que pertencem aos grupos aninhados sob ele são sincronizados quando o grupo tem a qualificação. Observe que os grupos aninhados não são sincronizados; somente os usuários que pertencem aos grupos aninhados são sincronizados. No diretório do VMware Identity Manager, esses usuários serão membros do grupo primário que você selecionou para sincronização. Se a opção “Sincronizar membros do grupo aninhado” estiver desativada, quando você especificar um grupo para sincronização, todos os usuários que pertencem diretamente a esse grupo serão sincronizados. Os usuários que pertencem a grupos aninhados abaixo dele não são sincronizados. A desativação dessa opção é útil para grandes configurações do Active Directory em que percorrer uma árvore de grupo exige muitos recursos e tempo. Se você desativá-la, certifique-se de selecionar todos os grupos cujos usuários deseja sincronizar.

**11 Clique em Salvar e Avançar.** Na página **Seleção do usuário**, clique em **Adicionar usuário** e especifique os DNs dos usuários a serem sincronizados. Especifique os DNs do usuário que estão na Base DN que você especificou na caixa de texto Base DN na página Adicionar diretório. Se um DN do usuário estiver fora da Base DN, os usuários desse DN serão sincronizados, mas não poderão fazer login. Clique em **Salvar e Avançar**.

**12 Revise a guia Verificação do exercício de simulação**, leia o resumo, clique em **Sincronizar e Concluir** para iniciar a sincronização com o diretório. A conexão com o Active Directory será estabelecida, e os nomes de usuários e grupos serão sincronizados do Active Directory com o diretório do VMware Identity Manager.

**13 Clique em Enviar.**

**14 Para editar**, clique no ícone **Editar** no Active Directory específico na lista de diretórios ativos. Qualquer informação adicionada é anexada à configuração do VMware Identity Manager. No entanto, qualquer remoção através da edição apenas remove a configuração do inventário do vRealize Suite Lifecycle Manager e não do VMware Identity Manager.

**15 Para excluir**, clique no ícone **Excluir** no Active Directory específico na lista de diretórios ativos. A ação de exclusão exclui o Active Directory somente do inventário do vRealize Suite Lifecycle Manager e não do VMware Identity Manager.

## Adicionar o Active Directory com a autenticação integrada do Windows

Você pode criar esse tipo de diretório se pretender se conectar a um ambiente do Active Directory de vários domínios. O conector se vincula ao Active Directory usando a autenticação integrada do Windows.

### Pré-requisitos

Verifique se você tem as credenciais de usuário necessárias para adicionar um diretório.

## Procedimentos

- 1 Clique em **Gerenciamento de Identidade e Tenants** no dashboard Meus Serviços.
- 2 Navegue até a guia Gerenciamento de diretórios e clique em **Diretórios**.
- 3 Clique em **+Adicionar Diretório** e em **Adicionar Active Directory com IWA**.
- 4 Na guia **Detalhes do diretório**:

Campos	Descrição
<b>Informações do diretório</b>	Digite um nome de diretório válido.
<b>Sincronização e autenticação do diretório</b>	Selecione o conector a ser sincronizado com o Active Directory. O Connector é um componente de serviço do VMware Identity Manager que sincroniza os dados de usuários e grupos entre o Active Directory e o serviço do VMware Identity Manager. Ele autentica os usuários. Cada nó do dispositivo do VMware Identity Manager contém um componente do conector padrão. Se necessário, um conector dedicado também pode ser implementado por meio de um ambiente global.
<b>Autenticação ativada</b>	Você pode indicar se o conector selecionado também realiza a autenticação. Se você estiver usando um provedor de identidade de terceiros para autenticar usuários, clique em <b>Não</b> .
<b>Atributo de Pesquisa de Diretório</b>	Selecione um atributo de pesquisa no menu suspenso.
<b>Certificados</b>	<ul style="list-style-type: none"> <li>■ Se o Active Directory exigir acesso por SSL/TLS marque a caixa de seleção <b>Diretório requer que todas as conexões usem STARTTLS</b> na seção <b>Certificados</b> e copie e cole os certificados intermediários (se usados) e a CA raiz dos controladores de domínio na caixa de texto <b>Certificado SSL</b>. Digite primeiro o certificado de CA intermediária e, em seguida, o certificado de CA raiz. Verifique se cada certificado está no formato PEM e inclui as linhas BEGIN CERTIFICATE e END CERTIFICATE. Se os controladores de domínio possuem certificados de várias Autoridades de Certificação Raiz e Intermediária, digite todas as cadeias de certificado de CA Raiz-Intermediária, uma após a outra. Se o Active Directory exigir acesso por SSL/TLS e você não fornecer os certificados, não será possível criar o diretório.</li> </ul>
<b>Detalhes de Ingresso em um Domínio</b>	Digite o nome de domínio, o nome de domínio do usuário administrador e a senha do domínio.
<b>Detalhes do usuário do bind</b>	<ul style="list-style-type: none"> <li>■ Digite o <b>Nome de usuário da vinculação</b> e a <b>Senha da vinculação</b> do usuário da vinculação com permissão para consultar usuários e grupos para os domínios necessários. Digite o nome de usuário como <code>sAMAccountName@domain</code>, onde domínio é o nome de domínio completo. Usando uma conta usuário da vinculação com uma senha que não expire.</li> </ul>

- 5 Clique em **Criar e Avançar**.

Você pode selecionar os domínios que devem ser associados à conexão do Active Directory.

- 6 Na guia **Detalhes da Seleção do Domínio**, selecione o domínio e clique em **Enviar e Avançar**.

O Active Directory com IWA preenche a lista de domínios e você pode selecionar ou editar os domínios conforme necessário.

- 7 Para verificar se os nomes de atributos do diretório do VMware Identity Manager estão mapeados para os atributos corretos do Active Directory, na guia **Mapear atributo**, selecione o atributo necessário e clique em **Enviar e Avançar**.

- 8 Na guia **Seleção do grupo**, especifique os detalhes do DN do grupo e clique em **Avançar**.

Para selecionar grupos, clique em **Adicionar nome distinto do grupo** e especifique um ou mais DNs do grupo e selecione os grupos sob eles. Especifique os DNs do grupo que estão na Base DN que você especificou na caixa de texto Base DN na seção Adicionar diretório. Se um DN do grupo estiver fora da Base DN, os usuários desse DN serão sincronizados, mas você não poderá fazer login.

Quando você sincroniza um grupo, todos os usuários que não possuem Usuários de Domínio como grupo primário no Active Directory não são sincronizados.

- a Seleccione a opção **Sincronizar Membros do Grupo Aninhado**.

- 9 Na guia **Seleção do usuário**, digite os detalhes do DN do usuário e clique em **Avançar**.

---

**Observação** Quando essa opção está ativada, todos os usuários que pertencem diretamente ao grupo selecionado e todos os usuários que pertencem a grupos aninhados sob ele são sincronizados quando o grupo tem a qualificação. Observe que os grupos aninhados não são sincronizados; somente os usuários que pertencem aos grupos aninhados são sincronizados. No diretório do VMware Identity Manager, esses usuários são membros do grupo primário que você selecionou para sincronização. Se a opção **Sincronizar Membros do Grupo Aninhado** estiver desativada, quando você especificar um grupo para sincronização, todos os usuários que pertencem diretamente a esse grupo serão sincronizados. Os usuários que pertencem a grupos aninhados abaixo dele não são sincronizados. A desativação dessa opção é útil para grandes configurações do Active Directory em que percorrer uma árvore de grupo exige muitos recursos e tempo. Se você desativá-la, certifique-se de selecionar todos os grupos cujos usuários deseja sincronizar.

---

Administradores do conjunto é um nome de usuário no Active Directory que atua como um usuário administrador para os produtos implantados do conjunto, registros e tabela AD.

- 10 Na guia **Verificação do exercício de simulação**, leia o Resumo.

- 11 Clique em **Sincronizar e Concluir** para iniciar a sincronização com o diretório. A conexão com o Active Directory será estabelecida e os nomes de usuários e grupos serão sincronizados do Active Directory com o VMware Identity Manager diretório público.

- 12 Clique em **Enviar**.

- 13 Para editar, clique no ícone **Editar** no Active Directory específico na lista de diretórios ativos. Qualquer informação adicionada fica anexada à configuração do VMware Identity Manager. No entanto, se remover através da edição, você só poderá remover a configuração do inventário vRealize Suite Lifecycle Manager inventário e não do VMware Identity Manager.

- 14 Para excluir, clique no ícone **Excluir** no Active Directory específico na lista de diretórios ativos. Você pode excluir o Active Directory somente do inventário do vRealize Suite Lifecycle Manager e não do VMware Identity Manager.

## Gerenciamento de tenants no vRealize Suite Lifecycle Manager

A partir do 8.1, o vRealize Suite Lifecycle Manager é compatível com a criação e o gerenciamento de tenants. Os tenants são criados no VMware Identity Manager e estão associados a produtos que são sensíveis ao tenant. Portanto, além de gerenciar diretórios sobre o VMware Identity Manager, os tenants também são gerenciados. O suporte ao recurso multiempresa só está disponível no VMware Identity Manager 3.3.2. O Gerenciamento de Usuário chamado assim anteriormente é renomeado agora para Gerenciamento de Identidade e Tenant.

### Visão geral da multilocação

Esta seção descreve os principais conceitos e terminologias que devem ser compreendidos antes de iniciar a multilocação.

#### Familiarize-se com os termos de gerenciamento de tenants

---

**Observação** O tenant principal agora é chamado de tenant primário.

---

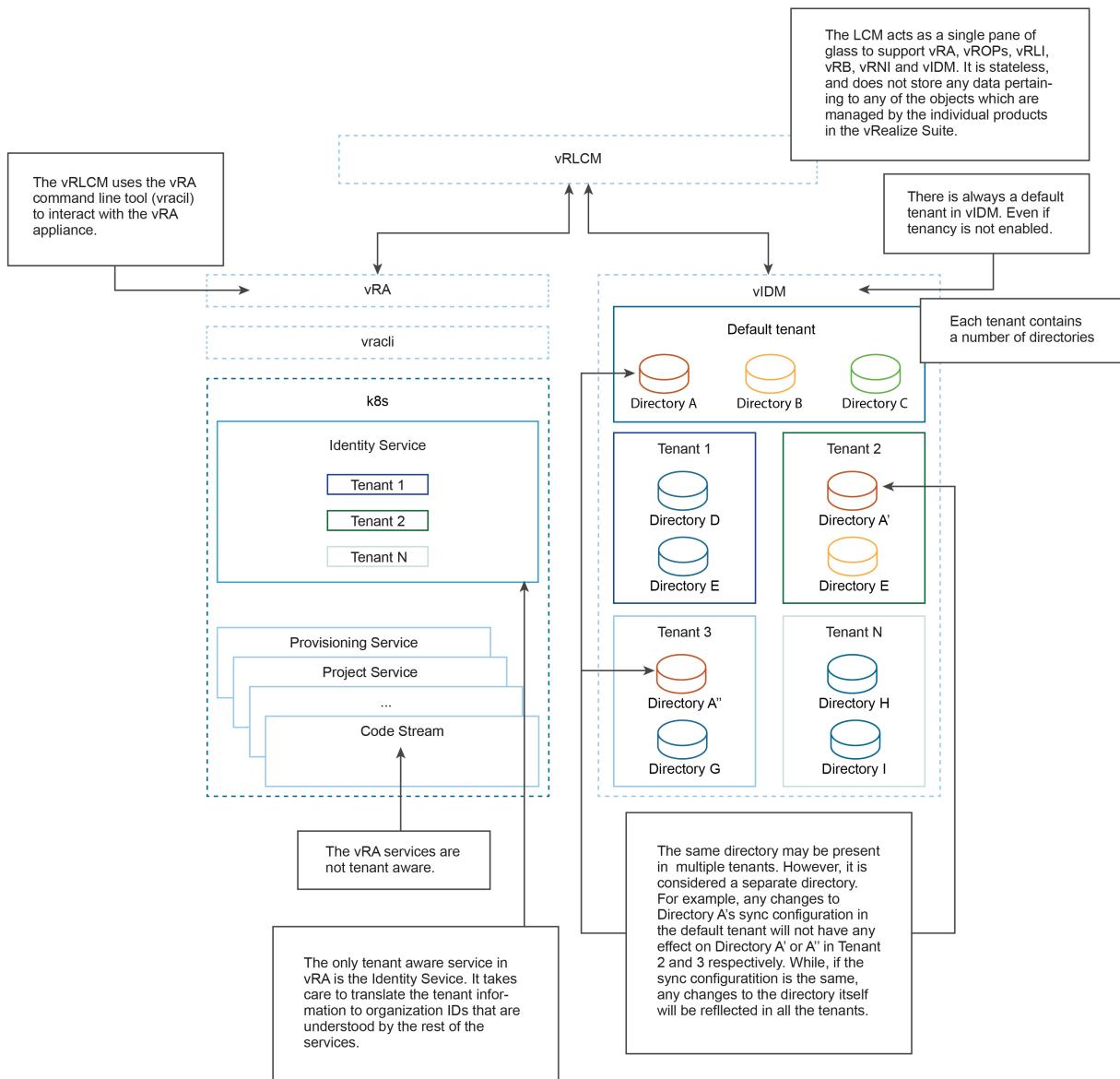
- Tenant: é o nível mais alto em uma estrutura organizacional no VMware Identity Manager. Todos os objetos, como diretórios, usuários, grupos e IDPs de terceiros, são mantidos individualmente para cada tenant. Cada tenant é isolado do restante dos tenants, e eles não compartilham recursos entre si.
- Tenant primário: há sempre pelo menos um tenant (primário, padrão ou base) presente no VMware Identity Manager, que é chamado de tenant primário.

Para usuários do vRealize Automation 7.x, este é o “vsphere.local” que estava presente por padrão em implementações do vRealize Automation 7.x. O tenant primário no vRealize Automation 7.x era inicializado por padrão com “vsphere.local” como nome. Porém, isso não acontece em uma implantação autônoma do VMware Identity Manager. O nome do tenant primário é formado com base no primeiro nó do VMware Identity Manager a ser implantado e inicializado. Por exemplo, se “idm1.vmwlab.local” for o primeiro nó do VMware Identity Manager a ser implantado, quando você inicializar o VMware Identity Manager , o tenant primário será criado com o nome “idm1”. Nós subsequentes dimensionados, como “idm2.vmwlab.local” e “idm3.vmwlab.local”, não têm efeito. O nome do tenant primário é formado apenas uma vez e permanece o mesmo em uma instância única ou em cluster.

- Alias do tenant primário: você não poderá criar subtenants no VMware Identity Manager abaixo do tenant principal até que algumas configurações sejam definidas e habilitadas. Definir um nome de alias para o tenant primário é uma configuração importante. Um alias deve ser criado no tenant primário, que, por sua vez, sempre deve ser acessado por meio do FQDN do alias do tenant primário em um único nó ou em uma instância em cluster.
- Administrador de provedor: um administrador que possui a infraestrutura de gerenciamento, que inclui o VMware Identity Manager, o vRealize Automation e outros produtos. O administrador cria e gerencia todos os tenants e associa produtos a eles. O usuário administrador do vRealize Suite Lifecycle Manager, “admin@local” é o único administrador de provedor e está autorizado a executar as funcionalidades de gerenciamento de tenants.

- Administrador de tenant: um administrador com o nível mais alto de permissão administrativa em cada tenant do VMware Identity Manager. Essa permissão pode ser atribuída a usuários locais do VMware Identity Manager e usuários do Active Directory presentes no tenant do VMware Identity Manager.
- Produtos com Reconhecimento de Tenant: produtos que oferecem suporte para multilocação e mantêm o isolamento adequado com cada instância de tenant lógica são produtos com reconhecimento de tenant. Eles têm um mapeamento de um-para-um com tenants do VMware Identity Manager. A partir do vRealize Suite Lifecycle Manager versão 8.1, apenas o vRealize Automation 8.1 tem reconhecimento de tenant.
- Organização e Proprietário da Organização do vRealize Automation: no vRealize Automation 8.x, a organização é a construção de nível superior e tem um mapeamento de 1:1 com o tenant do VMware Identity Manager. O Proprietário da Organização tem permissão administrativa na Organização ou tenant do vRealize Automation. Ao adicionar tenants e associar o vRealize Automation com o tenant recém-adicionado, o administrador de tenant do VMware Identity Manager torna-se o proprietário da organização para o novo tenant. Para obter mais informações sobre como adicionar tenants, consulte [Como adicionar tenants](#).
- Diretório: diretórios são o segundo nível de objetos no VMware Identity Manager. Ele representa um armazenamento ou provedor de identidade externo, como o Active Directory (AD) ou um servidor OpenLDAP. Existem várias variantes de diretórios com suporte no VMware Identity Manager. Você pode adicionar o Active Directory via LDAP e Active Directory com IWA na seção Gerenciamento de Diretórios.
- Sincronização de Diretórios: ao adicionar diretórios, opções de configuração são fornecidas para filtrar e sincronizar os usuários e grupos necessários do armazenamento ou provedor de identidade para o banco de dados do VMware Identity Manager. Somente após uma sincronização bem-sucedida, você poderá integrar os usuários e grupos com o VMware Identity Manager.
- Diretórios no tenant: cada tenant pode conter vários diretórios. A mesma configuração de diretório pode estar presente em vários tenants. Porém, ela é considerada um diretório separado. Por exemplo: você adicionou o Diretório A ao tenant primário com algumas configurações de diretório (DNs de usuário, DNs de grupo, configurações de sincronização). E tem dois subtenants chamados Tenant-1 e Tenant-2. As mesmas configurações do diretório A podem ser usadas para adicionar os diretórios A1 e A2 em cada um dos subtenants, respectivamente, de modo que o mesmo conjunto de usuários e grupos sejam sincronizados nos subtenants: Tenant-1 e Tenant-2. Após a adição, alterações nas configurações de sincronização do diretório A no tenant primário não afetarão os diretórios A1 e A2 e seus usuários e grupos sincronizados no Tenant-1 e Tenant-2. Todos os três diretórios e suas configurações são independentes uns dos outros. Todos os três diretórios apenas serão afetados se o armazenamento ou provedor de identidades externo for alterado. Por exemplo, se usuários ou grupos estiverem sendo removidos diretamente do provedor de identidades, isso influenciará todos os três diretórios em todos os três tenants.

**Figura 2-1. Modelo de multilocação**



## Modelo de multilocação

Esta seção descreve o modelo de multilocação, explicando como os tenants podem ser acessados por meio de FQDNs de tenant e a importância de habilitar a multilocação junto com o certificado e os requisitos de DNS.

## Ativando a multilociação

O tenant principal agora é chamado de tenant primário. Mesmo que no dia 0 o VMware Identity Manager pronto para uso inclua um tenant primário já disponível, ele é mantido com uma configuração mínima, e a criação adicional de tenants abaixo do tenant primário não é possível. Uma sequência de configurações e chamadas de API deve ser executada no VMware Identity Manager para habilitar a multilociação. Deve haver um nome de alias criado para o tenant primário quando você ativa a multilociação. Para obter mais informações sobre como ativar a multilociação, consulte [Ativar o recurso multiempresa](#).

Por exemplo, um VMware Identity Manager com FQDN “idm1.vmwlab.local” já pode ter um tenant primário com o nome “idm1”. Antes de ativar a multilociação, é obrigatório criar um alias para o tenant primário. Por exemplo, defina “master-tenant” e use o mesmo nome de alias em todos os lugares onde o tenant principal é referenciado.

## FQDNs de tenants

Por padrão, os tenants criados no VMware Identity Manager são acessados por meio de URLs de tenant que não passam de FQDNs mapeados para o servidor VMware Identity Manager. Todos os tenants têm seu próprio FQDN de tenant. Por exemplo, em um VMware Identity Manager de nó único com o nome de host `idm1.vmwlab.local`, o nome de tenant primário (`idm1`) e o alias de tenant primário (master-tenant), o tenant primário deve ser acessado por meio de seu FQDN `master-tenant.vmwlab.local`. Se um novo tenant (tenant 1) for criado, ele deverá ser acessado somente por meio de `tenant1.vmwlab.local`.

Como cada tenant requer um FQDN dedicado, a criação de tenants no VMware Identity Manager requer obrigatoriamente um registro de DNS do tipo A mapeando o FQDN do tenant para o endereço IP do servidor do VMware Identity Manager. Para uma implantação do VMware Identity Manager em cluster, cada FQDN de tenant deve ter um mapeamento de registro do tipo A para o endereço IP do balanceador de carga do VMware Identity Manager.

O mesmo modelo também se aplica ao vRealize Automation. Quando o vRealize Automation está associado a um tenant, o tenant do vRealize Automation deve ser acessado por FQDNs de tenant do vRealize Automation. Por exemplo, o VMware Identity Manager com o FQDN `idm1.vmwlab.local` e um tenant “tenant 1” acessível via `tenant1.vmwlab.local` e o vRealize Automation 8.1 `vra1.vmwlab.local` integrado a esse VMware Identity Manager e associado a

“tenant 1”. Como mencionado, o tenant do vRealize Automation e o tenant do VMware Identity Manager têm um mapeamento de 1:1, de modo que o vRealize Automation do tenant primário ainda possa ser acessado por `vra1.vmwlab.local` e o vRealize Automation “tenant 1” deve ser acessado por `tenant1.vra1.vmwlab.local`.

---

**Observação** Há uma diferença entre os FQDNs de tenant do VMware Identity Manager e do vRealize Automation. Para uma instância do VMware Identity Manager, o formato do FQDN do tenant é o nome do tenant (tenant1) seguido pelo nome de domínio do VMware Identity Manager (vmwlab.local). Por exemplo, `tenant1.vmwlab.local`. Como é o nome do tenant seguido do domínio, ele permanece o mesmo para o VMware Identity Manager em cluster. Para um vRealize Automation, o formato do FQDN do tenant do vRealize Automation é o nome do tenant (tenant1) seguido do FQDN do servidor do vRealize Automation (`vra1.vmwlab.local`). Por exemplo, `tenant1.vra1.vmwlab.local`. Para um vRealize Automation em cluster atrás de um balanceador de carga `vra-lb.vmwlab.local`, o tenant 1 deve ser acessado via `tenant1.vra1.lb.vmwlab.local`.

---

Igual ao VMware Identity Manager, até mesmo os FQDNs de tenant do vRealize Automation exigem mapeamento de DNS. Porém, para um vRealize Automation, ele deve ser o registro do tipo CNAME mapeando os FQDNs de tenants do vRealize Automation para o FQDN do servidor do vRealize Automation. Para uma implantação do vRealize Automation em cluster, todos os FQDNs de tenants do vRealize Automation devem ter um registro de DNS do tipo CNAME apontando para o FQDN do balanceador de carga do vRealize Automation.

Além de ter mapeamentos de DNS como pré-requisito obrigatório, certificados também são obrigatórios para que a locação funcione. Ambos os servidores VMware Identity Manager e vRealize Automation e seus平衡adores de carga, dependendo da arquitetura de implantação, devem ter seus certificados correspondentes contendo todos os FQDNs de tenants necessários.

FQDNs de tenants em uma configuração de nó único

- Nó do VMware Identity Manager: `idm1.vmwlab.local`
- Nó do vRealize Automation: `vra1.vmwlab.local`
- Nome do alias do tenant primário: `master-tenant`
- Tenants: `tenant-1, tenant-2`

Nomes dos tenants	FQDNs de tenants do VMware Identity Manager	FQDNs de tenants do vRealize Automation
<code>master-tenant</code>	<code>https://master-tenant.vmwlab.local</code>	<code>https://vra1.vmwlab.local</code>
<code>tenant-1</code>	<code>https://tenant-1.vmwlab.local</code>	<code>https://tenant-1.vra1.vmwlab.local</code>
<code>tenant-2</code>	<code>https://tenant-2.vmwlab.local</code>	<code>https://tenant-2.vra1.vmwlab.local</code>

FQDNs de tenants em uma configuração em cluster

- Balanceador de carga do VMware Identity Manager: `idm-lb.vmwlab.local`

Nós do VMware Identity Manager: `idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local`

Balanceador de carga do vRealize Automation: `vra-lb.vmwlab.local`

Nós do vRealize Automation: `vra1.vmwlab.local`, `vra2.vmwlab.local`, `vra3.vmwlab.local`

Nome do alias do tenant primário: **master-tenant**

Tenants: tenant-1, tenant-2

<b>Nomes dos tenants</b>	<b>FQDNs de tenants do VMware Identity Manager</b>	<b>FQDNs de tenants do vRealize Automation</b>
<code>master-tenant</code>	<code>https://master-tenant.vmwlab.local</code>	<code>https://vra-lb.vmwlab.local</code>
<code>tenant-1</code>	<code>https://tenant-1.vmwlab.local</code>	<code>https://tenant-1.vra-lb.vmwlab.local</code>
<code>tenant-2</code>	<code>https://tenant-2.vmwlab.local</code>	<code>https://tenant-2.vra-lb.vmwlab.local</code>

**Observação** Depois que você habilitar a multilocação, o VMware Identity Manager só deverá ser acessado por meio de seus FQDNs de tenants. Os antigos FQDNs e nomes de host (`idm1.vmwlab.local`, `idm2.vmwlab.local`, `idm3.vmwlab.local` e `idm-lb.vmwlab.local`) se tornarão inválidos.

### Requisitos de certificados obrigatórios

Dependendo do tipo de implantação do VMware Identity Manager e do vRealize Automation, seus certificados de servidor correspondentes devem conter todos os FQDNs de tenants. Como cada tenant forma seu próprio FQDN de tenant (tanto o FQDN de tenant do VMware Identity Manager quanto o FQDN de tenant do vRealize Automation), cada tenant criado exige que seu FQDN

de tenant seja adicionado como parte de ambos os certificados do VMware Identity Manager e do vRealize Automation. Habilitar a multilocação no VMware Identity Manager também requer certificados do VMware Identity Manager atualizados à medida que o tenant primário obtém um novo nome de alias e o FQDN do tenant primário sofre uma alteração.

---

## Observação

- Quando você altera os certificados no VMware Identity Manager para ativar a multilocação ou cria tenants, isso desativa o serviço e resulta em tempo de inatividade. Se o certificado do VMware Identity Manager for alterado, isso resultará em um tempo de inatividade do serviço. Os produtos ou serviços integrados com o VMware Identity Manager para fins de autenticação não podem usar o login de autenticação do VMware Identity Manager durante o tempo de inatividade. Além disso, a alteração do certificado do VMware Identity Manager requer nova confiança em todos os produtos ou serviços, o que novamente resulta em tempo de inatividade para os produtos.
- Para cada novo tenant criado e associado ao vRealize Automation, até mesmo os certificados do vRealize Automation devem ser alterados, e isso resulta em tempo de inatividade de serviço para o vRealize Automation.
- Para evitar tempos de inatividade de serviço no vRealize Automation, no VMware Identity Manager e em outros produtos ou serviços integrados com o VMware Identity Manager, geralmente é recomendável ter certificados curinga. Para um novo tenant, qualquer alteração feita no certificado do VMware Identity Manager ou do vRealize Automation pode criar um tempo de inatividade no vRealize Automation.
- Se certificados curinga não forem usados, entradas específicas de SAN deverão ser criadas para cada FQDN de tenant em todos os certificados necessários.
- O serviço Locker do vRealize Suite Lifecycle Manager ajuda no gerenciamento de certificados nos nós de servidor do VMware Identity Manager e do vRealize Automation. Com o vRealize Suite Lifecycle Manager, quando você substitui o certificado do VMware Identity Manager, a redefinição da confiança do certificado do VMware Identity Manager em todos os produtos é realizada automaticamente.
- Produtos ou serviços externos ao vRealize Suite Lifecycle Manager são tratados manualmente. O serviço Locker não lida com a atualização de certificados de平衡adores de carga. Isso deve ser feito manualmente pelo usuário. Sempre que os certificados de平衡adores de carga forem alterados, sua confiança deverá ser redefinida nos produtos.
  - Para o VMware Identity Manager, a operação de atualização ou substituição de certificado do VMware Identity Manager no vRealize Suite Lifecycle Manager garante internamente que o certificado do平衡ador de carga do VMware Identity Manager tenha a confiança redefinida antes da atualização dos certificados de servidor do VMware Identity Manager. Portanto, é recomendável primeiro alterar o certificado do平衡ador de carga do VMware Identity Manager manualmente e, em seguida, fazer uma operação de atualização ou substituição do certificado do VMware Identity Manager por meio do serviço Locker do vRealize Suite Lifecycle Manager.
  - Para o vRealize Automation 8.x, quando SSL é encerrado no平衡ador de carga do vRealize Automation e o certificado do平衡ador de carga é alterado manualmente, certifique-se de clicar em “Confiar novamente no平衡ador de carga” no cartão do produto vRealize Automation 8.x para confiar novamente no certificado do平衡ador de carga no vRealize Automation. Para obter mais detalhes, consulte [Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager](#).

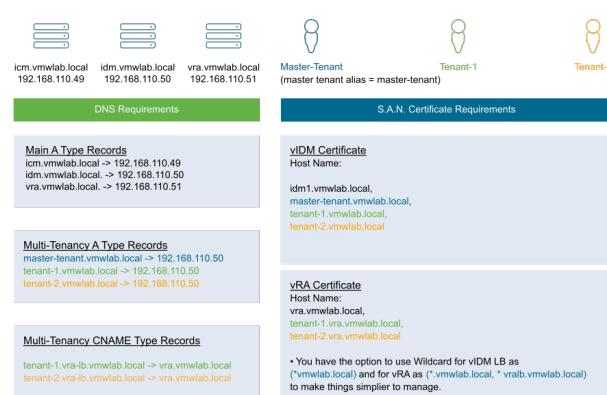
## Requisitos obrigatórios de DNS

Para o VMware Identity Manager de um único nó, você precisa de registros de DNS do tipo A realçando os FQDNs de tenant para o endereço IP do servidor do VMware Identity Manager. E, para um VMware Identity Manager em cluster, são necessários registros de DNS do tipo A que apontem os FQDNs de tenants para o endereço IP do balanceador de carga do VMware Identity Manager.

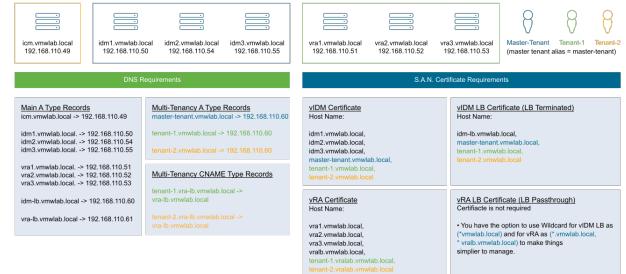
Para o vRealize Automation, para um único nó, são necessários registros de DNS do tipo CNAME que apontem FQDNs de tenants do vRealize Automation para o FQDN do servidor do vRealize Automation. E, para um vRealize Automation em cluster, são necessários registros de DNS do tipo CNAME que apontem FQDNs de tenants do vRealize Automation para o FQDN do balanceador de carga do vRealize Automation.

## Requisitos para multilocação

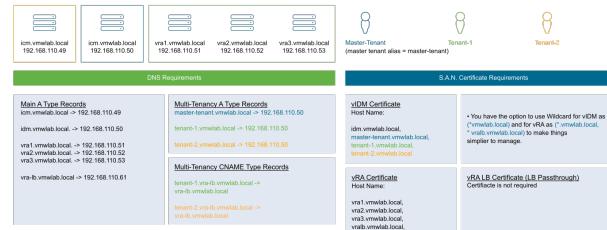
**Figura 2-2. VMware Identity Manager de nó único e vRealize Automation**



**Figura 2-3. VMware Identity Manager e vRealize Automation Cluster**



**Figura 2-4. vIDM Single e vRA Cluster**



**Figura 2-5. VMware Identity Cluster e vRealize Automation Single**



## Ativar o recurso multiempresa

O recurso multiempresa não é ativado imediatamente. Você pode optar por ativar o recurso multiempresa.

## Pré-requisitos

- A versão do ambiente global do VMware Identity Manager deve ser 3.3.2 ou posterior.
- Verifique se os inventários estão sincronizados para todos os ambientes no vRealize Suite Lifecycle Manager e se todos os ambientes e produtos estão atualizados. Isso é para descobrir todas as integrações de produto com o VMware Identity Manager necessárias para registrar novamente o VMware Identity Manager.
- Verifique se o certificado do ambiente global do VMware Identity Manager é gerenciado por meio do serviço de Locker do vRealize Suite Lifecycle Manager.
- Certifique-se de tirar um smartphone VMware Identity Manager. É recomendável, pois ativar o recurso multiempresa permite que o VMware Identity Manager seja acessado por meio de FQDNs de tenant e as URLs de VMware Identity Manager existentes não estarão acessíveis.
- Para um VMware Identity Manager agrupado em cluster, verifique se o status de integridade de cluster do VMware Identity Manager está verde ao disparar a integridade do cluster. Para obter mais informações, [Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager](#)
- Verifique se o certificado do VMware Identity Manager está atualizado com o FQDN do alias de tenant primário. Certifique-se também de que o registro de DNS tipo A seja adicionado, mapeando o FQDN do alias do tenant primário. Para obter mais informações sobre os requisitos obrigatórios de DNS e certificado, consulte [Modelo de multilocação](#).

## Procedimentos

- 1 Clique em **Identidade e Gerenciamento de tenants** e navegue até **Gerenciamento de tenants**.
- 2 Leia a mensagem Opt-in e clique em **Ativar recurso multiempresa**.
- 3 Digite o nome do alias do tenant primário.

Certifique-se de que esse nome de host ou FQDN já não existe. Durante a ativação do recurso multiempresa, esse FQDN é atribuído ao tenant primário.

Certifique-se de que todos os produtos atualmente integrados ao ambiente global do VMware Identity Manager já estão listados e selecionados para registrar novamente em relação ao novo FQDN do alias de tenant primário na tabela "Registrar novamente o produto". Para obter mais informações sobre Referências de Produto, consulte [Referências do Produto](#).

- 4 Clique em **Enviar**, após validar as entradas.

Depois de ativar o recurso multiempresa no VMware Identity Manager, ele só poderá ser acessado por meio de seus FQDNs do tenant e, nesse momento, como o tenant primário é o único tenant disponível, o FQDN do alias de tenant primário é o único endpoint através do qual o VMware Identity Manager pode ser acessado. Quando o vRealize Suite Lifecycle Manager ativar a solicitação do recurso multiempresa for concluída, crie tenants na guia **Gerenciamento de tenants**.

## Gerenciamento de tenants

Esta seção descreve todas as funcionalidades de gerenciamento de tenant disponíveis para o vRealize Suite Lifecycle Manager.

Enquanto você está gerenciando seus tenants, é possível adicionar, excluir, pesquisar e gerenciar seus tenants também.

### Adicionar Tenants

Adicionar Tenant permite que você adicione tenants ao VMware Identity Manager junto com a criação de um administrador de tenants e, opcionalmente, adicione diretórios ao tenant criado e associe produtos com reconhecimento do tenant ao tenant recém-criado.

Quando você adiciona um tenant, o fluxo de trabalho também contém uma etapa de pré-verificação que valida todas as entradas fornecidas e os ambientes selecionados para garantir que a criação de tenants e as associações de produtos funcionem perfeitamente.

#### Pré-requisitos

- Verifique se você tem o DNS configurado no vRealize Automation e no VMware Identity Manager. Para acessar um tenant, o servidor DNS deve ser configurado corretamente antes de iniciar o fluxo do vRealize Suite Lifecycle Manager “Adicionar Tenant”.
- Certifique-se de que o registro de DNS do tipo A seja adicionado ao novo FQDN do tenant. Para um ambiente de vários SAN, verifique se o certificado do VMware Identity Manager está atualizado com o novo FQDN do tenant a ser criado. Para obter mais detalhes, consulte [Modelo de multilocação](#). Para todas as instâncias do vRealize Automation que devem ser associadas ao novo tenant, certifique-se de que os registros DNS do tipo CNAME sejam adicionados e os requisitos de certificado sejam cumpridos.
- Para todas as instâncias do vRealize Automation que devem ser associadas ao novo tenant, certifique-se de que os registros DNS do tipo CNAME sejam adicionados e os requisitos de certificado sejam inseridos.

#### Procedimentos

- 1 No dashboard Meus Serviços, clique em **Gerenciamento de identidade e tenants**.
- 2 Navegue até o Gerenciamento de Tenants, clique em **ADICIONAR TENANT**.
- 3 Digite um nome de tenant e, em Detalhes do administrador, digite **Nome de usuário, Nome, Sobrenome, ID do e-mail** e **Senha** do Administrador de Tenants.
- 4 Clique em **Avançar**.
- 5 (Opcional) Na guia Detalhes do Diretório, escolha os diretórios do tenant primário que devem ser migrados para o novo tenant que está sendo criado.  
Você pode encontrar os nomes de diretório existentes listados na coluna de diretório.

- 6 Você pode selecionar qualquer diretório e clicar em **Avançar**.
  - a Aceitar para migrar diretórios lista todos os diretórios existentes do tenant primário. Somente o AD Sobre LDAP e o AD com diretórios IWA estão listados.
  - b Para migrar, selecione os diretórios.
  - c Digite as senhas necessárias para validação
  - d Clique em **Validar**. Quando a validação for bem-sucedida, clique em **Salvar e Avançar**.
- 7 Selecione os produtos que devem ser associados ao novo tenant. Para o vRealize Suite Lifecycle Manager 8.1 e versões mais recentes, o vRealize Automation 8.1 e versões mais recentes podem ser listados.

**Observação** Verifique se você considerou a recomendação dada para o certificado e o DNS.

- 8 Clique em **Salvar e Avançar**.
- 9 Clique em **Executar pré-verificação** para validar os detalhes do tenant e os detalhes do certificado.
  - Verificação de validação do nome do tenant – Para validar se o nome do tenant inserido corresponde aos critérios.
  - Verificação de Existência do Nome do Tenant: para validar se um tenant já existe.
  - A capacidade de acesso e a verificação de capacidade de resolução de FQDN do tenant do VMware Identity Manager
  - Verificação do certificado FQDN do tenant do VMware Identity Manager
  - A capacidade de acesso e a verificação de capacidade de resolução de FQDN do tenant do vRealize Automation
  - Verificação do certificado FQDN do tenant do vRealize Automation
- a Se as validações não forem bem-sucedidas e você quiser fazer alterações e, em seguida, retomar a operação de criação de tenants, clique em **Salvar e Sair**. O mesmo assistente pode ser aberto a qualquer momento para executar novamente a pré-verificação até a conclusão e continuar.
- b Se as validações de pré-verificação estão em verde, clique em **Salvar e Avançar**. Um resumo de toda a seleção será exibido.
- 10 Clique em **Avançar** e em **Criar Alterações do Tenant** após a leitura do resumo.

É possível exibir a criação de tenants na página **Detalhes da solicitação**. O VMware Identity Manager e tenants do vRealize Automation podem ser acessados através de seus FQDNs do tenant. Para obter mais informações, consulte [Gerenciamento de tenants no vRealize Suite Lifecycle Manager](#). Você pode fazer login no FQDN do tenant do VMware Identity Manager e no FQDN do tenant do vRealize Automation com as credenciais do administrador de tenants. O administrador de tenants do VMware Identity Manager também é o proprietário da organização em um novo vRealize Automation do tenant.

## Excluir um tenant

Excluir a operação do tenant exclui o tenant do VMware Identity Manager incluindo os recursos produzidos sob esse tenant. A partir do vRealize Suite Lifecycle Manager 8.1, a opção de excluir tenant só estará disponível para um tenant se não houver associações de produtos.

## Gerenciar tenants no Dia 2

Esta seção descreve as operações de Dia 2 de um tenant. Todas as operações disponíveis no assistente "Adicionar Tenant" estão disponíveis como uma operação individual de Dia 2.

### Gerenciar administradores de tenant

Quando tenants são criados, apenas um usuário local do VMware Identity Manager é criado, e esse usuário recebe permissões de administrador de tenant. É possível adicionar e gerenciar administradores de tenant em um estágio posterior quando necessário.

#### Gerenciar Administradores de Tenant – Adicionar Administradores de Tenant

Essa opção é usada para adicionar um novo usuário local no VMware Identity Manager e atribuir a permissão de administrador de tenant a ele.

- 1 Navegue até **Gerenciamento de Identidade e Tenants** e clique em **Gerenciamento de Tenant**.
- 2 Para adicionar um administrador, selecione o tenant.
- 3 Clique em **ADICIONAR ADMINISTRADOR DE TENANT**. A página Criar administrador de tenant é carregada
- 4 Insira os detalhes do novo administrador de tenant e clique em **Criar Administrador de Tenant**.

Após o envio, é criada uma solicitação cuja conclusão pode ser rastreada, e o usuário aparece na lista de administradores de tenant.

#### Gerenciar administradores de tenant - Pesquisar e atribuir

Essa opção é usada quando já existem usuários presentes no VMware Identity Manager sob o tenant em questão e eles exigem a permissão de administrador de tenant. A pesquisa pode localizar usuários locais do VMware Identity Manager e usuários do Active Directory sincronizados no tenant em questão. Vários usuários podem ser pesquisados e atribuídos à permissão de administrador de tenant. Para pesquisar usuários:

- 1 Navegue até **Gerenciamento de Identidade e Tenants** e clique em **Gerenciamento de Tenant**.
- 2 Para adicionar um administrador, selecione o tenant.
- 3 Clique em **PESQUISAR E ATRIBUIR**.
- 4 Quando todos os usuários estiverem selecionados, clique em **Atribuir Administrador de Tenant**.

Após o envio, é criada uma solicitação cuja conclusão pode ser rastreada, e o usuário aparece na lista de administradores de tenant.

## Associar produtos

Quando os tenants são criados, como uma operação de dia 2 em qualquer momento, você pode associar mais produtos. Para o vRealize Suite Lifecycle Manager 8.1 e versões posteriores, somente o vRealize Automation 8.1 e versões posteriores pode ser associado. A opção **Associações de Produtos** lista os produtos atuais associados ao tenant. Para adicionar mais associações, clique em **Adicionar Associação de Produtos**. Selecione o produto e verifique as recomendações fornecidas. Para o vRealize Automation 8.x, certifique-se de que os requisitos de Certificado e DNS sejam inseridos. Selecione os administradores de tenant na lista disponível. O administrador de tenant se torna o proprietário da organização do novo tenant do vRealize Automation. Execute a pré-verificação para validar suas entradas e clique em **Enviar**. Quando a solicitação for concluída, o produto associado aparecerá na lista **Associação de Produtos**.

## Migrar diretórios

O processo de migrar diretórios no dia 2 é semelhante ao assistente para **Adicionar Tenant**. A guia **Diretórios** na exibição do tenant lista os diretórios atuais presentes no tenant.

---

**Observação** Esses diretórios são somente leitura. O vRealize Suite Lifecycle Manager não permite o gerenciamento completo de diretórios para diretórios de subtenants. O gerenciamento de diretórios só está disponível para diretórios presentes no tenant primário.

---

Quando você clica em **Adicionar Diretórios**, todos os diretórios do tenant principal são recuperados. Selecione diretórios que devem ser migrados, valide-os e, em seguida, envie-os.

## Como usar a Migração de Tenant

A Migração de Tenant foi introduzida para migrar tenants e dados de tenant específicos para o VMware Identity Manager (agora renomeado como VMware Workspace ONE Access) usando o vRealize Suite Lifecycle Manager.

A Migração de Tenant é compatível com o vRealize Suite Lifecycle Manager 8.2 Patch 1 e versões posteriores. Ela envolve a coordenação próxima entre o VMware Identity Manager, o vRealize Suite Lifecycle Manager e o vRealize Automation.

O vRealize Suite Lifecycle Manager migra os seguintes dados do VMware Identity Manager no ambiente vRealize Automation 7 para o Ambiente Global do VMware Identity Manager versão 3.3.3 e versões posteriores:

- Tenants
- Diretórios
- Grupos personalizados
- Funções e conjunto de regras
- Atributos de usuários
- Políticas de acesso
- Intervalos de rede

- Configurações de IDP de terceiros

## Migrar o VMware Identity Manager

É possível migrar o VMware Identity Manager usando o vRealize Suite Lifecycle Manager.

### Pré-requisitos

- As informações de SMTP do tenant de origem devem ser configuradas no Ambiente Global do VMware Identity Manager. Essas informações são necessárias para receber instruções por e-mail para redefinir a senha de todos os usuários locais. Antes da migração do tenant, todos os usuários locais no tenant de origem devem ter IDs de e-mail válidos.
- Para a migração de grupo personalizada, você deve ativar a conexão remota do Ambiente Global do VMware Identity Manager com o banco de dados vRealize Automation 7.x. Consulte a [base de conhecimento 81219](#) para obter mais informações sobre como ativar a conexão remota.
- Certifique-se de ter o DNS configurado no vRealize Automation e no VMware Identity Manager.
- Certifique-se de que o ambiente de origem do vRealize Automation 7.x esteja em um estado íntegro e que os diretórios sejam sincronizados antes da migração de tenants.

### Procedimentos

- 1 No painel Meus Serviços do vRealize Suite Lifecycle Manager, clique em **Gerenciamento de Identidade e Tenants**.
- 2 Selecione **Gerenciamento de Tenants** e depois clique em **Migrações de Tenants**.
- 3 Leia as informações sobre Migração de Tenants do VMware Identity Manager e Mapeamento de Tenants do vRealize Automation e clique em **Continuar**.
- 4 Na guia Seleção do Ambiente, selecione o **Ambiente de Origem** e o **Ambiente de Destino**.  
Com base na sua seleção dos ambientes de origem e de destino, você pode visualizar uma representação em tabela dos tenants disponíveis no vRealize Automation de origem. Você também pode exibir o status dos tenants migrados ou mesclados no ambiente do vRealize Automation 8.
- 5 Clique em **Avançar**.

- 6 Na página Fluxo de Trabalho de Migração de Tenants, você pode visualizar o fluxo de trabalho de Migração de Tenants e Mesclagem de Tenants e compreender a correlação entre as duas operações.

O vRealize Suite Lifecycle Manager também cria o endpoint da versão 7.x ao adicionar um novo tenant no ambiente do vRealize Automation 8. Em Mesclagem de Tenants, os diretórios e tenants já foram criados no ambiente do vRealize Automation 8 de origem. O vRealize Suite Lifecycle Manager cria o endpoint da versão 7.x para os tenants existentes no ambiente do vRealize Automation 8, para que você possa migrar os grupos de negócios, a infraestrutura e outros tenants específicos no vRealize Automation.

- 7 Clique em **SALVAR E AVANÇAR** e leia a lista de etapas manuais que devem ser executadas para prosseguir com a migração. Marque a caixa de seleção para confirmar que você leu e verificou os pré-requisitos e as limitações.
- 8 Para especificar o Fluxo de Trabalho de Migração de Tenants, insira estes detalhes na guia Datalhes do Tenant.
  - a Selecione o **Tenant de Origem**.  
Os tenants de origem listados não são os tenants migrados ou mesclados.
  - b Insira o **Nome do Tenant**.
  - c Em Detalhes do administrador do tenant de destino, insira o **Nome de Usuário do Tenant de Destino**, o **Nome**, o **Sobrenome**, um **ID de E-mail** válido e uma **Senha**.

---

**Observação** Como a migração de um diretório é uma operação única, selecione todos os diretórios que devem ser migrados. Se os diretórios necessários não forem selecionados durante a migração, você deverá executar essa operação manualmente.
- 9 Clique em **SALVAR E AVANÇAR**.
- Para especificar um diretório que deve ser migrado do vRealize Automation versão 7 de origem para o tenant do vRealize Automation versão 8, selecione um desses diretórios na guia Migração de Diretório.
  - Diretório do Sistema: a seleção do Conector e a criação de uma senha não são necessárias.
  - Diretório JIT: a seleção do Conector e a criação de uma senha não são necessárias.
  - Active Directory via LDAP: selecione um Conector de destino do Windows ou do Linux e insira a Senha de Associação.
  - OpenLDAP: selecione um Conector de destino para Windows ou Linux e insira a Senha de Vinculação.

- Active Directory com IWA: somente é possível selecionar um conector de destino do Windows para o VMware Identity Manager versão 3.3.3. Digite a **Senha de associação** e a **Senha do administrador do domínio** necessárias para a migração.

#### Observação

- Para uma versão 3.3.5 ativada para FIPS do VMware Identity Manager, os usuários do AD e a senha de associação do usuário devem ter catorze caracteres.
- Como a migração de um diretório é uma operação única, selecione todos os diretórios que devem ser migrados. Se os diretórios necessários não forem selecionados durante a migração, você deverá executar essa operação manualmente.

10 Clique em **Validar**. Após uma validação bem-sucedida, clique em **SALVAR E AVANÇAR**.

11 Clique em **Executar Pré-verificação** para validar os detalhes do tenant e os detalhes do certificado. Clique em **SALVAR E AVANÇAR**.

12 Na guia Etapa de Resumo, é possível exibir o resumo das suas seleções.

13 Clique em **ENVIAR** se as suas validações tiverem sido bem-sucedidas.

Se as validações não forem bem-sucedidas e você quiser fazer alterações e, em seguida, retomar a operação de migração de tenants, clique em **SALVAR E SAIR**. O mesmo assistente pode ser aberto a qualquer momento para executar novamente a pré-verificação e continuar.

É possível exibir os detalhes da migração de tenants na página Detalhes da Solicitação. Os tenants do VMware Identity Manager e do vRealize Automation podem ser acessados por meio de seus FQDNs de tenant.

## Mesclar tenants

Na operação de Mesclagem de tenants, os diretórios e tenants já foram criados no ambiente do vRealize Automation 8 de destino.

O vRealize Suite Lifecycle Manager cria os endpoints do vRealize Automation 7.x para os tenants existentes no ambiente do vRealize Automation 8. Você pode migrar os grupos de negócios, a infraestrutura e outros tenants específicos no vRealize Automation.

#### Pré-requisitos

- O vRealize Automation 8.1 não exigia a aceitação de um certificado de origem durante a avaliação da migração. Para mesclar ou gerenciar o tenant usando vRealize Suite Lifecycle Manager, você pode excluir do vRealize Automation o ambiente de origem manualmente adicionado.
- Certifique-se de que os dados específicos do VMware Identity Manager sejam migrados para os dados de destino no Ambiente Global.

#### Procedimentos

1 No painel Meus Serviços do vRealize Suite Lifecycle Manager, clique em **Gerenciamento de Identidade e Tenants**.

- 2 Selecione **Gerenciamento de Tenants** e depois clique em **Migrações de Tenants**.
- 3 Leia as informações sobre Migração de Tenants do VMware Identity Manager e Mapeamento de Tenants do vRealize Automation e clique em **Continuar**.
- 4 Na guia Seleção de Ambiente, selecione o **Ambiente de Origem** e o **Ambiente de Destino**.

Com base na sua seleção dos ambientes de origem e de destino, você pode visualizar uma representação em tabela dos tenants disponíveis no vRealize Automation de origem. Você também pode exibir o status dos tenants migrados ou mesclados no ambiente do vRealize Automation 8.

- 5 Clique em **Avançar** e, na página Fluxo de Trabalho de Migração do Tenant, é possível exibir o fluxo de trabalho de Migração de Tenants e Mesclagem de Tenants.
- 6 Na guia Detalhes da Mesclagem, você pode selecionar um ou vários mapeamentos de tenants para o vRealize Automation 7.x e mesclá-los com tenants de destino iguais ou diferentes para o vRealize Automation 8.x.

Se você não puder visualizar o tenant de destino, realize uma sincronização de inventário ou uma associação de produtos para o tenant.

- 7 Clique em **Avançar** para visualizar o resumo de suas seleções na guia Etapa de Resumo.
- 8 Clique em **ENVIAR** se as suas validações tiverem sido bem-sucedidas.

---

**Observação** Se as validações não forem bem-sucedidas e você quiser fazer alterações e, em seguida, retomar a operação de mesclagem de tenants, clique em **SALVAR E SAIR**. O mesmo assistente pode ser aberto a qualquer momento para executar novamente a pré-verificação e continuar.

---

# Criar um ambiente no vRealize Suite Lifecycle Manager

3

Você pode criar um ambiente e instalar os produtos do vRealize Suite.

Para obter mais informações sobre produtos e versões compatíveis do vRealize Suite, consulte [Requisitos do sistema](#).

Este capítulo inclui os seguintes tópicos:

- Criar um novo ambiente de nuvem privada usando o assistente de instalação
- Importar um ambiente existente usando o Assistente de instalação
- Criar um ambiente de nuvem privada usando um arquivo de configuração
- Criação de ambientes no vRealize Cloud

## Criar um novo ambiente de nuvem privada usando o assistente de instalação

Você pode usar o assistente de instalação para criar um ambiente de nuvem privada e instalar produtos do vRealize Suite.

### Pré-requisitos

- Configure os binários do produto para os produtos a serem instalados. Consulte [Configurar binários de produto](#).
- Certifique-se de ter adicionado um vCenter Server ao centro de dados com credenciais válidas e que a solicitação esteja concluída.
- Gere um único certificado SAN com nomes de host para cada produto a ser instalado na guia Certificado na IU.
- Verifique se o sistema atende aos requisitos de hardware e software para cada um dos produtos do vRealize Suite que você deseja instalar. Consulte a seguinte documentação de produto para ver os requisitos do sistema.
  - [Documentação do vRealize Automation](#)
  - [Documentação do vRealize Business for Cloud](#)
  - [Documentação do vRealize Operations Manager](#)
  - [Documentação do vRealize Log Insight](#)

- O vRealize Automation SaltStack Config (anteriormente conhecido como Salt Stack Enterprise) oferece duas opções de configuração:
  - vRA integrado do vRealize Automation SaltStack Config: esta instalação é introduzida como parte do vRealize Automation SaltStack Config (SSC) 8.3.0 é uma configuração de nó único que não oferece suporte à configuração de vários nós nem opções para expandir verticalmente. Antes de instalar o vRA integrado do SaltStack Config, verifique se a versão suportada do vRealize Automation está instalada. Após a instalação do vRealize Automation, se vários tenants não estiverem ativados, a instância do SaltStack será associada ao tenant base do vRealize Automation. Quando vários tenants estão ativados no vRealize Automation, o vRA integrado do SaltStack Config se associa aos tenants recém-adicionados e continua com a instalação. Quando o vRealize Automation é importado, as instâncias do vRA integrado do SaltStack Config que estão associadas a vRealize Automation também são importadas.
  - vRealize Automation SaltStack Config autônomo: esta instalação não tem dependência sobre o vRealize Automation.

Para obter mais informações sobre como instalar e configurar o Salt Stack em um ambiente do vRealize Automation, consulte a *documentação do Salt Stack*.

Ao instalar o vRealize Automation SaltStack Config, você precisa das seguintes licenças.

- vRA integrado do vRealize Automation SaltStack Config: vRealize Automation Enterprise, vRealize Automation Advanced ou Suite.
- vRealize Automation SaltStack Config autônomo: licença do vRealize Automation Standard Plus.
- Se você estiver instalando o vRealize Automation, deverá atender aos seguintes pré-requisitos adicionais.
  - Configure o平衡ador de carga do vRealize Automation. Consulte [Balanceamento de carga do vRealize Automation](#).
  - Desative o segundo membro de cada pool no balanceador de carga do vRealize Automation. Você pode reativar esses membros após a conclusão da instalação.
  - O administrador da nuvem adicionou todos os nós IaaS e o servidor do banco de dados do Windows ao domínio.
  - O servidor do banco de dados do Windows e o IaaS atendem aos pré-requisitos do vRealize Automation. Consulte [Servidores Windows IaaS](#).

Adicione o usuário do domínio como parte da **Atribuição de direitos do usuário** em **Políticas de segurança local** para **para fazer logon como um serviço** e **fazer logon como um trabalho em lote**.

  - O usuário do domínio adicionou o servidor SQL ao domínio.
  - Adicione o usuário do domínio como parte da **Logins** lista de usuários do banco de dados SQL com o **sysadmin** privilégio.

- Instale o JRE mais recente (Java 1.8 ou posterior) e crie uma variável de ambiente `JAVA_HOME` em todos os nós do Windows.
- Instale o Microsoft .NET Framework 3.5.
- Instale o Microsoft .NET Framework 4.5.2 ou posterior.
  - Uma cópia do .NET está disponível em qualquer dispositivo do vRealize Automation: <https://vrealize-automation-appliance-fqdn:5480/installer/>  
Se você usa o Internet Explorer para fazer o download, verifique se a Configuração de Segurança Reforçada está desativada. Navegue para o `res://iesetup.dll/SoftAdmin.htm` no servidor Windows.
- Defina as configurações de **Controle de acesso do usuário** para **Nunca notificar** nas máquinas virtuais do Windows e no servidor do banco de dados.
- Tire um snapshot da máquina do banco de dados e de todas as máquinas Windows IaaS após a configuração e antes de acionar a implantação no vRealize Suite Lifecycle Manager.
- Configure um NSX Edge como Ativo e outro como Passivo para a máquina Windows. Para obter informações detalhadas sobre como configurar o balanceador de carga do NSX, consulte [Balanceamento de Carga da Plataforma de Gerenciamento de Nuvem na Região A](#).
- Em todas as máquinas Windows IaaS usadas na implantação do vRealize Automation, faça login na máquina Windows pelo menos uma vez como usuário do domínio. Se você não fizer login pelo menos uma vez nas máquinas do IaaS, o seguinte erro será exibido:
 

A chave privada é inválida: ocorreu um erro durante a decodificação da chave privada. O computador deve ser confiável para delegação, e o usuário atual deve ser configurado para permitir a delegação.
- Certifique-se de que os nós do IaaS não tenham componentes do vRealize Automation já instalados. Siga as etapas no artigo KB [58871](#) para desinstalar todos os componentes do vRealize Automation no nó do IaaS.
- Atualize a chave do registro em máquinas virtuais do servidor Windows e do banco de dados.
  - 1 Use o PowerShell padrão e execute o seguinte comando como administrador em todas as máquinas virtuais do Windows e do servidor do banco de dados: `Set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value "0"`
  - 2 Reinicialize a máquina virtual do Windows.
- Verifique se os valores TLS 1.0 e 1.1 não estão presentes no caminho de registro da máquina Windows IaaS `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`.

- Como alternativa, a pré-verificação de instalação do vRealize Automation fornece um script que pode ser executado em todos os servidores Windows e do banco de dados para realizar as operações acima.
- Se você estiver importando uma instalação existente do vRealize Operations Manager, defina uma senha raiz para essa instalação.

## Procedimentos

### 1 Instalar o VMware Identity Manager no vRealize Suite Lifecycle Manager

A partir do vRealize Suite Lifecycle Manager 8.4.1, o Federal Information Processing Standard (FIPS) e o modo não FIPS são compatíveis durante uma nova instalação do VMware Identity Manager versão 3.3.5. No entanto, não é possível alternar o modo FIPS após a instalação do VMware Identity Manager. Durante um upgrade do VMware Identity Manager, apenas o modo não FIPS é compatível. Para o vRealize Suite Lifecycle Manager versão 8.4 e posteriores, a instalação do VMware Identity Manager é opcional ao criar um ambiente.

### 2 Definir configurações de ambiente para uma nova nuvem privada

Defina as configurações de ambiente, como nome, senha e centro de dados para um ambiente de nuvem privada.

### 3 Instalar os produtos vRealize Suite

Selecione quais produtos vRealize Suite instalar no ambiente de nuvem privada.

### 4 Aceitar a seleção de EULA e licença

Aceite o contrato de licença do usuário final da VMware e digite a chave de licença.

### 5 Configurar detalhes do certificado

Para criar um ambiente, é possível usar o certificado existente.

### 6 Configurar detalhes da infraestrutura

Você pode configurar os detalhes da infraestrutura ao criar um ambiente.

### 7 Configurar detalhes de rede

Você pode configurar um ambiente ao estabelecer uma conexão de rede em um ambiente.

### 8 Configurar os detalhes do produto

Você pode visualizar e configurar os produtos que foram selecionados na criação do ambiente.

### 9 Configurar produtos do vRealize Suite para instalação

Configure os detalhes do produto para cada produto do vRealize Suite que você está instalando no ambiente de nuvem privada.

### 10 Validar detalhes do ambiente de nuvem privada

Configure os detalhes do vCenter Server, do cluster, da rede, do repositório de dados e do certificado para um novo ambiente de nuvem privada.

## 11 Confirmar as configurações de ambiente e instalação

Verifique se as configurações de ambiente e instalação estão corretas.

## Instalar o VMware Identity Manager no vRealize Suite Lifecycle Manager

A partir do vRealize Suite Lifecycle Manager 8.4.1, o Federal Information Processing Standard (FIPS) e o modo não FIPS são compatíveis durante uma nova instalação do VMware Identity Manager versão 3.3.5. No entanto, não é possível alternar o modo FIPS após a instalação do VMware Identity Manager. Durante um upgrade do VMware Identity Manager, apenas o modo não FIPS é compatível. Para o vRealize Suite Lifecycle Manager versão 8.4 e posteriores, a instalação do VMware Identity Manager é opcional ao criar um ambiente.

Nas versões anteriores, a instalação do VMware Identity Manager era obrigatória antes da criação de um ambiente no vRealize Suite Lifecycle Manager. Se uma instância do VMware Identity Manager não tiver sido criada, você será direcionado automaticamente para instalá-la na UI do vRealize Suite Lifecycle Manager.

Agora, você pode ativar ou desativar o botão de alternância do VMware Identity Manager.

---

**Observação** Antes de instalar ou importar o vRealize Automation 8.x, verifique se o ambiente global do VMware Identity Manager está presente no vRealize Suite Lifecycle Manager. Se o ambiente global não estiver instalado, você não poderá prosseguir com a implantação do vRealize Automation 8.x. Para instalar o ambiente global, ative o botão de alternância na página Criar Ambiente.

---

### Procedimentos

- 1 Navegue até o dashboard **Meus serviços** e clique em **Lifecycle Operations**.
- 2 Ative o botão de alternância **Instalar o Identity Manager** para instalar o VMware Identity Manager. Desative o de alternância **Instalar o Identity Manager** para prosseguir com qualquer outra instalação de produto do vRealize Suite.
- 3 Clique em **Criar ambiente** e digite os detalhes do ambiente.
  - a O nome do ambiente permanece como ambiente global por padrão.
  - b (Opcional) Insira a descrição do ambiente, que pode ter no máximo 1.024 caracteres.
  - c Adicione os detalhes da Senha.

---

**Observação** Se não houver senha listada, vá para o Locker e adicione uma senha.

---

- d Selecione o nome do **Centro de dados**.
- e Ative ou desative a barra de alternância da Configuração JSON, conforme necessário. Ao habilitar a configuração JSON, é possível colar o texto do arquivo JSON manualmente ou importar o arquivo do seu sistema local.
- f Clique em **Avançar**.

- 4 Se você tiver ativado a opção Instalar o Identity Manager na etapa 2, selecione **Nova Instalação** para instalar o VMware Identity Manager. Se a alternância estiver desativada, selecione a opção **Nova instalação** de outros produtos vRealize Suite.
- 5 Selecione a versão com suporte necessário para o VMware Identity Manager e clique em **Avançar**.

#### Resultados

Para obter mais informações sobre como configurar o VMware Identity Manager, consulte as seções em [Instalar os produtos vRealize Suite](#).

## Definir configurações de ambiente para uma nova nuvem privada

Defina as configurações de ambiente, como nome, senha e centro de dados para um ambiente de nuvem privada.

#### Procedimentos

- 1 Faça login no vRealize Suite Lifecycle Manager como administrador e clique em **Criar ambiente**.
- 2 No **Nome do ambiente**, digite um nome descritivo para o novo ambiente de nuvem privada. Esse nome deve ser exclusivo entre os ambientes nesta instância do vRealize Suite Lifecycle Manager.
- 3 (Opcional) Digite a **Descrição de ambiente** com no máximo 1.024 caracteres.
- 4 Digite uma **Senha do administrador padrão** e confirme-a.

A senha padrão deve ter no mínimo oito caracteres.

---

**Observação** A senha padrão não será aplicada à senha do aplicativo do vRealize Business for Cloud se a vRealize Business for Cloud for implantada em modo autônomo. No modo autônomo, as credenciais do aplicativo do vRealize Business for Cloud permanecem como admin/admin. Para integrar vRealize Business for Cloud com o vRealize Automation, adicione o vRealize Automation ao ambiente de nuvem privada antes ou ao mesmo tempo que adicionar o vRealize Business for Cloud.

---

- 5 Em **Centro de dados**, selecione um centro de dados existente para esse ambiente ou clique em **+** para adicionar um centro de dados para o vRealize Suite Lifecycle Manager.  
Para obter informações sobre como adicionar um centro de dados, consulte [Adicionar um Centro de dados a vRealize Suite Lifecycle Manager](#).
- 6 Ative ou desative a barra de alternância da Configuração JSON, conforme necessário. Ao habilitar a configuração JSON, é possível colar o texto do arquivo JSON manualmente ou importar o arquivo do seu sistema local.

- 7 (Opcional) Selecione **Participar do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do CEIP deste ambiente.

Esse produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. Detalhes sobre os dados coletados pelo CEIP e as finalidades para as quais eles são usados pela VMware são apresentados na Central de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

- 8 Clique em **Avançar**.

## Instalar os produtos vRealize Suite

Selecione quais produtos vRealize Suite instalar no ambiente de nuvem privada.

### Pré-requisitos

Verifique se você já tem as credenciais de centro de dados e de ambiente criadas.

### Procedimentos

- 1 Selecione se deseja instalar os produtos vRealize Suite por produto.
  - a Selecione quais produtos individuais vRealize Suite adicionar ao ambiente de nuvem privada e se deseja fazer uma nova instalação de cada produto ou importar e instalar o existente. Para cada nova instalação, selecione a **Versão** e o **Tamanho** do produto a ser implantados.
- 2 Clique em **Avançar**.

---

**Observação** Começar com a 8.2, o vRealize Lifecycle Manager permite disponibilidade contínua (CA) para o vRealize Operations Manager. Para mais informações, consulte [Disponibilidade contínua para vRealize Operations Manager](#).

---

## Aceitar a seleção de EULA e licença

Aceite o contrato de licença do usuário final da VMware e digite a chave de licença.

### Procedimentos

- 1 Leia o contrato de licença do usuário final, selecione **Concordo com os termos e condições** e clique em **Avançar**.

- 2 Na seção de licenças,
  - a Para selecionar as chaves de licença do locker, clique em **Selecionar** para abrir a lista de licenças aplicáveis aos produtos e versões selecionados. Caso contrário, selecione todas as chaves disponíveis na lista.
  - b Clique em **Adicionar**, para adicionar uma nova chave de licença ao locker de dentro do fluxo de instalação.
  - c Clique em **Validar** para validar a licença. Se várias chaves de licença estiverem disponíveis para um produto, esta ação sugerirá escolher uma por produto selecionado para a implantação.

Agora você pode visualizar as chaves de licença aplicáveis na tabela. A próxima etapa não será ativada até que todos os produtos implantados tenham a licença adequada correspondente selecionada.

---

**Observação** Licenças de produtos autônomos ou licenças vRealize Suite válidas ou uma combinação de ambos são permitidas para a implantação de produtos vRealize Suite Lifecycle Manager. A validação da licença não verifica a funcionalidade permitida pelas licenças em si. Portanto, selecione a chave de licença considerando a combinação dos produtos que serão implantados e sua interconectividade.

---

## Configurar detalhes do certificado

Para criar um ambiente, é possível usar o certificado existente.

### Pré-requisitos

Verifique se o certificado importado ou criado tem todos os endereços IP e nomes de domínio ou de host adicionados.

### Procedimentos

- 1 Em **Detalhes do certificado**, selecione o **certificado** no menu suspenso.

Se quiser fornecer detalhes do certificado no nível do produto, poderá especificar o certificado nas propriedades do produto de cada produto. A ação pode substituir os certificados selecionados no nível da infraestrutura.

- 2 Para criar um certificado, clique no sinal de mais.

Na janela **Adicionar certificado**, digite os detalhes necessários.

Campos	Descrição
Nome do certificado	Digite um nome de certificado válido.
Nome comum	Para identificar o certificado, digite um nome comum.
Organização	Digite o nome da organização.
Unidade organizacional	Digite a unidade da organização.
Código do país	Digite um código de país que deverá ter apenas dois caracteres.

Campos	Descrição
Localidade	Digite sua localidade.
Estado	Digite o estado.
Comprimento da chave	Selecione o comprimento da chave. Você pode selecionar 2.048 ou 4.096 bits.
Nome do domínio	Digite um nome de domínio válido.
Endereço IP	Digite o endereço IP no qual você está atribuindo o certificado.

- 3 Clique em **Gerar**.
- 4 Para importar um certificado existente, selecione a opção **Importar certificado**.

Campos	Descrição
Nome do certificado	Digite um nome de certificado válido.
Selecionar arquivo	<p>1 Clique em <b>Escolher arquivo</b>.</p> <p>2 Procure o arquivo PEM salvo.</p>
Frase-chave	Vá ao campo Frase-chave, digite <Cert- Senha> (se aplicável).
Digite a chave privada	Quando você carrega um arquivo PEM, os detalhes da chave privada são preenchidos automaticamente.
Digite a cadeia de certificados	Quando você carrega um arquivo PEM, os detalhes do certificado são preenchidos automaticamente.

- 5 Clique em **Importar**.
- 6 Clique em **Avançar**.

## Configurar detalhes da infraestrutura

Você pode configurar os detalhes da infraestrutura ao criar um ambiente.

### Pré-requisitos

Se o centro de dados selecionado não tiver um vCenter Server associado a ele, você deverá adicionar um vCenter Server.

### Procedimentos

- 1 Selecione um vCenter Server no menu suspenso.

**Observação** Deve haver pelo menos um vCenter Server associado a um centro de dados.

- 2 Selecione um **Cluster**.
- 3 Ao clicar em **Selecionar uma pasta**, todas as pastas associadas novCenter Server são listadas.

Se as pastas não forem exibidas, atualize a coleta de dados do vCenter na página de configurações do vRealize Suite Lifecycle Manager.

- 4 Para implantar a VM, clique em **Selecionar um pool de recursos**.

Todos os pools de recursos associados ao cluster selecionado são listados.

---

**Observação** Você pode selecionar um pool de recursos para implantar a VM. A seleção da pasta e do pool de recursos é opcional. Se você não especificar um pool de recursos, a VM será implantada no pool de recursos padrão raiz do cluster selecionado. Se você não especificar os detalhes da pasta para o vCenter Server e o pool de recursos, a implantação da VM será salva na pasta da VM padrão raiz do centro de dados no vCenter.

---

- 5 Selecione a **Rede**, o **Repositório de dados** e o **Modo de disco** necessários.

---

**Observação** A implantação do vRealize Operations Manager falha quando você fornece detalhes de infraestrutura incorretos, como detalhes incorretos de DNS ou de gateway sem executar uma pré-verificação durante a criação de um fluxo de ambiente. Se a implantação falhar, talvez você não veja a causa correta da falha na implantação usando a mensagem de erro ou de código exibida na IU do vRealize Suite Lifecycle Manager e não poderá continuar com essa implantação. Como resultado, você pode ter que excluir o cartão de ambiente do vRealize Suite Lifecycle Manager com todos os produtos ou nós que foram implantados como parte desse ambiente. Você pode executar a pré-verificação para que os problemas relacionados à infraestrutura sejam detectados e possam ser corrigidos antes de acionar a implantação.

---

- 6 Com o Lifecycle Manager 8.0, para integrar com o VMware Identity Manager, selecione o botão de alternância **Integrar com o Identity Manager**.

---

**Observação** O administrador de configuração padrão fornecido durante a instalação do VMware Identity Manager (ambiente global) será o administrador do produto também durante a integração com o VMware Identity Manager.

O VMware Identity Manager atua como um provedor de identidade e gerencia o SSO para os produtos vRealize Suite e o vRealize Suite Lifecycle Manager quando integrado com o vRealize Suite Lifecycle Manager. O SSO fornece um único conjunto de credenciais para acessar todos os aplicativos do vRealize Suite e vRealize Suite Lifecycle Manager. Com o SSO, você só precisa fazer o login uma vez para acessar perfeitamente todos os aplicativos do vRealize Suite.

---

- 7 Selecione **Usar Biblioteca de conteúdo** para usar OVFs hospedados na Biblioteca de conteúdo do vCenter, se houver uma latência de rede do vRealize Suite Lifecycle Manager para o vCenter Server

Copiar arquivos OVF e VMDK para implantação do vRealize Suite Lifecycle Manager para o vCenter Server pode levar mais tempo e levar a uma falha de implantação se houver uma latência de rede do vRealize Suite Lifecycle Manager para o vCenter Server de destino. As

bibliotecas de conteúdo no vCenter podem ser usadas para hospedar OVF, e o mesmo pode ser usado no vRealize Suite Lifecycle Manager para implantar produtos. Você pode realizar as etapas antes de acionar uma Sincronização de inventário do vCenter no vRealize Suite Lifecycle Manager:

- Para criar uma biblioteca de conteúdo, consulte [Criar biblioteca](#).
- Para importar uma biblioteca de conteúdo, consulte [Importar biblioteca](#).

O vRealize Suite Lifecycle Manager oferece suporte à implantação apenas de bibliotecas de conteúdo locais ou de editores.

**8** Para configurar o **Mapeamento Binário**, clique em **Avançar**.

## Configurar detalhes de mapeamento binário

Para criar um ambiente, selecione um ou mais binários para os produtos.

Certifique-se de mapear os itens de biblioteca corretos para os respectivos produtos. Se nenhum binário for selecionado para um produto, um padrão vRealize Suite Lifecycle Manager será usado para implementar o produto.

### Procedimentos

- 1 Clique em **+SELECIONAR ITENS DA BIBLIOTECA DE CONTEÚDO** para adicionar um item da biblioteca de conteúdo.
- 2 Você pode procurar um item da biblioteca ou abrir a árvore da biblioteca de conteúdo para selecionar um.

---

**Observação** Você pode adicionar vários produtos da biblioteca de conteúdo e associar produtos do conjunto conforme sua necessidade.

---

- 3 Clique em **Selecionar**.
- 4 Selecione um **Produto** correspondente ao item da biblioteca de conteúdo selecionado.

---

**Observação** vRealize Suite Lifecycle Manager valida o pacote OVF no item da biblioteca de conteúdo especificado correspondente ao produto selecionado.

---

- 5 Clique em **Avançar**.
- 
- Observação** Caso um item da biblioteca de conteúdo para um determinado nó precise ser implantado em um vCenter Server diferente, ele poderá ser selecionado em Configurações avançadas.
- 

### Resultados

Depois de enviar os mapas binários, clique em avançar para definir as configurações de rede.

## Configurar detalhes de rede

Você pode configurar um ambiente ao estabelecer uma conexão de rede em um ambiente.

## Pré-requisitos

- O conjunto de endereços IP estáticos é necessário para qualquer implantação de produto do vRealize Suite Lifecycle Manager. Isso se aplica para iniciar desde o vRealize Suite Lifecycle Manager 1.0 e superior.
- Verifique se você tem o Nome de Domínio mapeado para os endereços IP usados para a implantação.

## Procedimentos

- 1 Na página **Rede**, digite o endereço do **Gateway padrão**
- 2 Digite o endereço IP da **Máscara de rede**.
- 3 Digite o **Nome de domínio** e o **Caminho do domínio da pesquisa**.
- 4 Os Servidores DNS são listados automaticamente, mas, se não forem, clique em **Novo servidor** ou **Editar seleção do servidor**.
- 5 Selecione o modo de sincronização de Hora necessário:

Opção	Descrição
<b>Usar Servidor de Horário (NTP)</b>	Ao selecionar o Servidor NTP, você precisa selecionar o servidor de horário atribuído na lista NTP. Se um servidor NTP não for adicionado, para adicionar um, clique em <b>Configurações globais</b> . Em seguida, você será direcionado para a página de <b>Configurações</b> para adicionar um servidor NTP. Para obter mais informações, consulte <a href="#">Configurar Servidores NTP</a> .
<b>Usar Horário do Host</b>	Quando você selecionar o horário do Host, o ambiente prossiga com a hora do sistema.

- 6 Depois de adicionar servidores NTP, é possível clicar em **Selecionar servidores** para adicionar um NTP em um nível de Infraestrutura.
- 7 Selecione os servidores NTP na lista e poderá reordenar os servidores NTP com base na precedência clicando nas setas.

Ao selecionar um produto vRealize Suite, você pode configurar o uso desses servidores de Horário para o componente selecionado.

## Configurar os detalhes do produto

Você pode visualizar e configurar os produtos que foram selecionados na criação do ambiente.

## Procedimentos

- ◆ Em **Detalhes do produto**, selecione os produtos para uma nova instalação.

Produto	Função
vRealize Automation	<p>a Para monitorar a integridade do vRealize Automation, marque a caixa de seleção <b>Monitorar com vROps</b>.</p> <p>b Para gerenciar a carga de trabalho usando o balanceador de carga e recuperar recursos não utilizados do pool de recursos, marque a caixa de seleção <b>Posicionamento e recuperação da carga de trabalho</b>.</p> <p><b>Observação</b> Isso só está disponível para uma nova instalação na qual o vRealize Operations Manager monitora a integridade do vRealize Automation. A configuração entre produtos não é suportada por um ambiente existente.</p> <p>Se o vRealize Operations Manager estiver presente, você poderá integrar os produtos fora do LCM.</p> <p>A integração entre produtos do vRealize Automation com vRealize Operations Manager não é aplicável para uma importação do vRealize Automation. E só será aplicável se houver uma nova instalação do vRealize Automation.</p> <p>Você também pode realizar uma configuração entre produtos quando o vRealize Automation for o único produto e o vRealize Operations Manager fizer parte de um ambiente ou quando o vRealize Automation estiver sendo implantado com Importar ou Nova instalação do vRealize Operations Manager.</p>
	<p><b>Observação</b> A partir da versão 8.2, ao recém-instalar o vRealize Automation, selecione a caixa de seleção <b>Configurar pods internos e subconjuntos de serviços</b> e, em seguida, digitar os valores para <b>Intervalo de IPs do Cluster K8</b> e o <b>Intervalo de IPs do Serviço K8</b>.</p>
	<p><b>Observação</b> Na versão 8.3, o suporte ao Federal Information Processing Standard 140-2 (FIPS) é compatível com o vRealize Automation.</p>
	<p>c Selecione o Certificado do produto no menu suspenso.</p> <p>d (Opcional) Selecione LIGADO ou DESLIGADO para ativar ou desativar o Modo de conformidade FIPS.</p> <p>e Selecione o <b>modo de Sincronização de Tempo Aplicável</b>.</p> <p>f Selecione o <b>Servidor de horário (NTP)</b>. Para obter mais informações, consulte <a href="#">Configurar Servidores NTP</a>.</p> <p>g Se quiser configurar IPs virtuais do cluster, selecione as opções <b>Sim</b> ou <b>Não</b>.</p> <p>h (Opcional) Clique na caixa de seleção <b>Regra de antiafinidade/afinidade</b> para criar regras de host no vCenter para as VMs implantadas.</p>
	<p><b>Observação</b> Para obter mais informações sobre a criação de banco de dados, consulte <a href="#">Criar um novo ambiente de nuvem privada usando o assistente de instalação</a>.</p>
Configuração do vRealize Automation Salt Stack	<p>a Para Configuração do vRealize Automation Salt Stack do vRA integrado, selecione ID de Tenant no menu suspenso em <b>Propriedades do Produto</b>.</p>
■ vRA integrado	
■ Autônomo	

Produto	Função
	<p>b Para a configuração do vRealize Automation Salt Stack do vRA integrado e autônomo, digite o nome da <b>VM</b>, o <b>FQDN</b> e o <b>endereço IP virtual</b> em <b>Componentes</b>.</p>
	<p><b>Observação</b></p> <ul style="list-style-type: none"> <li>■ Para a configuração do vRA integrado do vRealize Automation SaltStack Config, você só pode executar uma instalação do SaltStack Config com um único nó de cada vez. Para a implementação do vRealize Automation junto com o vRA integrado do SaltStack Config, o ID de tenant é selecionado por padrão. Qualquer implantação adicional do SaltStack Config pode ser realizada com base no tenant como crescimento contínuo.</li> <li>■ Na versão 8.4, o Suporte FIPS (Federal Information Processing Standard 140-2) é compatível com o vRealize Automation SaltStack Config.</li> </ul>
vRealize Business for Cloud	<p>a Em <b>Propriedades do produto</b> digite o <b>Nome da VM</b>, o <b>Nome do host</b> e o <b>endereço IP</b>.</p>
vRealize Log Insight	<p><b>Observação</b> Na versão 8.3, o suporte ao Federal Information Processing Standard 140-2 (FIPS) é compatível com o vRealize Log Insight. Ele também é aceito como uma operação de Dia 2.</p> <p>a Selecione o tamanho do nó no menu suspenso.</p> <p>b (Opcional) Selecione LIGADO ou DESLIGADO para ativar ou desativar o Modo de conformidade FIPS.</p> <p>c Em <b>Configuração de balanceamento de carga integrado</b>, se você selecionar <b>Configurar IPs virtuais do cluster</b>, digite o <b>FQDN</b> e o <b>endereço IP virtual</b>.</p> <p>d Para adicionar mais nós, clique em <b>ADICIONAR NÓ</b>.</p> <p>e Selecione o <b>modo de Sincronização de horário</b> aplicável.</p> <p>f Em componentes, digite os detalhes do nó primário <b>vRLI</b>.</p> <p>g (Opcional) Clique na caixa de seleção <b>Regra de antiafinidade/afinidade</b> para criar regras de host no vCenter para as VMs implantadas.</p> <p>h (Opcional) Clique em <b>Adicionar componentes</b> para definir configurações adicionais.</p> <p>i Preencha os campos obrigatórios.</p>

Produto	Função
vRealize Operations Manager	<p><b>Observação</b> Na versão 8.3, o suporte ao Federal Information Processing Standard 140-2 (FIPS) é compatível com o vRealize Log Insight. Ele também é aceito como uma operação de Dia 2.</p> <ul style="list-style-type: none"> <li>a Em <b>Propriedades do produto</b>, selecione a <b>versão do TLS desativada</b> no menu suspenso.</li> <li>b (Opcional) Selecione LIGADO ou DESLIGADO para ativar ou desativar o Modo de conformidade FIPS.</li> <li>c Selecione o <b>Certificado</b> no menu suspenso.</li> <li>d (Opcional) Clique na caixa de seleção <b>Regra de antiafinidade/afinidade</b> para criar regras de host no vCenter para as VMs implantadas.</li> <li>e Adicione a <b>Senha do produto</b>.</li> <li>f (Opcional) Clique na caixa de seleção <b>Integrar com o Identity Manager</b>.</li> <li>g Selecione o <b>modo de Sincronização de horário</b> aplicável.</li> <li>h Para implantação baseada em disponibilidade contínua (CA), em <b>Componentes</b>, digite os detalhes de <b>Infraestrutura e Rede</b> para o domínio Witness.</li> <li>i Para implantação baseada em disponibilidade contínua (CA), digite os detalhes de <b>infraestrutura e rede</b> para o domínio de falha 1 e domínio de falha 2.</li> <li>j Se desejar adicionar nós de dados adicionais para um cluster, clique na guia <b>Adicionar componentes</b>.</li> </ul> <p><b>Observação</b> Se você selecionar <b>Usar configuração global</b>, os dados do campo serão preenchidos com base nas informações fornecidas na guia <b>Infraestrutura</b>. Você pode selecionar essa opção para Domínio Witness, Domínio de Falha 1 ou Domínio de Falha 2. Certifique-se de que cada domínio está em uma localização física diferente para que, se um domínio de falha errar, os nós do outro domínio de falha permaneçam ativos.</p> <ul style="list-style-type: none"> <li>k Se quiser adicionar coletores remotos, clique em <b>Adicionar grupo de coletores</b> e, em seguida, adicione os detalhes para os novos nós de coletor.</li> </ul>

Produto	Função
vRealize Network Insight	<ul style="list-style-type: none"> <li>a Em <b>Propriedades do produto</b>, selecione o tamanho do nó no menu suspenso.</li> <li>b Selecione o <b>modo de Sincronização de horário aplicável</b>.</li> <li>c Em componentes, digite a <b>plataforma vrni</b> e os detalhes do <b>coletor vrni</b>.</li> <li>d (Opcional) Clique na caixa de seleção <b>Regra de antiafinidade/afinidade</b> para criar regras de host no vCenter para as VMs implantadas.</li> </ul>
VMware Identity Manager	<ul style="list-style-type: none"> <li>a Em <b>Propriedades do Produto</b>, selecione o certificado no menu suspenso.</li> <li>b Selecione a senha do administrador no Locker.</li> <li>c Definir o nome de usuário administrador da configuração padrão. Ele será criado como usuário local no VMware Identity Manager e é usado para a integração do produto do vRealize Suite.</li> <li>d Selecione a senha para o usuário administrador da configuração padrão.</li> <li>e Verifique os <b>membros do grupo de sincronização</b>. Quando ativado, os membros dos grupos são sincronizados no Active Directory. Quando desativado, os nomes de grupo são sincronizados com o diretório, mas os membros do grupo não são sincronizados.</li> <li>f Para uma implantação de cluster, em IP Virtual do Cluster, digite <b>Cluster VIP FQDN</b>, que é usado para balancear a carga do aplicativo.</li> <li>g Para uma implantação de cluster, digite o IP do banco de dados usado internamente para proxy no postgres mestre (primário).</li> </ul> <p><b>Observação</b> Isso não é o mesmo que aquele usado para balancear a carga do aplicativo, e o endereço IP deve estar livre e disponível.</p> <ul style="list-style-type: none"> <li>h Em <b>Componentes</b> digite os detalhes do nó único ou do nó de cluster do VMware Identity Manager.</li> </ul>

## Configurar produtos do vRealize Suite para instalação

Configure os detalhes do produto para cada produto do vRealize Suite que você está instalando no ambiente de nuvem privada.

As guias de configuração aparecem apenas para os produtos que você selecionou para instalar. Você poderá acessar as propriedades avançadas se quiser atualizar as configurações avançadas, como adicionar vCenter diferente, ativar ou desativar o registro com o VMware Identity Manager e assim por diante.

## Procedimentos

1 Clique na caixa de seleção **vRealize Automation** para configurar os detalhes da instalação do vRealize Automation.

- a Se você selecionar o 8.x, digite o nome de domínio completo no formulário e o endereço IP do dispositivo do vRealize Automation.

O usuário do Windows deve ter direitos de administrador.

- b Digite o nome de domínio completo no formulário e o endereço IP do dispositivo do vRealize Automation .

Para obter mais informações sobre o dispositivo do vRealize Automation , consulte [Dispositivo do vRealize Automation](#) e o artigo [55706](#) da base de conhecimento.

O vRealize Automation 8.x inclui Padrão e Cluster.

2 O vRealize Automation SaltStack Config (anteriormente conhecido como Salt Stack Enterprise) disponibiliza duas opções de configuração:

- vRealize Automation SaltStack Config independente: essa configuração não tem dependência no vRealize Automation e a instalação prossegue sem integração com o VMware Identity Manager.
- vRealize Automation SaltStack Config integrado ao vRA: o vRealize Automation SaltStack Config pode ser instalado para cada tenant configurado no vRealize Automation proporcionando crescimento orgânico. A integração do VMware Identity Manager no Dia 0 e no Dia 2 é compatível com o vRealize Automation SaltStack Config versão 8.4.2 e posteriores integrado ao vRA.

3 Clique na caixa de seleção **vRealize Business for Cloud** para configurar os detalhes de instalação do vRealize Business for Cloud.

- a Selecione a **Moeda** a ser usada no menu suspenso.

- b (Opcional) Para adicionar um componente, clique no sinal de mais em **Adicionar componentes** e selecione o tipo de componente a ser adicionado.

- c Digite o nome do host no formulário de um nome de domínio completo e o endereço IP de cada componente.

Se o vRealize Automation não estiver presente no ambiente e não estiver sendo implantado juntamente com o vRealize Business for Cloud, especifique a propriedade **Implantar autônomo vRealize Business for Cloud** como verdadeira nas **Propriedades avançadas**. Se VMware Identity Manager estiver presente no vRealize Suite Lifecycle Manager, então o vRealize Business for Cloud será registrado no vIDM automaticamente.

Há apenas um tipo de implantação com o cluster de nó Padrão no vRealize Business for Cloud.

- 4 Clique na caixa de seleção **vRealize Operations** para configurar os detalhes da instalação do vRealize Operations Manager.
  - a Digite o endereço do servidor NTP.
  - b (Opcional) Clique no sinal de mais para **Adicionar componentes** e selecione o tipo de componente.
  - c Digite o nome do host no formulário de um nome de domínio completo e o endereço IP de cada componente.
  - d Selecione a **contagem de nós** ou o **tamanho do nó** para a implantação do **vRealize Operations**. O **vRealize Operations** recomenda que o número de nós de análise disponíveis para uma seleção dependa do tamanho do nó selecionado.

O tipo padrão de implantação para o vRealize Operations Manager é um tamanho de nó e uma contagem de nós.

- 5 Clique na caixa de seleção **vRealize Log Insight** para configurar os detalhes da instalação do vRealize Log Insight.
  - a (Opcional) Clique no sinal de mais em **Adicionar componentes** e selecione o tipo de componente a ser adicionado.
  - b Digite o nome do host no formulário de um nome de domínio completo e o endereço IP de cada componente.
  - c Se você estiver adicionando o IPS virtual do cluster, opcionalmente, digite as configurações do平衡ador de carga.
  - d Clique no ícone **Componentes +**, para adicionar e ativar qualquer uma das configurações durante a implantação.

O tipo de implantação disponível para o vRealize Log Insight é Autônomo e Cluster.

- 6 Clique na caixa de seleção **vRealize Network Insight** para configurar os detalhes da instalação do vRealize Network Insight.
  - a (Opcional) Clique no sinal de mais em **Adicionar componentes** e selecione o tipo de componente a ser adicionado.
  - b Selecione a chave de licença, se ela estiver registrada em My VMware, ou digite-a manualmente.
  - c Digite os detalhes da Infraestrutura e selecione os servidores NTP.
  - d Digite os detalhes da Rede e do Certificado.
  - e Em Detalhes do Produto, clique em **Adicionar** componente para adicionar uma plataforma ou um coletor do vRealize Network Insight. Essa opção depende dos tipos do vRealize Network Insight que você está selecionando inicialmente. Se você tiver selecionado um cluster do vRealize Network Insight, poderá ter duas plataformas e um coletor por padrão.

O tipo de implantação disponível para o vRealize Network Insight é Padrão e Cluster.

- 7 Clique em **Avançar**.

## Pontos a serem lembrados ao configurar o vRealize Automation

Você pode encontrar alguns problemas durante a realização de operações de dimensionamento horizontal, implantação, substituição de certificado e importação de brownfield do vRealize Automation 8.0.

- Quando a operação substituição de certificado do vRealize Automation 8.x falhar intermitentemente ao inicializar o cluster depois de substituir o certificado, tente repetir a substituição de certificado do vRealize Automation 8.0 com falha.
- A operação substituição de certificado do vRealize Automation 8.0 HA falha no cluster inicial após a substituição do certificado quando o certificado SAN tem nomes de host adicionais. Nesse caso, substitua o certificado HA do vRealize Automation por um certificado SAN que tenha os nomes de host necessários, como o nome de host do Balanceador de Carga do vRealize Automation e três nomes de host do vRealize Automation.
- Quando o dimensionamento horizontal do vRealize Automation 8.0 falha ao inicializar o cluster devido a bloqueios de liquibase, clique na opção para repetir na solicitação de dimensionamento horizontal do vRealize Automation 8.0 com falha para tentar novamente a etapa de inicialização do cluster.
- Verifique se o certificado SAN é usado em vez do certificado curinga para a implantação do vRealize Automation 8.0.
- Verifique para fornecer todos os quatro nomes de host, incluindo o nome de host de três nós do vRealize Automation e o nome de host do balanceador de carga do vRealize Automation no certificado SAN quando o certificado personalizado for usado.

## Disponibilidade contínua para vRealize Operations Manager

A disponibilidade contínua (CA) para vRealize Operations Manager evita a perda de dados durante uma falha de nó e garante a disponibilidade de vRealize Operations durante uma falha de localização física.

---

**Observação** Agora, o nó mestre é chamado de nó primário. O nó de réplica mestre agora é chamado de nó de réplica primário.

O CA separa o cluster vRealize Operations Manager em dois domínios de falha, estendendo entre vSphere clusters e protege o cluster de técnicas de análise contra a perda de um domínio de falha inteiro. Os dois domínios de falha são **Domínio de Falha 1** e **Domínio de Falha 2**. Por padrão, o nó primário e o nó de réplica são atribuídos ao **Domínio de Falha 1** e ao **Domínio de Falha 2**. Se o **Domínio de Falha 1** falhar, a funcionalidade não será interrompida, pois o outro nó de par garante que o incidente resulta em nenhuma perda de dados.

O **Nó testemunha** é o terceiro domínio de rede que existe de forma independente e identifica o particionamento de rede nos dois domínios de falha. Se a conectividade de rede entre os dois domínios de falha for perdida, o cluster se transformará em uma situação de dupla função, que é detectada pelo **Nó testemunha**. Imediatamente, um dos domínios com falha fica offline para evitar problemas de inconsistência de dados.

**Observação** É necessário um mínimo de três pares de nós para ativar o CA. Você pode adicionar no máximo 16 nós de dados, incluindo os nós primário e de réplica.

## Ativar a disponibilidade contínua para o vRealize Operations Manager

Agora você pode ativar a disponibilidade contínua (CA) para o vRealize Operations Manager .

### Pré-requisitos

Verifique se você já tem as credenciais de centro de dados e de ambiente criadas.

### Procedimentos

- 1 Em **Selecionar Produto**, selecione **vRealize Operations Manager** e, em seguida, selecione **Nova Instalação** .
- 2 Selecione a **Versão** no menu suspenso.
- 3 Selecione **CA** como a opção de **Disponibilidade**.
- 4 Selecione o **Tipo de implantação** no menu suspenso e, com base na seleção do **Tipo de implantação**, selecione o número de nós do menu suspenso de **Contador de nós** .

**Observação** Para obter mais informações sobre as diretrizes de disponibilidade contínua do vRealize Operations, consulte [KB 78495](#) .

## Validar detalhes do ambiente de nuvem privada

Configure os detalhes do vCenter Server, do cluster, da rede, do repositório de dados e do certificado para um novo ambiente de nuvem privada.

### Procedimentos

- 1 Digite os detalhes do vCenter Server em que você está instalando a vRealize Suite e os nomes do cluster, da rede e do repositório de dados a ser usados para este ambiente.  
O nome do vCenter Server deve estar no formato de um nome de domínio completo.
- 2 Selecione o formato do arquivo de disco e clique em **Avançar**.

Opção	Descrição
Reduzido	Use para avaliação e teste.
Expandido	Use o para ambientes de produção.

- 3 Digite o gateway padrão, o domínio, o caminho de pesquisa de domínio, o servidor DNS e os detalhes da máscara de rede para o ambiente e clique em **Avançar**.
- 4 Digite a chave da Frase-chave e a chave privada.
- 5 Digite a cadeia de certificados do certificado SAN para importar ou selecionar a opção **Certificado gerado** e clique em **Avançar**.  
Para obter informações sobre como gerar um certificado SAN consulte [Configurar certificado no Locker](#).
- 6 Digite os detalhes do produto para cada um dos produtos vRealize Suite que você selecionou para instalar fornecendo seu nome de host do Windows e endereço IP.
- 7 Clique em **PRE-VERIFICAÇÃO** para executar e validar as propriedades de cada um dos produtos vRealize Suite.

---

**Observação** Se a pré-verificação falhar, você deverá verificar as recomendações, reparar os problemas do produto selecionado e executar a pré-verificação novamente.

- 8 Leia o resumo e clique em **Enviar**.

## Validação de pré-verificação

Com base na validação pré-verificação, você pode alterar sua entrada a qualquer momento nas etapas anteriores e executar a verificação de pré-validação novamente.

### Como funciona a validação pré-verificação?

Quando você clica no botão **Executar Pré-verificação**, é gerado um relatório indicando se a pré-validação está no estado APROVADO ou REPROVADO. Portanto, com base no relatório, você pode modificar suas entradas fornecidas nas etapas anteriores e clicar no botão **REPETIR PRÉ VERIFICAÇÃO**. O relatório contém as seguintes informações:

- Status da verificação
- Nome da verificação
- Componente/Recurso em relação ao qual a verificação atual é executada.
- Descrição do resultado sobre a execução da verificação
- Recomendação, se houver FALHA ou AVISO

O relatório também gera um status codificado por cores:

- SÍMBOLO VERDE - APROVADO
- SÍMBOLO VERMELHO - REPROVADO
- SÍMBOLO AMARELO - AVISO
- SÍMBOLO VERDE CORRIGIDO - REMEDIADO E CORRIGIDO

Você só poderá prosseguir se a pré-validação for concluída com êxito. O progresso da solicitação de pré-validação pode ser rastreado na guia **Solicitação** por meio de uma solicitação criada com um nome VALIDATE\_CREATE\_ENVIRONMENT. Assim que a pré-validação for executada e o botão AVANÇAR estiver habilitado, você poderá ENVIAR a solicitação de implantação. Ao enviar, é possível pular a pré-validação. Por padrão, esse sinalizador está habilitado. Isso verifica se as pré-validações são executadas de qualquer maneira antes que a implantação seja acionada. Se quiser pular essa etapa, você poderá desmarcar o sinalizador e clicar em Enviar. A verificação de pré-validações não é executada novamente antes do início da implantação.

Se você clicar em **Enviar** com o sinalizador de pré-validação habilitado, uma solicitação com o nome VALIDATE\_AND\_CREATE\_ENVIRONMENT será criada. Se você apenas clicar em ENVIAR, desmarcando o sinalizador de pré-validação, uma solicitação com o nome CREATE\_ENVIRONMENT será criada. É possível acompanhar o andamento das solicitações de pré-validação na guia Solicitação que o vRealize Suite Lifecycle Manager fornece por padrão. Antes de executar uma pré-verificação no vRealize Automation, verifique se todas as VMs de componentes de IaaS estão se comunicando com o dispositivo Lifecycle Manager. Depois que você habilitar a pré-verificação e enviar o ambiente de criação, se a pré-verificação falhar, o usuário poderá retomar o assistente na página Solicitação com um estado de solicitação PRE\_VALIDATION\_FAILED. No relatório, se a falha for devida a uma credencial de IaaS incorreta, uma nova execução da pré-verificação ao atualizar a senha do Windows na página de Detalhes do produto ainda resultará na credencial de IaaS incorreta. Para corrigir isso, atualize a senha do Windows na página de detalhes do produto em cada nível de nó e execute novamente a pré-verificação.

Se a solicitação VALIDATE\_AND\_CREATE\_ENVIRONMENT falhar com um status PRE-VALIDATION-FAILED, você poderá validar suas entradas clicando no ícone da guia de ação. Isso direcionará você até um assistente no qual é possível modificar suas entradas e executar a PRÉ-VERIFICAÇÃO ou clicar em ENVIAR para implantação. Assim que a implantação for concluída, você poderá ver o último relatório de pré-validação executado. Essa opção está disponível na página de ambientes da página **Gerenciar Ambientes**. Você também pode exibir o último relatório executado em **Exibir Resultado da Última Pré-verificação em Ambiente**.

---

**Observação** A pré-verificação no LCM não leva em consideração o armazenamento estendido. Isso significa que, se a opção de armazenamento estendido for usada para implantar nós do vRealize Operations Manager usando o vRealize Suite Lifecycle Manager, a pré-verificação poderá ser bem-sucedida, mas a implantação propriamente dita ainda poderá falhar devido a espaço em disco insuficiente. Para obter mais informações, consulte o artigo da base de conhecimento [56365](#).

---

Apenas a ação **Automatizar verificações** é automatizada para executar um pré-requisito manual para o vRealize Suite no vRealize Suite Lifecycle Manager 1.2. Você pode BAIXAR O SCRIPT e executá-lo em todas as máquinas Windows. O zip contém um arquivo LeiaMe, que explica como executar o script. Essa etapa será obrigatória se você tiver selecionado o vRealize Automation como um dos produtos durante a criação de um ambiente.

## Agente do vRealize Suite Lifecycle Manager

O agente do vRealize Suite Lifecycle Manager é usado para executar pré-validações nos servidores Windows IaaS, mesmo antes de qualquer um dos componentes do vRealize Automation estarem instalados. O Agente do vRealize Suite Lifecycle Manager é executado como serviço do Windows. Ele registra o Windows Server como nó identificado com o dispositivo do vRealize Suite Lifecycle Manager. Cada Windows Server é registrado como nó no vRealize Suite Lifecycle Manager.

Quando o usuário inicia a pré-validação, o agente LCM é implantado e inicializado em todos os Windows Servers, juntamente com alguns metadados de configuração. Os binários do agente são mantidos em uma pasta padrão `C:\Program Files (x86)\VMware\LCM\Agent\` na máquina Windows.

Quando os binários do agente são empurrados, um serviço é iniciado com o nome de Serviço de agente do vRealize Suite Lifecycle Manager apontando para os binários que, em última análise, iniciam o agente. O agente trabalha com base em pull, onde pesquisa no dispositivo do vRealize Suite Lifecycle Manager para ver se há algum comando marcado para que o nó atual seja executado. Depois de receber um comando, o agente atualiza o comando de volta em cada alteração de status e, finalmente, atualiza o resultado após a conclusão. O serviço do agente é interrompido após uma pré-validação completa.

### Desinstalar o agente do vRealize Suite Lifecycle Manager

Como todos os servidores Windows usados para a pré-verificação são registrados exclusivamente, para usar o mesmo servidor em uma instância diferente do dispositivo do vRealize Suite Lifecycle Manager, o agente deve ser desinstalado. Para ver as etapas que serão desinstaladas, consulte a [base de conhecimento 58871](#).

## Substitua o certificado para o vRealize Automation

Você pode substituir o certificado SSL do serviço do site de gerenciamento se o seu certificado expirar ou se você estiver usando um certificado autoassinado e a política de segurança da sua empresa exigir que você use seus certificados SSL. Você protege o serviço do site de gerenciamento na porta 5480.

### Pré-requisitos

- Os novos certificados devem estar no formato PEM e a chave privada não pode ser criptografada. Por padrão, a chave privada e o certificado SSL do site de gerenciamento do appliance do vRealize Automation são armazenados em um arquivo PEM localizado em `/opt/vmware/etc/lighttpd/server.pem`.

### Procedimentos

- 1 Faça login usando o console do appliance ou SSH.
- 2 Faça backup do arquivo de certificado atual.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

- 3 Copie o novo certificado para seu dispositivo substituindo o conteúdo do arquivo `/opt/vmware/etc/lighttpd/server.pem` pelas informações do novo certificado.
- 4 Execute o comando a seguir para reiniciar o servidor lighttpd.  

```
service vami-lighttp restart
```
- 5 Execute o comando a seguir para reiniciar o serviço haproxy.  

```
service haproxy restart
```
- 6 Faça login no console de gerenciamento e verifique se o certificado foi substituído. Talvez seja necessário reiniciar o navegador.

---

**Observação** Por padrão, o vRealize Log Insight instala um certificado SSL autoassinado no dispositivo virtual. O vRealize Suite Lifecycle Manager gera certificados personalizados para produtos durante a criação do ambiente, mas a geração de certificados personalizados falha para o vRealize Log Insight. Para obter mais informações, consulte o artigo da base de conhecimento [55705](#).

---

## Confirmar as configurações de ambiente e instalação

Verifique se as configurações de ambiente e instalação estão corretas.

### Procedimentos

- 1 Verifique se as configurações de ambiente e instalação listadas estão corretas.
- 2 (Opcional) Clique em **Voltar** ou clique na página relevante no painel de navegação para alterar qualquer configuração.
- 3 (Opcional) Clique em **Exportar** para exportar um arquivo de configuração com todos os dados do produto e do usuário para esta nuvem privada.

Você pode usar o arquivo de configuração exportado para criar uma nuvem privada. Consulte [Criar um ambiente de nuvem privada usando um arquivo de configuração](#). Modifique o arquivo de configuração exportado conforme necessário antes de usá-lo para criar outra nuvem privada. As chaves privada e primária não são incluídas no arquivo de configuração exportado durante a implantação de um arquivo exportado. Você precisa inserir essas chaves manualmente.

Atualize/modifique o arquivo de configuração exportado conforme necessário antes de usá-lo para criar outra nuvem privada.

- 4 (Opcional) Selecione a guia Topologia para ter uma visualização de alto nível e um fluxo de integração dos produtos do vRealize Suite disponíveis no vRealize Suite Lifecycle Manager. Clique em um produto, grupo ou nó específicos do vRealize Suite para exibir as propriedades do produto ou do nó, como FQDN, endereço IP, rede, DNS e muito mais.
- 5 Clique em **Concluir**.

O vRealize Suite Lifecycle Manager cria o ambiente de nuvem privada e começa a instalar os produtos do vRealize Suite selecionados em segundo plano.

## Próximo passo

Para monitorar o progresso da instalação do produto, clique em **Página inicial**. O progresso da instalação é exibido em **Solicitações recentes**.

# Importar um ambiente existente usando o Assistente de instalação

Você pode usar o assistente de instalação para importar um ambiente de nuvem privada existente para um produto do vRealize Suite.

## Pré-requisitos

- Verifique se existe uma instância do vRealize Suite.
- Verifique se existe servidor de centro de dados.
- Verifique se você criou ou importou um certificado.

---

**Observação** O certificado não é obrigatório para importar um ambiente existente, no entanto, ele é obrigatório quando você seleciona a importação e a nova instalação em um fluxo ao criar um ambiente.

---

## Procedimentos

- 1 Faça login no vRealize Suite Lifecycle Manager como administrador do LCM ou administrador do LCM Cloud e clique em **Criar ambiente**.
- 2 Depois de inserir os campos de dados do ambiente, em cada um dos produtos vRealize Suite necessários, selecione **Importar** e clique na caixa de seleção do produto do vRealize Suite necessário na parte superior do nome do conjunto.
- 3 Clique em **Avançar**.
- 4 No assistente de instalação inicial, na página **Detalhes de produto**, atualize os detalhes e selecione todos os vCenters em que todos os componentes do produto estão instalados.

Se você selecionar uma combinação de importação e instalação para dois ou mais produtos ao criar um ambiente, digite os detalhes como uma nova Instalação do produto. Se você optar por um crescimento contínuo adicionando outro produto depois de criar um ambiente com a **Nova instalação** ou uma combinação de **Importar** e **New Instalar**, os detalhes no Assistente de instalação já estarão preenchidos. Prossiga e clique em **Avançar**. Se optar por um crescimento contínuo adicionando outro produto depois de criar um ambiente somente com **Importar**, os detalhes no Assistente de Instalação não serão previamente preenchidos. Afinal, você nunca forneceu esses detalhes ao criar o ambiente.

Depois de importar um produto para uma dimensionamento horizontal, você precisa adicionar um certificado. Para gerenciar um certificado, é necessário adicionar o certificado da guia Configurações e, em seguida, importar durante o dimensionamento horizontal.

- 5 Leia o resumo e clique em **Enviar**.

## Importar ambiente do VMware Identity Manager

Você pode importar uma instância do VMware Identity Manager para o vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 Após criar um ambiente na página Criar Ambiente, no cartão de produtos, marque a caixa de seleção do VMware Identity Manager.
- 2 Selecione **Importar** e clique em **Avançar**.
- 3 Digite um endereço de FQDN válido. Para importar um VMware Identity Manager agrupado em cluster use o nome do host do balanceador de carga.
- 4 Para importar o recurso multiempresa ativo do VMware Identity Manager, digite o **Nome do host do alias do tenant padrão**.
- 5 O Administrador do Sistema. As senhas de administrador, usuário SSH e raiz são listadas automaticamente.
- 6 Digite o **Nome de usuário administrador da configuração padrão**.
- 7 (Opcional) Marque a caixa **Sincronizar membros do grupo** e a lista vCenter Server.
- 8 Clique em **Avançar** e leia o resumo.
- 9 Clique em **Enviar**.

## Importar ambiente do vRealize Business for Cloud

Você pode importar uma instância do vRealize Business for Cloud para o vRealize Suite Lifecycle Manager.

### Pré-requisitos

Verifique se tem as credenciais de IP necessárias.

### Procedimentos

- 1 Após criar um ambiente em **Criar ambiente**, no cartão de produtos, marque a caixa de seleção do vRealize Business for Cloud.
- 2 Selecione **Importar** e clique em **Avançar**.
- 3 Digite o **FQDN** do vRealize Business for Cloud e selecione **Senha Raiz** nas entradas já existentes do Locker. Se a senha não existir no locker, você poderá criar entradas no locker. Clique em **Adicionar senha** no canto superior direito da janela.

- 4 Selecione o tipo de autenticação válido para a instância do vRealize Business for Cloud.
  - a Se um tipo de autenticação for autônomo, continue para selecionar um vCenter Server válido.
  - b Se um tipo de autenticação for do VMware Identity Manager, forneça o **FQDN** do Identity Manager, o **Nome do usuário** e selecione o **Nome do usuário administrador**.
  - c Se um tipo de autenticação for do vRealize Automation, forneça os detalhes relevantes para o **FQDN do vRA Cafe**, o **nome de usuário administrador do vRA Cafe SSO** e selecione **a senha do vRA Cafe SSO** da lista de senhas pré-preenchidas.
- 5 Selecione um vCenter Server válido na lista. Se a instância do vRealize Business for Cloud tiver nós do coletor espalhados por vários vCenters, então todos esses vCenters devem ser selecionados, caso contrário, a operação de importação falhará.
- 6 Clique em **Avançar** e leia o resumo.
- 7 Clique em **Enviar** para importar.

## Importar ambiente do vRealize Automation

Você pode importar uma instância existente do vRealize Automation.

Para criar um ambiente global, você ainda será solicitado a instalar o VMware Identity Manager se tiver ignorado essa etapa quando instalou o vRealize Suite Lifecycle Manager. Para instalar o VMware Identity Manager, consulte o [Instalar o VMware Identity Manager no vRealize Suite Lifecycle Manager](#). Para importar o ambiente brownfield do vRealize Automation 8.0, verifique se o VMware Identity Manager presente no vRealize Suite Lifecycle Manager é igual ao VMware Identity Manager registrado com o vRealize Automation. Certifique-se de usar o mesmo usuário administrador de configuração para o VMware Identity Manager e o vRealize Automation no vRealize Suite Lifecycle Manager.

### Pré-requisitos

Verifique se tem as credenciais de IP necessárias.

### Procedimentos

- 1 Após criar um ambiente na página Criar Ambiente, no cartão de produtos, marque a caixa de seleção do vRealize Automation.
- 2 Clique em **Importar** e clique em **Avançar**.
- 3 Em Detalhes do produto, digite os documentos necessários para configurar as propriedades do vRealize Automation, selecione **Importar** a versão.

- 4 Se você selecionou 8.x
  - a Forneça o Nome do host do nó Primário.
  - b Selecione **Senha raiz do nó primário**.

**Observação** Se os nós tiverem senhas diferentes, a solicitação de importação falhará.

Você pode fornecer a senha correta na nova tentativa de cada solicitação com falha.

- c Selecione o **vCenter Server** onde os nós do produto residem. Para mais informações na configuração do vRealize Automation, consulte [Pontos a serem lembrados ao configurar o vRealize Automation](#).
- 5 Se você selecionou 7.x
    - a Selecione uma instância do vCenter Server em vCenter Server.
    - b Clique em **Avançar** e leia o resumo.

Ao importar vRealize Automation, você precisa inserir detalhes específicos com relação ao vRealize Automation e ao aplicativo. A Senha do administrador tenant padrão é uma dessas entradas. O tenant padrão é definido como `vsphere.local` e não é editável. Você poderá encontrar o tenant bloqueado se o tenant do `vsphere.local` não estiver definido na configuração do vRealize Automation. Isso ocorre principalmente porque você pode ter optado por não configurar conteúdo de amostra pronto para uso durante a instalação. Você deve inserir a senha do administrador do sistema no campo **Senha do administrador de tenant padrão** e então, prosseguir com a importação.

- 6 Clique em **Enviar**.

## Importar a configuração da pilha de sal autônoma do VMware vRealize

Você pode importar uma instância do SaltStack Config do vRealize no vRealize Suite Lifecycle Manager.

### Pré-requisitos

Certifique-se de que tem as credenciais de IP necessárias.

### Procedimentos

- 1 Após criar um ambiente na página Criar Ambiente, no cartão de produtos, marque a caixa de seleção do SaltStack Config do vRealize Automation.
- 2 Selecione **Importar** e clique em **Avançar**.
- 3 Digite o **Endereço IP do Nó Mestre**, a **Raiz** e a **Senha do Administrador** do vRealize Automation SaltStack Config.
- 4 Selecione uma instância ativa do vCenter Server em vCenter Servers.
- 5 Clique em **Avançar** e leia o resumo.

- 6 Clique em **Enviar** para importar.

## Importar ambiente do vRealize Network Insight

Você pode importar um ambiente existente do vRealize Network Insight.

### Pré-requisitos

Verifique se há uma instância do vRealize Network Insight junto com suas credenciais de usuário disponíveis.

### Procedimentos

1 Depois de criar uma página **Criar Ambiente**, no cartão de produtos, marque a caixa de seleção do vRealize Network Insight.

2 Clique em **Importar** e clique em **Avançar**.

3 Na página Detalhes do Produto, digite o **nome de usuário administrador do vRNI**.

Todos os tokens de autorização e tokens CSRF são gerados usando-se o nome e a senha do usuário administrador.

4 Digite a **Senha do console** e a **Senha de suporte**.

Com as credenciais de usuário do console e de usuário de suporte, você pode executar comandos específicos do vRealize Network Insight e depurar o ambiente.

---

**Observação** A senha de suporte de todos os nós deve ser a mesma. Embora a importação de vRNI possa ser bem-sucedida, operações futuras como pré-verificação de atualização, atualização, atualização de senha e agrupação em clusters falharão. Você deve alterar a senha de suporte de todos os nós para uma única senha. Da mesma forma, as senhas de console de todos os nós devem ser as mesmas. No entanto, a senha de console e de suporte podem ser iguais em todos os nós. Se os nós tiverem senhas diferentes, a solicitação de importação falhará. Você pode fornecer a senha correta na nova tentativa de cada solicitação com falha.

5 Digite a **senha de administrador do vRNI** e o **endereço IP da plataforma**.

6 Selecione a instância do vCenter Server no menu suspenso e clique em **Avançar**.

7 Revise o resumo da solicitação e clique em **Enviar**.

### Exemplo: Exemplo de senha de console e de suporte

Em um cluster de 2 nós

- Plataforma: senha de suporte = VMware1! senha de console =Test@123
- Coletor: senha de suporte = VMware1! senha de console =Test@123

Em um cluster de 3 nós com 1 coletor

- Plataforma 1: senha de suporte = VMware1! senha de console =Test@123
- Plataforma 2: senha de suporte = VMware1! senha de console =Test@123

- Plataforma 3: senha de suporte = VMware1! senha de console =Test@123
- Coletor: senha de suporte = VMware1! senha de console =Test@123

## Importar ambiente do vRealize Operations Manager

Você pode importar uma instância do vRealize Operations Manager para o vRealize Suite Lifecycle Manager.

### Pré-requisitos

Verifique se tem as credenciais de IP necessárias.

### Procedimentos

- 1 Após criar um ambiente na página Criar Ambiente, no cartão de produtos, marque a caixa de seleção do vRealize Operations Manager.
- 2 Selecione **Importar** e clique em **Avançar**.
- 3 Digite o **Endereço IP do Nó Mestre**, a **Raiz** e a **Senha do Administrador** do vRealize Operations Manager.

**Observação** A senha de administrador deve ser somente para um usuário local, e não para um usuário com permissões de administrador.

**Observação** Se os nós tiverem senhas diferentes, a solicitação de importação falhará. Você pode fornecer a senha correta na nova tentativa de cada solicitação com falha.

**Observação** Agora, o nó mestre é chamado de nó primário.

- 4 Selecione uma instância do vCenter Server em **vCenter Servers**.
- 5 Clique em **Avançar** e leia o resumo.
- 6 Clique em **Enviar** para importar.

**Observação** Se você estiver importando uma instalação existente do vRealize Operations Manager, o SSH deverá estar habilitado para todos os nós e definidas senhas raiz em todos os nós do vRealize Operations Manager.

## Importar ambiente do vRealize Log Insight

Você pode importar uma instância do vRealize Log Insight para o vRealize Suite Lifecycle Manager.

### Pré-requisitos

Verifique se tem as credenciais de IP necessárias.

## Procedimentos

- 1 Após criar um ambiente na página **Criar ambiente**, no cartão do produto, marque a caixa de seleção do vRealize Log Insight.
- 2 Selecione **Importar** e clique em **Avançar**.
- 3 Digite o **FQDN do nó primário**, a **Raiz** e a **Senha de administrador** do vRealize Log Insight.

**Observação** A senha de administrador deve ser somente para um usuário local, e não para um usuário com permissões de administrador.

**Observação** Se os nós tiverem senhas diferentes, a solicitação de importação falhará. Você pode fornecer a senha correta na nova tentativa de cada solicitação com falha.

**Observação** Agora, o nó mestre é chamado de nó primário.

- 4 Selecione uma instância do vCenter Server em **vCenter Servers**.
- 5 Clique em **Avançar** e leia o resumo.
- 6 Clique em **Enviar** para importar.

## Criar um ambiente de nuvem privada usando um arquivo de configuração

É possível criar um ambiente de nuvem privada usando um arquivo de configuração do produto.

Saiba mais sobre [Nuvem privada](#), antes de configurar o ambiente.

Ao criar um ambiente utilizando uma especificação JSON, se o ID do Locker para as senhas for utilizado, você deverá certificar-se de usar o respectivo ID de locker do vRealize Suite Lifecycle Manager. Navegue para **Senhas do > Locker** e copie a ID da senha e use na especificação. Não é necessária nenhuma ação para uma senha de texto simples.

Ao usar a especificação JSON, certifique-se de atualizar todos os parâmetros nas configurações avançadas de cada nó conforme necessário. Se você não fizer a atualização, serão necessários os valores originais da especificação JSON.

## Pré-requisitos

- Defina as configurações do OVA dos produtos para instalar. Consulte [Configurar binários de produto](#).
- Verifique se você adicionou um vCenter ao centro de dados com credenciais válidas e se a solicitação foi concluída.

## Procedimentos

- 1 Faça login no vRealize Suite Lifecycle Manager como administrador e clique em **Criar ambiente**.

- 2 Em **Centro de dados**, selecione um centro de dados existente para esse ambiente ou clique em + para adicionar um centro de dados para o vRealize Suite Lifecycle Manager.  
Para obter informações sobre como adicionar um centro de dados, consulte [Adicionar um Centro de dados a vRealize Suite Lifecycle Manager](#).
- 3 Ative ou desative a barra de alternância da Configuração JSON, conforme necessário. Ao habilitar a configuração JSON, é possível colar o texto do arquivo JSON manualmente ou importar o arquivo do seu sistema local.
- 4 (Opcional) Selecione **Participar do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do CEIP deste ambiente.

Esse produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. Detalhes sobre os dados coletados pelo CEIP e as finalidades para as quais eles são usados pela VMware são apresentados na Central de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

- 5 Clique em **Usar recurso de alternância do arquivo de configuração**.
- 6 Cole o texto do arquivo JSON de configuração do produto na caixa de texto **JSON de configuração do produto** e clique em **Avançar**.

Você pode baixar o arquivo de configuração na página de resumo para criar um arquivo JSON para o produto ou a solução com as entradas mais recentes que foram fornecidas durante a configuração do ambiente.

O assistente de instalação de criação é instalado e os dados JSON são preenchidos. Você pode validar os dados antes de clicar em Enviar. Para obter mais informações sobre como obter um arquivo JSON de amostra, consulte o artigo KB [75255](#).

#### Próximo passo

Para monitorar o progresso da instalação do produto, clique no botão **Página inicial**. vRealize Suite Lifecycle Manager exibe o progresso da instalação para o ambiente em **Solicitações recentes** e na guia **Solicitações**.

## Criação de ambientes no vRealize Cloud

Quando quiser criar um ambiente híbrido e precisar que o software como serviço gerencie seus dados locais, você poderá usar o proxy de nuvem. O ambiente do Cloud Proxy permite que os serviços do software como serviço e do VMware Cloud se comuniquem com os serviços locais.

### Definir configurações de ambiente para um novo Cloud Proxy

Defina as configurações de ambiente, como nome, senha e centro de dados para um ambiente de novo proxy de nuvem.

## Procedimentos

- 1 Faça login no vRealize Suite Lifecycle Manager como administrador e clique em **vRealize Cloud**.
- 2 Clique em **Criar/implementar Cloud Proxy**.
- 3 No **Nome do ambiente**, digite um nome descritivo para o novo ambiente de proxy de nuvem.  
Esse nome deve ser exclusivo.
- 4 Digite a **Descrição de ambiente** com no máximo 1.024 caracteres.
- 5 Digite uma **Senha do administrador padrão** e confirme-a.  
A senha padrão deve ter no mínimo oito caracteres.
- 6 Em **Centro de dados**, selecione um centro de dados existente para esse ambiente ou clique em **+** para adicionar um centro de dados.
- 7 Ative ou desative a barra de alternância da Configuração JSON, conforme necessário. Ao habilitar a configuração JSON, é possível colar o texto do arquivo JSON manualmente ou importar o arquivo do seu sistema local.
- 8 Selecione **Participar do Programa de Aperfeiçoamento da Experiência do Cliente da VMware** para participar do CEIP deste ambiente.  
Esse produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. Detalhes sobre os dados coletados pelo CEIP e as finalidades para as quais eles são usados pela VMware são apresentados na Central de Confiança e Garantia, em <http://www.vmware.com/trustvmware/ceip.html>.

## Instalação de produtos Cloud Proxy

Os produtos de proxy de nuvem disponíveis são o proxy de extensibilidade de nuvem (proxy de nuvem do AVX), o VMware Cloud Services Data Collector (proxy de Nuvem de destino) e o proxy de nuvem do vRNI. Selecione quais produtos de proxy de nuvem instalar no ambiente de nuvem privada.

### Pré-requisitos

Verifique se você já tem as credenciais de centro de dados e de ambiente criadas.

## Procedimentos

- 1 Selecione os produtos Cloud Proxy a serem adicionados ao ambiente de nuvem privada e, em seguida, selecione **Tipo de instalação**. É possível realizar uma nova instalação de um produto ou importar de uma instalação existente do produto.
- 2 Selecione o **Tipo de implantação**.
- 3 Clique em **Avançar**.

## Próximo passo

Após instalar os produtos na nuvem, siga as etapas descritas em [Criar um novo ambiente de nuvem privada usando o assistente de instalação](#) para selecionar licença e EULA, configurando os detalhes do certificado e os detalhes da sua rede.

## Configuração de detalhes do produto de proxy de nuvem

Você pode visualizar e configurar os produtos proxy de nuvem selecionados durante a criação do ambiente.

Produto	Função
Instale o Proxy de extensibilidade de nuvem	<ol style="list-style-type: none"> <li>Em Propriedades do produto, digite o <b>Nome do proxy</b>.</li> <li>Selecione a <b>Senha do produto</b>.</li> <li>Selecione a <b>Chave de atualização</b>.</li> <li>Em Componentes, digite <b>Nome da VM, FQDN e Endereço IP</b>.</li> <li>Clique em <b>Avançar</b>.</li> </ol>
Instale o VMware Cloud Services Data Collector	<ol style="list-style-type: none"> <li>Em Propriedades do produto, digite o <b>Nome do proxy</b>.</li> <li>Marque as caixas de seleção <b>Cloud Assembly</b> e <b>Log Insight</b>, conforme aplicável.</li> <li>Selecione a <b>Senha do produto</b>.</li> <li>Selecione a <b>Chave de atualização</b>.</li> <li>Em Componentes, digite <b>Nome da VM, FQDN e Endereço IP</b>.</li> <li>Clique em <b>Avançar</b>.</li> </ol>
Instale o proxy de nuvem do vRNI	<ol style="list-style-type: none"> <li>Em Propriedades do produto, digite o <b>Nome do proxy</b>.</li> <li>Selecione a <b>Senha do produto</b>.</li> <li>Selecione a <b>Chave de atualização</b>.</li> <li>Para adicionar um novo servidor, insira os seguintes detalhes.             <ol style="list-style-type: none"> <li>Adicione o <b>Nome</b> e <b>FQDN/Endereço IP</b> do servidor.</li> <li>Clique em <b>Enviar</b>.</li> </ol> </li> <li>Para editar um servidor existente, insira os seguintes detalhes.             <ol style="list-style-type: none"> <li>Selecione os <b>Servidores NTP</b>.</li> <li>Clique em <b>Avançar</b>.</li> <li>Altere a Prioridade do servidor, conforme necessário.</li> <li>Clique em <b>Concluir</b>.</li> </ol> </li> <li>Em Componentes, digite <b>Nome da VM, FQDN e Endereço IP</b>.</li> <li>Clique em <b>Avançar</b>.</li> </ol>

## Próximo passo

Após configurar os detalhes do produto proxy de nuvem, siga as etapas listadas em [Criar um novo ambiente de nuvem privada usando o assistente de instalação](#) para validar os detalhes da nuvem e concluir o processo de instalação.

## Integração de assinaturas do vRealize Cloud Universal

vRealize Cloud Universal é um pacote de gerenciamento de nuvem SaaS que combina automação, operações e análises de log em uma única licença. Você pode começar a usar e gerenciar sua assinatura do vRealize Cloud Universal com a ajuda do vRealize Suite Lifecycle Manager e do vRealize Cloud Subscription Manager.

### Pré-requisitos

Para obter mais informações sobre como ativar sua licença de assinatura e começar com uma experiência de integração expressa, consulte o [Guia de integração do vRealize Cloud Universal](#). Para gerenciar as licenças do vRealize Cloud no vRealize Suite Lifecycle Manager, consulte [Gerenciar licenças do vRealize Cloud no vRealize Suite Lifecycle Manager](#).

# Como gerenciar ambientes no vRealize Suite Lifecycle Manager

4

Você pode gerenciar centros de dados, vCenters Servers e produtos vRealize Suite nos seus ambientes de nuvem privada.

Este capítulo inclui os seguintes tópicos:

- Operações do Dia 2 para o Ambiente Global no vRealize Suite Lifecycle Manager
- Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager
- Adicionar um produto a um ambiente de nuvem privada existente
- Adicionar uma Fonte de dados a um Ambiente de nuvem privada existente
- Gerenciar uma fonte de dados em um ambiente de nuvem privada já existente
- Atualizar senhas em massa para a fonte de dados
- Dimensionar horizontalmente o VMware Identity Manager
- Dimensionar horizontalmente produtos do vRealize Suite
- Expandir verticalmente produtos do vRealize Suite
- Exportar um arquivo de configuração do ambiente de nuvem privada
- Download de logs de produtos da nuvem privada
- Excluir um ambiente
- Gerenciar produtos vRealize Suite em uma nuvem privada
- Configurar o monitoramento de integridade da pilha de gerenciamento do vRealize Suite
- Como adicionar e gerenciar conteúdo do Marketplace

## Operações do Dia 2 para o Ambiente Global no vRealize Suite Lifecycle Manager

Um ambiente global é criado após uma instalação ou migração do vRealize Suite Lifecycle Manager. Um ambiente global exibe a instância do VMware Identity Manager como também a versão. Ao clicar em **Exibir detalhes** em um ambiente criado, você pode exibir as listas de informações primárias, secundárias e do conector do VMware Identity Manager que são usadas no vRealize Suite Lifecycle Manager. Você pode exibir as propriedades do produto para cada

cluster do VMware Identity Manager. Para exibir a lista de configurações entre produtos, clique em **Referências do produto**.

Após um upgrade, todos os produtos atualmente integrados ao ambiente global do VMware Identity Manager são mostrados nesta lista. O ambiente global do VMware Identity Manager, na página **Exibir detalhes**, contém as operações do Dia 2:

- Topologia - O Visualizador de topologia foi introduzido para ajudar você a visualizar a estrutura do grupo e dos nós, o vCenter e os detalhes de integração do produto entre o VMware Identity Manager e os produtos do vRealize Suite.
- Acionar a integridade do Cluster - Aciona uma verificação instantânea de integridade no cluster do VMware Identity Manager nos nós e fornece uma notificação na IU do vRealize Suite Lifecycle Manager.

Com base no status de integridade dos nós do cluster, a notificação "vIDM vPostgres Cluster Health" estará marcada como CRÍTICA ou OK. Para que a notificação seja precisa, verifique se o VMware Identity Manager pode se comunicar com todos os nós do VMware Identity Manager no cluster e se o inventário do ambiente global do VMware Identity Manager está atualizado no vRealize Suite Lifecycle Manager.

A verificação de integridade inclui verificação de status do serviço postgres, verificação de status do serviço pgpool (responsável pelo failover automático) e verificação de disponibilidade do IP delegado (IP do balanceador de carga de banco de dados) além das verificações básicas de disponibilidade do serviço do VMware Identity Manager.

Se o status estiver marcado como CRÍTICO, para solucionar problemas, será fornecido um link para o artigo KB [75080](#). Essa verificação de integridade também é executada a cada hora como um trabalho agendado no back-end e os status de integridade mais recentes são atualizados na notificação "vIDM vPostgres Cluster Health".

Se o VMware Identity Manager estiver agrupado em cluster através do vRealize Suite Lifecycle Manager, a opção LIGAR também poderá ser usada para remediar a integridade crítica do cluster.

- LIGAR - Liga os nós do VMware Identity Manager e garante que todos os serviços necessários sejam inicializados. Para uma instância agrupada em cluster do (vRealize Suite Lifecycle Manager agrupado em cluster do VMware Identity Manager), esta operação corrige qualquer inconsistência no cluster. Por exemplo, corrigindo o IP delegado (IP do balanceador de carga do banco de dados) e todos os atrasos de replicação nos nós secundários. Se o VMware Identity Manager estiver agrupado em cluster através do vRealize Suite Lifecycle Manager, use essa opção para qualquer caso de uso que envolva ligar o cluster como reversão, reinicialização, ligação de snapshot.
- DESLIGAR - Desativa todos os serviços do VMware Identity Manager desligando-os e também desativa os serviços responsáveis por um failover automático e seus componentes relacionados em uma implantação em cluster. Essa opção é fornecida para nó único e nó agrupado em cluster do VMware Identity Manager.

Se o VMware Identity Manager estiver agrupado em cluster através do vRealize Suite Lifecycle Manager, recomenda-se sempre usar essa opção para um cenário que envolva desligar o cluster, como reinicializar e desligar. Criar snapshot do VMware Identity Manager através do vRealize Suite Lifecycle Manager armazena o snapshot depois de desativar os serviços do VMware Identity Manager normalmente.

**Observação** Uma alteração no certificado do VMware Identity Manager exige a recuperação do certificado do VMware Identity Manager em todos os produtos ou serviços atualmente integrados a ele. Ao atualizar o certificado, você pode selecionar todos os produtos referenciados atualmente para ativar a recuperação. Para obter mais informações sobre referências de produtos, consulte [Referências do Produto](#). Para saber mais sobre os requisitos de hardware dependendo do número de usuários no diretório, consulte [Requisitos de configuração de sistema e rede](#).

## Redimensionar os recursos de hardware para o VMware Identity Manager

Este tópico descreve como redimensionar o hardware necessário para o VMware Identity Manager quando ele for implantado por meio do vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 Em Ambiente global VMware Identity Manager, clique nas reticências.
- 2 Clique em **Integridade de cluster**.

Após a conclusão da coleta da integridade do cluster, o status da integridade do vRealize Suite Lifecycle Manager é exibido na lista de notificações no canto superior direito da UI.

**Observação** Se o status estiver vermelho, para corrigir, clique em **Ligar** ou consulte o artigo do KB [75080](#).

- 3 Você pode expandir verticalmente até o tamanho necessário realizando uma expansão vertical. Para obter mais informações sobre expansão vertical, consulte [Expansão vertical de produtos do vRealize Suite](#).

### Resultados

Para obter mais informações sobre requisitos de hardware do VMware Identity Manager quando integrado com o vRealize Automation, consulte os requisitos de hardware na Arquitetura de Referência do vRealize Automation 8.1 no <https://docs.vmware.com/br/vRealize-Automation/8.1/reference-architecture/GUID-0332A798-93DA-435E-B45B-17A7233AE04F.html>. Para saber mais sobre os requisitos de hardware dependendo do número de usuários no diretório, consulte [Requisitos de configuração de sistema e rede](#).

## Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager

Agora você pode realizar as operações de Dia 2 no vRealize Suite Lifecycle Manager.

### Operações do Dia 2 para todos os produtos (exceto o VMware Identity Manager )

Os produtos do vRealize Suite nos ambientes consistem nos seguintes recursos:

- Topologia - o visualizador de topologia foi introduzido para ajudar você a visualizar a estrutura do nó e a compreender a integração entre diferentes produtos do vRealize Suite no vRealize Suite Lifecycle Manager. Você pode selecionar os produtos vRealize Suite e visualizar a versão, o certificado e os detalhes da licença. Você também pode selecionar o em um nó primário ou secundário para exibir o FQDN, o endereço IP, a rede, o DNS e outras propriedades do nó.
- Novo grupo de coletores - novos grupos de coletores estão disponíveis para o vRealize Operations Manager. O novo grupo de coletores permite adicionar novos coletores, agrupar os novos nós de coletor e mover os nós de coletor em novos grupos de coletores. Você pode adicionar coletor remoto e proxy de nuvem ao grupo de coletores.

---

**Observação** Recomenda-se não adicionar o proxy de nuvem a um grupo de coletores de coletores remotos. Para o proxy de nuvem, é possível criar um grupo de proxies de nuvem separado contendo somente proxies de nuvem.

- Confiar novamente com o Identity Manager – Sempre que o certificado do VMware Identity Manager é alterado, é necessário que todos os produtos/serviços atualmente integrados ao VMware Identity Manager confiem novamente no certificado do VMware Identity Manager. Embora a partir do vRealize Suite Lifecycle Manager 8.1, ao substituir ou alterar um certificado do VMware Identity Manager todos os produtos integrados ao VMware Identity Manager, cujos links estão nas Referências de Produto são definidos para confiar novamente de forma automática. Esse botão pode ser usado a qualquer momento quando você deseja confiar novamente no certificado do VMware Identity Manager de forma explícita no produto.

---

**Observação** Essa opção só é aplicável se um produto estiver integrado ao ambiente global do VMware Identity Manager e constar da tabela de Referências do Produto em ambiente global VMware Identity Manager.

- Registrar novamente com o Identity Manager – Quando os produtos se integram ao VMware Identity Manager, ele é registrado em um endpoint do VMware Identity Manager que, em geral, está com o FQDN do VMware Identity Manager. Sempre que o FQDN do VMware Identity Manager é alterado, há a necessidade de produtos ou serviços atualmente integrados ao VMware Identity Manager de se registrar novamente com o novo FQDN do VMware Identity Manager.

- Ativar Modo de conformidade FIPS – a partir do vRealize Suite Lifecycle Manager versão 8.3, o Modo de Conformidade FIPS está disponível para o vRealize Log Insight e o vRealize Operations Manager. Você pode ativar ou desativar o modo FIPS durante a implantação do produto. Como alternativa, você pode selecionar a opção Ativar conformidade com FIPS para a operação no nível do produto a partir da página Gerenciar ambientes.

**Observação** Se ativar o modo FIPS para um produto vRealize Suite, não poderá reverter e executá-lo em um modo não FIPS.

- Atualizar a configuração do NTP – a partir do vRealize Suite Lifecycle Manager 8.6, você pode atualizar os detalhes da configuração do NTP após implantar os produtos existentes do vRealize Suite. O Modo de sincronização de hora oferece duas opções de configuração, usando a hora do servidor NTP ou do host EXSi. Ao escolher o servidor NTP, você pode adicionar os novos detalhes do servidor ou editar os detalhes existentes do servidor, como o nome do servidor e o endereço FQDN/IP. Clique em Enviar para visualizar os novos detalhes do servidor NTP. Em Alterar prioridade do servidor NTP, é possível alterar a prioridade dos servidores. Em seguida, execute a pré-verificação para visualizar os detalhes das verificações aprovadas com êxito e as entradas com falha. Após clicar em Enviar, a solicitação de atualização de configuração do NTP é enviada.

## Operações do Dia 2 para implantação agrupada em cluster do vRealize Automation

Se o balanceador de carga do vRealize Automation for configurado de forma que o SSL seja encerrado no balanceador de carga, para qualquer alteração de certificado no balanceador de carga deverá ser feita a confiança novamente no vRealize Automation. Em uma implantação agrupada em cluster do vRealize Automation 8.x, você pode clicar em **Confiar novamente no balanceador de carga** que confiará novamente no certificado do balanceador de carga no vRealize Automation.

**Observação** Esta operação verifica principalmente o inventário agrupado em cluster do vRealize Suite Lifecycle Manager vRealize Automation 8.x antes de executar o confiar novamente. Os dados de inventário para o vRealize Automation 8.x agrupado em cluster terão um parâmetro - `O vra-va- SSL terminated at load-balancer` na seção **Cluster VIP** das propriedades do produto. O parâmetro decide se o SSL é encerrado no balanceador de carga do vRealize Automation ou não. Para todas as implantações de caixa de texto verde do vRealize Automation 8.x, essa opção é fornecida como uma entrada a ser preenchida pelo usuário e, para uma implantação de campo marrom existente, o valor do parâmetro é calculado automaticamente.

**Observação** As operações de início e encerramento também estão disponíveis para o vRealize Automation, o que ajuda a iniciar e desligar normalmente os serviços do vRealize Automation.

## Reconfigurar pods internos e sub-redes de serviço

A partir da 8.2, você pode modificar o intervalo de IPs usado internamente por serviços do vRealize Automation.

## Pré-requisitos

Verifique se um produto tem valores de intervalo de IPs internos existentes. Para obter informações sobre o serviço K8 e o intervalo de IPs de cluster, consulte [Instalar e configurar o vRealize Automation usando o vRealize Suite Lifecycle Manager Easy Installer para vRealize Automation e VMware Identity Manager](#).

## Procedimentos

- 1 Na página Ambiente, selecione um cartão de produto e clique nas reticências verticais.
- 2 Selecione **Reconfigurar pods internos e sub-redes de serviço**.
- 3 Digite valores do intervalo de IPs internos para o **Intervalo de IP do cluster K8 e Intervalo de IPs do serviço K8**.
- 4 Clique em **Avançar**.
- 5 Para validar as informações do intervalo de IPs, clique em **EXECUTAR PRÉ-VERIFICAÇÃO** e clique em **Concluir**.

## Adicionar um produto a um ambiente de nuvem privada existente

Se quiser alterar seu ambiente, é possível adicionar um produto a um ambiente existente.

O crescimento contínuo permite importar um vRealize Suite existente para um ambiente existente ou disparar uma nova implantação do produto para adicionar a um ambiente existente.

Um ambiente pode conter apenas uma instância de cada produto de vRealize Suite com suporte.

## Pré-requisitos

Ter um ambiente de nuvem privada existente vRealize Suite Lifecycle Manager que não contenha todos os produtos da vRealize Suite com suporte.

## Procedimentos

- 1 Clique em **Gerenciar Ambientes**.
- 2 Clique nas reticências (...) do ambiente e selecione **Adicionar Produtos** para executar o crescimento contínuo.
- 3 Selecione os produtos a adicionar e digite as informações de configuração necessárias.

## Adicionar uma Fonte de dados a um Ambiente de nuvem privada existente

É possível adicionar uma fonte de dados ao seu ambiente para coletar informações de rede.

## Pré-requisitos

Ter uma instância do vRealize Network Insight existente no vRealize Suite Lifecycle Manager.

## Procedimentos

- 1 Clique em **Gerenciar ambientes**.
- 2 Clique em **Exibir detalhes. dos Ambientes** onde você deverá adicionar a origem de dados.
- 3 Clique nas reticências (...) para o vRealize Network Insight e selecione **Adicionar Fonte de Dados**.
- 4 Digite os detalhes necessários e clique em **Enviar a solicitação**.

## Operações de dados com suporte pelo vRealize Network Insight

Você pode adicionar todos os tipos de fontes de dados que têm suporte pelo vRealize Network Insight.

Fonte de dados	Descrição
VMware vCenter	Você pode inserir as informações relacionadas ao vCenter nos campos fornecidos, juntamente com os detalhes do proxy.
VMware NSX Manager	Você pode inserir as informações relacionadas ao NSX Manager nos campos fornecidos, juntamente com os detalhes do proxy.
Roteadores e switches	Você pode inserir os detalhes de configuração do SNMP nos campos fornecidos clicando nas <b>Configurações avançadas</b> . <p><b>Observação</b> Você pode adicionar fontes de dados semelhantes para o vRealize Network Insight que são específicos de seus respectivos produtos ou funcionalidades.</p>

## Importar fontes de dados para o vRealize Suite Lifecycle Manager

Você pode importar fontes de dados em massa para o vRealize Network Insight por meio do vRealize Suite Lifecycle Manager. Esse recurso é útil quando o mesmo SNMP ou outras configurações têm que ser usados para vários switches. As configurações comuns juntamente com outros parâmetros variáveis, como endereço IP, precisam ser importadas no vRealize Suite Lifecycle Manager e provisionadas para o vRealize Network Insight. Com o vRealize Suite Lifecycle Manager 8.2, você pode importar fontes de dados, juntamente com a importação de uma instância do vRealize Network Insight.

## Pré-requisitos

Verifique se existe uma instância do vRealize Network Insight.

## Procedimentos

- 1 Em um ambiente do vRealize Network Insight, clique com o botão direito do mouse nas reticências verticais e selecione **Adicionar Fontes de Dados > Lote**.
- 2 Selecione o formato CSV ou JSON para importar as fontes de dados em um formato de relatório definido.

- 3 Clique em **SELECIONAR Arquivo** e, em seguida, selecione o arquivo JSON, clique em **Avançar**.
- 4 Clique em **Enviar a solicitação**.  
Para exibir o status da solicitação, exiba-o na página de Solicitação.
- 5 Para atualizar o arquivo CSV no formato necessário, clique em **Baixar modelo**.

## Gerenciar uma fonte de dados em um ambiente de nuvem privada já existente

A partir do vRealize Suite Lifecycle Manager 8.2, você pode editar ou excluir uma fonte de dados no seu ambiente.

### Pré-requisitos

Verifique se você criou uma fonte de dados do vRealize Network Insight no vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 No dashboard do vRealize Suite Lifecycle Manager 8.2, clique em **Gerenciar Ambientes**.
- 2 Na página Ambientes, selecione o cartão do produto vRealize Network Insight e clique em **Exibir Detalhes**.
- 3 Clique em **EDITAR FONTE DE DADOS** ou **EXCLUIR FONTE DE DADOS**, conforme aplicável.
  - a Se você clicar em **EXCLUIR FONTE DE DADOS**, a fonte de dados selecionada será excluída.

---

**Observação** Se uma fonte de dados for referenciada em qualquer outra fonte de dados do vRealize Suite Lifecycle Manager, não será possível excluí-la.

---

- b Se você clicar em **EDITAR FONTE DE DADOS**, poderá editar a VM do Coletor (Proxy), o nome de usuário da fonte de dados, a senha da fonte de dados e o apelido da fonte de dados.

---

**Observação** Por padrão, o endereço IP/FQDN da origem de dados fica desativado.

---

- 4 Clique em **ENVIAR**.

## Atualizar senhas em massa para a fonte de dados

Agora você pode realizar uma atualização de senhas em massa para senhas da fonte de dados.

### Pré-requisitos

Verifique se você já criou senhas da fonte de dados do vRealize Network Insight no vRealize Suite Lifecycle Manager.

## Procedimentos

- 1 Em Ambientes, selecione as fontes de dados que você deseja atualizar.
- 2 Selecione o cartão do produto vRealize Network Insight e clique nas reticências verticais do ambiente e, em seguida, clique em **Alterar Senha de Fontes de Dados**.
- 3 Em Selecionar Fontes de Dados, selecione as fontes de dados que você deseja atualizar e clique em **Avançar**.
- 4 Em Atualizar Credenciais, clique em **Nova Senha** para alterar a senha existente e, em seguida, clique em **Avançar**.

**Observação** Se você selecionar várias fontes de dados para atualizar senhas, a nova senha será aplicada em todas as fontes de dados selecionadas.

- 5 Em Pré-verificar detalhes, clique em **EXECUTAR PRÉ-VERIFICAÇÃO** para validar as novas senhas e, em seguida, clique em **Avançar**.
- 6 Em Resumo, você pode verificar as alterações para as fontes de dados.
- 7 Clique em **Concluir**.

**Observação** Quando você executa uma atualização de senha em massa e uma ou mais senhas não são atualizadas, a solicitação é marcada como concluída, mas você receberá uma mensagem de aviso para as senhas que não foram atualizadas. Clique nos detalhes da fonte de dados para obter informações e, em seguida, tente atualizar novamente as senhas em massa.

## Dimensionar horizontalmente o VMware Identity Manager

Você pode aumentar a opção de HA no VMware Identity Manager com um ou três nós para gerenciar o VMware Identity Manager.

- Certifique-se de tirar snapshots de nós do VMware Identity Manager antes de realizar operações de dimensionamento horizontal. O cluster do VMware Identity Manager é sempre três nós, incluindo um nó já existente.
- Verifique se há um certificado já adicionado ao Locker e realize também a substituição do certificado no nó autônomo do VMware Identity Manager. O certificado também deve ter entradas SAN de todos os três nós ou do certificado curinga. Para obter informações sobre a substituição de certificado, consulte [Substituir certificados de produtos vRealize Suite Lifecycle Manager](#).
- Não há suporte para o dimensionamento horizontal quando você implanta o cluster do VMware Identity Manager por meio do vRealize Suite Lifecycle Manager.

**Observação** Se você aplicar o patch da [Base de Conhecimento 87185](#) em um dispositivo de nó único e, em seguida, realizar operações de dimensionamento horizontal para o cluster, siga a [Base de Conhecimento 87185](#) para aplicar o patch nos nós dimensionados horizontalmente.

## Pré-requisitos

Para ações de substituição de certificado e cluster do VMware Identity Manager, certifique-se de tirar um snapshot dos nós do VMware Identity Manager.

## Procedimentos

- 1 Navegue para **Ambientes**, na página do ambiente e clique em **Adicionar Componente**.
- 2 Insira os detalhes de **Infraestrutura** e clique em **Avançar**.
- 3 Insira os detalhes de **Rede** e clique em **Avançar**.  
Verifique se o nó primário e os componentes adicionais usam o mesmo gateway padrão e se eles estão conectados uns aos outros.
- 4 Nas propriedades do produto, os detalhes do certificado são preenchidos automaticamente.
- 5 A guia Componentes tem duas opções. Portanto, você pode selecionar **Obter snapshot do produto** e **Reter o snapshot obtido do produto**. Se **Obter snapshot do produto** for definido como verdade, o snapshot será obtido antes de iniciar o dimensionamento horizontal e poderá ser revertido ao estado inicial durante uma falha de dimensionamento horizontal, o snapshot será obtido com o prefixo LCM\_AUTOGENERATED. Se **Reter o snapshot obtido do produto** for definido como verdade, ele poderá ser retido.

---

**Observação** A ação de Reversão de snapshot está disponível para a solicitação de dimensionamento horizontal com falha na página Solicitações.

---

- 6 Insira o nome do host do平衡ador de carga.
- 7 Digite um endereço IP delegado.

---

**Observação** O endereço IP delegado é usado internamente como proxy para o postgres principal (primário) e deve estar livre ou com um endereço IP disponível. Esse não é igual ao usado para balancear a carga do aplicativo.

---

**Observação** Você pode adicionar dois componentes do tipo secundário e fornecer FQDN e endereço IP. Recomenda-se que um cluster VMware Identity Manager contenha três nós atrás de um平衡ador de carga.

---

- 8 Clique em e execute a pré-verificação.
- 9 Clique em **Enviar**.

---

**Observação** É muito importante reiniciar o dispositivo, caso contrário, ocorre uma falha no procedimento de dimensionamento horizontal com o erro não é possível encontrar o certificado raiz. Os erros ocorrem devido a um problema no produto existente depois que você substitui os certificados para reiniciar o dispositivo.

---

## Verificação de integridade agendada

Assim que o VMware Identity Manager for agrupado em cluster, uma verificação de integridade agendada será registrada. Essa verificação agendada é realizada de hora em hora e pode aparecer uma notificação sobre o status geral de integridade do cluster postgres. A partir da versão 8.4, você também pode exibir o status de integridade do cluster no cartão do ambiente VMware Identity Manager.

Várias verificações importantes sob uma perspectiva do cluster postgres exigem atenção.

- 1 Acessibilidade de nós do VMware Identity Manager no vRealize Suite Lifecycle Manager.
- 2 Delegar atribuição IP a qualquer um dos nós do cluster.
- 3 Existência de nó primário do Postgres.
- 4 Nós do postgres com atraso de replicação.
- 5 Nós do Postgres sendo marcados como inoperante no cluster.
- 6 Existência de nó primário de pgpool.
- 7 Pgpool em execução em todos os nós.

Todas as verificações acima são capturadas e as mensagens de descrição apropriadas são exibidas na notificação que aparece com uma mensagem como o status de integridade do cluster postgres vIDM é crítico. Para obter mais informações sobre as etapas, consulte o artigo [75080](#) da base de conhecimento.

Se todas as verificações forem validadas, o vRealize Suite Lifecycle Manager que fornece um status de integridade do cluster, enviará uma notificação com uma mensagem como o status de integridade do cluster postgres vIDM está ok. Em uma operação de Dia 2, você pode clicar em Disparar a integridade do cluster no Ambiente Global para o VMware Identity Manager além de agendar a verificação de integridade por hora. Para obter mais informações sobre como disparar a integridade do cluster, consulte [Operações do Dia 2 para o Ambiente Global no vRealize Suite Lifecycle Manager](#).

Como operação de Dia 2, a Verificação de integridade do cluster em pausa é introduzido para pausar as notificações de integridade ao solucionar problemas, como o gerenciamento de senhas do VMware Identity Manager, a substituição de certificados, problemas relacionados à atualização e muito mais. Ao realizar uma verificação por hora ou durante uma manutenção, você pode clicar na **Verificação de integridade do cluster em pausa** e, em seguida, clicar em **Enviar** para pausar as notificações de integridade. Quando essas funções estão ativas e funcionando, você pode retomar a verificação de integridade no cartão do produto do ambiente.

## Dimensionar horizontalmente o VMware Identity Manager habilitado para tenant

Um VMware Identity Manager habilitado para tenant só pode ser acessado por meio de FQDNs de tenant, dimensionando horizontalmente um VMware Identity Manager habilitado para tenant

de um único nó para um cluster de três nós atrás de um平衡ador de carga que requer alterações nos requisitos de DNS e certificado.

Todos os FQDNs de tenant do VMware Identity Manager devem apontar agora para o endereço IP do balanceador de carga em vez de um único endereço IP de nó do VMware Identity Manager. E o certificado do balanceador de carga do VMware Identity Manager deve conter todos os FQDNs de tenant. Para obter mais informações sobre os requisitos de certificados e DNS obrigatórios, consulte [Modelo de multilocação](#)

As mesmas recomendações são fornecidas como pré-requisito manual para seleção antes do dimensionamento horizontal do ambiente global do VMware Identity Manager a partir da interface de usuário do vRealize Suite Lifecycle Manager. Para obter mais informações sobre FQDNs de Tenant, consulte [Modelo de multilocação](#).

## Dimensionar horizontalmente o Conector do Windows

Você pode optar por dimensionar horizontalmente um conector do Windows.

### Pré-requisitos

Siga estes pré-requisitos para um sistema do Windows no qual o conector será instalado.

- A versão do JRE com suporte está entre a atualização 8 181 e a atualização 8 251.
- A versão do .NET Framework com suporte é 4.6.0.
- As versões com suporte do Windows Server são 2012 R2, 2016 e 2019.
- Um sistema Windows exclusivo é necessário para a migração e deve estar conectado a um servidor de domínio.

### Procedimentos

- 1 Navegue até **Ambientes** na página de ambientes e clique em **Adicionar Componentes**.
- 2 Insira os detalhes de **Infraestrutura** e clique em **Avançar**.
- 3 Insira os detalhes de **Rede** e clique em **Avançar**.  
Verifique se o nó primário e os componentes adicionais usam o mesmo gateway padrão e se eles estão conectados uns aos outros.
- 4 Nas propriedades do produto, os detalhes do certificado são preenchidos automaticamente.
- 5 Na guia Componentes, selecione **Conector do Windows**.
  - a Insira o **Nome da VM Windows**
  - b Insira o **FQDN**.
  - c Insira um **Nome de conector** do Windows definido pelo usuário, em seguida, selecione a **Senha de administrador do conector**.
  - d Insira os detalhes de **Administrador de Domínio**.
- 6 Clique em e execute a pré-verificação.

- 7 Clique em **Enviar**.

## Dimensionar horizontalmente produtos do vRealize Suite

Você pode adicionar componentes ao seu produto para efetuar uma configuração de vários nós para formar um cluster.

### Pré-requisitos

O vRealize Suite Lifecycle Manager não permite que você adicione um componente de um produto até que o mapeamento do certificado desse produto seja criado no locker. Quando você substitui o certificado do vRealize Automation usando o novo certificado adicionado ao locker, o novo certificado contém entradas de host adicionais para novos componentes que devem ser adicionados como parte do dimensionamento horizontal. Depois de importar ou criar um certificado no locker, aplique esse certificado no produto e, somente então, os componentes adicionais estarão visíveis no produto.

Para mapear o certificado do produto no Locker, importe o certificado do produto no Locker e acione a sincronização de inventário para esse produto. Isso cria uma referência desse produto com o certificado no locker. Isso se aplica a um cenário de importação.

Verifique se o certificado foi substituído no produto cujo certificado contém todos os nomes de host dos componentes do produto, incluindo o nome do host do Balanceador de Carga e novos nomes de host adicionados de um componente adicional que também é especificado. Para obter mais informações sobre a substituição de certificados, consulte [Substituir certificados de produtos vRealize Suite Lifecycle Manager](#). Para obter mais informações sobre balanceador de carga, consulte [Balanceamento de carga do vRealize Automation](#).

### Procedimentos

- 1 No cartão de ambiente, selecione um produto, clique nas reticências verticais e selecione **Adicionar Componente**.

Para um ambiente importado, insira manualmente as caixas de texto para o produto selecionado.

---

**Observação** Às vezes, o dimensionamento horizontal de produtos com patch do vRealize Suite Lifecycle Manager pode falhar. Isso ocorre devido à falha de ingresso no cluster causada pela incompatibilidade de versão nos dispositivos do produto. Você pode baixar e usar o OVA correspondente ao patch. Quando você clica em Adicionar Componente, aparece uma mensagem de aviso indicando se o OVA necessário para dimensionar horizontalmente o produto com patches está disponível ou não no vRealize Suite Lifecycle Manager. O pacote OVA necessário pode ser baixado do Portal My VMware para o dispositivo do vRealize Suite Lifecycle Manager e mapeado. Você pode baixar e mapear os binários do produto com patches. Para obter mais informações sobre como baixar os binários de produtos com patches, consulte [Configurar os binários de produtos com patch](#).

---

- 2 Em detalhes de **Infra**, selecione **vCenter Server**, **Cluster**, **Rede**, **Datastore** e **Formato de disco** necessários nos menus suspensos.
- 3 Selecione o modo **Sincronização de Tempo Aplicável** e clique em **Avançar**.
- 4 Em detalhes de **Rede**, se o ambiente for recém-criado, as caixas de texto serão preenchidas automaticamente. Se o ambiente for importado, insira manualmente as caixas de texto.
- 5 Clique em **Avançar**.
- 6 Selecione o modo **Sincronização de hora aplicável** e, na seção de componentes, selecione o nó.

A configuração avançada fornece mais informações sobre como configurar o nó selecionado em um cluster. Para um ambiente importado no 2.0 no qual um produto é dimensionado horizontalmente, certifique-se de que o certificado fornecido seja certificado de nó primário, já que a pré-verificação corresponde ao certificado do nó primário. Para ambientes de versões anteriores do vRealize Suite Lifecycle Manager, você pode adicionar o certificado mais antigo durante um dimensionamento horizontal clicando no botão **Adicionar**. Isso preenche os dados do certificado mais antigos das propriedades de infraestrutura do ambiente.

- 7 A guia Componentes tem duas opções. Portanto, você pode selecionar **Obter snapshot do produto** e **Reter o snapshot obtido do produto**. Se **Obter snapshot do produto** for definido como verdade, o snapshot será obtido antes de iniciar o dimensionamento horizontal e poderá ser revertido ao estado inicial durante uma falha de dimensionamento horizontal, o snapshot será obtido com o prefixo LCM\_AUTOGENERATED. Se **Reter o snapshot obtido do produto** for definido como verdade, ele poderá ser retido.

---

**Observação** A ação de Reversão de snapshot está disponível para a solicitação de dimensionamento horizontal com falha na página Solicitações.

---

- 8 Em **Componente > Propriedades do produto**, selecione as caixas de texto necessárias.

O campo desta seção varia para diferentes produtos.

Nome do produto.	Componentes
vRealize Automation 7.x.	<ul style="list-style-type: none"> <li>■ vra-server-secondary</li> <li>■ iaas-web</li> <li>■ iaas-manager-passive</li> <li>■ iaas-dem-orchestrator</li> <li>■ iaas-dem-worker</li> <li>■ proxy-agent-vsphere</li> </ul>
vRealize Automation 8.x	Secundário
vRealize Operations Manager	<ul style="list-style-type: none"> <li>■ Dados</li> <li>■ Coletor remoto</li> </ul>
vRealize Business for Cloud	Coletor VRB

Nome do produto.	Componentes
vRealize Log Insight	Trabalhador VRLI
vRealize Network Insight	<ul style="list-style-type: none"> <li>■ Plataforma vRNI</li> <li>■ Coletor vRNI</li> </ul>

9 Insira as caixas de texto necessárias, clique em **Avançar** e execute a **Pré-verificação**.

10 Leia o resumo e clique em **Enviar**.

## Dimensionar horizontalmente o vRealize Automation ativado para tenant

O vRealize Automation habilitado para tenant só pode ser acessado por meio de FQDNs de tenant do vRealize Automation, o dimensionamento horizontal de um vRealize Automation habilitado para tenant de um único nó para um cluster de três nós atrás de um balanceador de carga requer alterações nos requisitos de DNS e certificado.

Para obter mais informações sobre FQDNs de Tenant, consulte [Modelo de multilocação](#). Após o dimensionamento horizontal, os tenants do vRealize Automation deverão ser acessados por meio de FQDNs e DNS de tenants do balanceador de carga, e as alterações de certificados deverão ser feitas conforme o necessário. As mesmas recomendações são mostradas ao usuário como pré-requisito manual a ser cuidado antes de dimensionar o vRealize Automation 8.x na interface do usuário do vRealize Suite Lifecycle Manager.

## Expandir verticalmente produtos do vRealize Suite

A expansão vertical foi apresentada para aumentar a RAM, a capacidade do disco ou as vCPUs nos nós de um cluster. Os nós de um cluster são agrupados, e cada grupo consiste em nós de tamanhos iguais. Um produto pode ter um único grupo ou vários grupos e, se os tamanhos dos nós variarem entre os diferentes grupos, será possível expandir verticalmente para padronizar os tamanhos dos nós.

As operações do Dia 2 incluem a operação de expansão vertical para gerenciar ambientes e evitar qualquer degradação de desempenho. A expansão vertical é compatível com o vRealize Log Insight, o vRealize Automation, o vRealize Operations, o vRealize Network Insight e o VMware Identity Manager. Você pode aumentar a capacidade de armazenamento de um produto expandindo verticalmente o tamanho atual e adicionando um disco com a capacidade necessária.

### Pré-requisitos

Verifique se você já tem um ambiente de nuvem privada no vRealize Suite Lifecycle Manager que contenha produtos do vRealize Suite compatíveis.

### Procedimentos

- 1 No painel vRealize Suite Lifecycle Manager, clique em **Gerenciar Ambientes**.
- 2 Clique em **Exibir Detalhes** para ambiente global ou um produto do vRealize Suite.

- 3 Clique nas reticências (...) para a operação do nível de produto e, em seguida, selecione **Expansão Vertical**.
- 4 Na janela pop-up **Prosseguir para a expansão vertical**, clique em **Disparar a sincronização de inventário**.
- 5 Clique em **Prosseguir** quando a sincronização de inventário estiver concluída.
- 6 Selecione o **Tipo de nó** e clique em **Avançar**.
- 7 Em **Detalhes da expansão vertical**, selecione **Expandir o tamanho verticalmente** no menu suspenso. Você pode selecionar o **Tamanho de disco adicional** (opcional).
- 8 Em Configurações Avançadas, selecione o datastore apropriado para os nós a partir dos menus suspensos e, em seguida, clique em **Avançar**.
- 9 Clique em **EXECUTAR PRÉ-VERIFICAÇÃO**.

**Observação** Se a validação for bem-sucedida, será exibida uma mensagem de validação bem-sucedida. Se você vir uma mensagem de erro, siga as instruções fornecidas na guia **Recomendações** e clique em **EXECUTAR PRÉ-VERIFICAÇÃO NOVAMENTE**.

- 10 Quando a validação for bem-sucedida, clique **Enviar** para exibir os detalhes da sua solicitação.

#### Observação

- Para o VMware Identity Manager (vIDM), a opção de implantação do vIDM padrão e o tamanho especificado do vRealize Automation de 8 CPU e 16 GB de memória são compatíveis. Para aumentar a capacidade de armazenamento do espaço em disco adicional fornecido para o vIDM 3.3.2, 70% pode ser atribuído a /db e 30% a /var. Para aumentar a capacidade de armazenamento do espaço em disco adicional fornecido para o vIDM 3.3.3, 70% pode ser atribuído a /db e 30% a /opt.
- Os parâmetros `requiredCpuCount` e `requiredMemory` são os parâmetros gerais de CPU e memória disponíveis para um nó.
- Para produtos vRealize Suite, você fornece o tamanho do disco extra para aumentar a capacidade. O parâmetro `requiredCapacity` adiciona um disco extra à capacidade disponível.
  - No vRealize Automation, selecione o disco necessário para expansão e escolha quanto expandir o disco existente.
- Se você estiver instalando o vRealize Automation, implemente o vIDM com o tamanho sugerido para o vRealize Automation.
- Para o VMware Identity Manager versão 3.3.3 ou posteriores, é necessária uma conexão com a Internet para realizar a operação de expansão vertical. Se não estiver conectado à Internet e quiser realizar a operação de expansão vertical off-line, instale os pacotes separados que estão em [packages.vmware.com](http://packages.vmware.com).

## Exportar um arquivo de configuração do ambiente de nuvem privada

Você pode exportar um arquivo de configuração do ambiente de nuvem privada para reutilizar a configuração de uma implantação para implantações futuras de ambiente.

Se qualquer fonte de dados for adicionada ao ambiente do vRealize Network Insight, a exportação do arquivo de configuração desse ambiente terá detalhes da fonte de dados. O arquivo de configuração pode ser usado para criar um novo ambiente do vRealize Network Insight e as fontes de dados serão adicionadas automaticamente.

### Procedimentos

- 1 Clique em **Gerenciar Ambientes**.
- 2 Clique nas reticências (...) para o ambiente e selecione **Exportar Configuração**.
- 3 Selecione o tipo de arquivo de configuração a ser exportado do **Simples** ou **Avançado**, com base em suas necessidades
- 4 Clique em **Salvar arquivo** e clique em **OK**.

Anteriormente, o recurso exportar arquivo de configuração estava disponível no nível do ambiente LCM. A partir do vRealize Suite Lifecycle Manager o 1.3, você pode exportar o arquivo de configuração no nível do produto também para o produto selecionado.

O arquivo de configuração é baixado no local de download padrão do seu navegador.

### Próximo passo

Use o arquivo de configuração para criar novos ambientes de nuvem privada. Consulte [Criar um ambiente de nuvem privada usando um arquivo de configuração](#).

## Download de logs de produtos da nuvem privada

Você pode baixar pacotes de arquivos de log de produto para compartilhar com o suporte da VMware.

### Procedimentos

- 1 Clique em **Gerenciar Ambientes**.
- 2 Clique nas reticências (...) para o ambiente e selecione **Baixar Logs**.

---

**Observação** Ao clicar em Baixar Logs, na página Gerenciar Ambientes no vRealize Suite Lifecycle Manager, o link para baixar o pacote de suporte não é exibido. Para obter mais informações, consulte o artigo KB [55744](#).

---

### Resultados

Os logs baixados são armazenados /data/support-bundle dentro do dispositivo do vRealize Suite LCM.

## Excluir um ambiente

Você pode excluir um ambiente existente do vRealize Suite Lifecycle Manager e não de produtos individuais. Não é possível selecionar um produto específico em um ambiente a excluir.

É possível excluir implantações de ambiente bem-sucedidas e com falha. É possível excluir ambientes que não foram implantados ou excluir um ambiente iniciado.

---

**Observação** É possível editar um ambiente existente em andamento ou com falha no estado de implantação no vRealize Suite Lifecycle Manager. Em Ambientes, selecione qualquer cartão de produto, clique nas reticências verticais para o produto escolhido e selecione Editar detalhes do ambiente para editar o ambiente. Você tem a opção de editar o nome do ambiente ou a descrição do ambiente. No entanto, não é possível editar o ambiente para ambiente global.

---

A instalação do VMware Identity Manager é opcional ao criar um ambiente. Se você excluir um ambiente do VMware Identity Manager:

- O vRealize Automation 8.x não pode ser instalado nem importado.
- Você não pode usar o VMware Identity Manager como uma fonte de autenticação para o vRealize Suite Lifecycle Manager.
- Não é possível acessar o gerenciamento de identidade e tenant. O usuário e o gerenciamento do Active Directory tornam-se inacessíveis. As funções e os mapeamentos de usuário existentes do VMware Identity Manager do vRealize Suite Lifecycle Manager foram removidos.

### Procedimentos

- 1 Clique em **Gerenciar ambientes** para excluir um ambiente instalado com êxito ou excluir uma implantação de ambiente com falha listada em **Solicitações recentes** na página Inicial.
- 2 Clique nos três pontos no canto superior direito do ícone do ambiente e selecione **Excluir ambiente**.
- 3 (Opcional) Selecione **Excluir máquinas virtuais relacionadas do vCenter** para excluir todas as máquinas virtuais associadas a este ambiente do vCenter server.  
Se você não selecionar essa opção, todas as máquinas virtuais associadas a esse ambiente permanecerão no vCenter após a exclusão do ambiente do vRealize Suite Lifecycle Manager.
- 4 (Opcional) Selecione **Excluir máquinas Windows relacionadas** para excluir máquinas Windows associadas a este ambiente do vRealize Automation.  
Essa opção estará disponível somente nas versões 7.x do vRealize Suite Lifecycle Manager se você optar por excluir todas as máquinas virtuais relacionadas do vCenter. Certifique-se de confirmar essa ação antes de continuar.

- 5 Selecione **Excluir máquinas virtuais relacionadas do vCenter** para excluir as máquinas virtuais associadas ao ambiente.

Essa opção estará disponível somente se você tiver uma máquina virtual associada a um ambiente no vCenter Server. Se selecionado, as máquinas virtuais associadas ao ambiente também serão excluídas do vCenter Server. Se não estiver selecionado, apenas o registro desse ambiente será excluído do inventário do vRealize Suite Lifecycle Manager.

- 6 Clique em **EXCLUIR**.
- 7 Se você optar por excluir as máquinas virtuais associadas ao ambiente, verifique se a lista de máquinas virtuais a serem excluídas está correta e clique em **CONFIRMAR EXCLUSÃO**.

Os nomes das máquinas virtuais IaaS não são exibidos nesta lista.

---

**Observação** Se a operação de exclusão falhar, uma opção Excluir ambiente do vRealize Suite Lifecycle Manager será ativada no cartão do ambiente. Essa ação exclui o ambiente do vRealize Suite Lifecycle Manager, e você pode excluir as VMs manualmente do vCenter Server. Para importação de brownfield, se você não conseguir adicionar uma lista do vCenter, a caixa de diálogo de confirmação de exclusão do ambiente não mostrará a lista de VM naquele vCenter em particular e você deverá fazer a limpeza manualmente. Para um crescimento orgânico, o cartão do ambiente da página inicial de atividades recentes não é excluído ou esmaecido.

---

- 8 Clique em **FECHAR**.

#### Resultados

O ambiente é removido do vRealize Suite Lifecycle Manager.

#### Próximo passo

Você pode visualizar o progresso da operação de exclusão na página **Solicitações**.

## Gerenciar produtos vRealize Suite em uma nuvem privada

Você pode usar o VMware vRealize Suite Lifecycle Manager para fazer upgrades e aplicar patches de produtos vRealize Suite e para baixar logs de produtos.

- [Criação e configuração de um snapshot do produto](#)

Agora você pode criar e gerenciar o snapshot de um produto para salvar o estado do produto em um determinado point-in-time.

- [Sincronização de inventário no vRealize Suite Lifecycle Manager](#)

Se você tiver atualizado qualquer configuração fora do vRealize Suite Lifecycle Manager, os produtos gerenciados a partir do vRealize Suite Lifecycle Manager estarão fora de sincronia. Para atualizar a configuração, você deve disparar a sincronização inventário.

- [Referências do Produto](#)

A partir do vRealize Suite Lifecycle Manager 8.1, os detalhes do produto têm uma nova guia vertical chamada **Referências de Produtos**, listando todas as integrações entre produtos.

Por exemplo, se o produto A estiver integrado ao produto B, ou vice-versa, a página **Exibir Detalhes** dos produtos A e B terá uma entrada na tabela **Referências de Produtos**, apontando uma referência entre eles.

- [Alterar sua senha para os produtos vRealize](#)

Você pode alterar a senha dos produtos vRealize instalados. Há diferentes tipos de opções de alteração de senha disponíveis na página Detalhes do produto.

- [Excluir um produto de um ambiente](#)

Você pode excluir uma instância de produto de um ambiente do Lifecycle Manager.

- [Adicionar licenças para os produtos do vRealize Suite](#)

Você pode configurar e substituir alterações de licença nos vRealize Automation por meio da UI do vRealize Suite Lifecycle Manager da sua empresa, onde poderá acessar os detalhes do produto no cartão do ambiente.

## Criação e configuração de um snapshot do produto

Agora você pode criar e gerenciar o snapshot de um produto para salvar o estado do produto em um determinado point-in-time.

Este procedimento não se aplica a snapshots de máquinas de bases de dados virtuais do vRealize Automation 7.x. Snapshots de máquinas de bases de dados virtuais do vRealize Automation 7.x devem ser obtidos manualmente, em vez de por meio do vRealize Suite Lifecycle Manager.

O gerenciamento de snapshots é restrito aos snapshots disparados do vRealize Suite Lifecycle Manager versão 8.6. Se você disparar um snapshot diretamente, ele não será mais gerenciado no vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 Para criar um snapshot, clique em **Gerenciar ambientes**.
- 2 Clique em **EXIBIR DETALHES**.
- 3 Clique no ícone de reticências ao lado do nome do produto a ser feito o smartphone e selecione **Criar Snapshot**.
- 4 Em Detalhes do snapshot, digite os detalhes do **Prefixo do snapshot** e da **Descrição do snapshot**.
- 5 (opcional) Para determinados produtos do vRealize Suite, você pode selecionar o botão de alternância **Snapshot com memória**.
- 6 (opcional) Você pode selecionar o botão de alternância **Encerrar antes de obter o snapshot**, conforme necessário.
- 7 Clique em **Avançar**.

- 8 Clique em **Executar pré-verificação** e, em seguida, clique em **Concluir**.

**Observação** As operações de Dia 2 que dependem do vCenter Server, como a criação de um smartphone, poderão falhar se as ferramentas de guest não estiverem em execução ou se o endereço IP/Nome do host não estiver visível no vCenter Server. A configuração do vRealize Operations Manager não pode ser acessada depois de reverter o instantâneo do vRealize Operations Manager, pois o cluster do vRealize Operations Manager pode estar inconsistente. Para obter mais informações, consulte o artigo KB [56560](#).

- 9 Para gerenciar um snapshot do produto, clique em **Gerenciar ambientes**.
- 10 Clique em **EXIBIR DETALHES**.
- 11 Clique no ícone de reticências ao lado do nome do produto do qual o snapshot será obtido e selecione **Gerenciar snapshot**.
- 12 Você pode exibir a estrutura em árvore do snapshot e os detalhes do snapshot. Clique em **Excluir** para excluir permanentemente um snapshot.
- 13 Clique em **Reverter** e clique em **EXECUTAR PRÉ-VERIFICAÇÃO** para reverter um snapshot.

## Resultados

### Observação

- O snapshot parcial ou inconsistente não fornece a opção de reversão.
- Você pode reverter um snapshot criado durante um upgrade ou um dimensionamento horizontal na guia **Solicitações**.
- Ao implantar produtos do vRealize Suite, um atributo personalizado é criado no vCenter para oferecer suporte ao inventário de snapshots vRealize Suite Lifecycle Manager.

O vRealize Suite Lifecycle Manager salva os detalhes de estado e de configuração do dispositivo virtual do produto. Para obter mais informações, consulte o artigo KB [56361](#).

### Próximo passo

Após criar um snapshot de produto, você pode reverter o dispositivo virtual do produto para o estado do snapshot.

## Sincronização de inventário no vRealize Suite Lifecycle Manager

Se você tiver atualizado qualquer configuração fora do vRealize Suite Lifecycle Manager, os produtos gerenciados a partir do vRealize Suite Lifecycle Manager estarão fora de sincronia. Para atualizar a configuração, você deve disparar a sincronização inventário.

Se tiver sido feito upgrade do produto fora do vRealize Automation ou do vRealize Operations Manager ou se houver alguma falha neles, a sincronização de inventário atualizará o nó primário correto do vRealize Suite Lifecycle Manager.

Se qualquer um dos componentes de produtos for adicionado ou excluído fora do vRealize Suite Lifecycle Manager, a sincronização de inventário será usada para atualizá-los. Se uma senha do produto for alterada por fora, ela poderá ser atualizada no vRealize Suite Lifecycle Manager por meio da sincronização com o inventário, mas a solicitação certamente falhará. No entanto, você pode fornecer a senha correta quando tentar novamente.

Para alterar a senha raiz do vRealize Operations Manager, você precisa criar uma senha raiz no Locker e usar a mesma para substituir a senha raiz do vRealize Operations Manager por meio do vRealize Suite Lifecycle Manager. Você não precisa alterar a senha raiz no vRealize Operations Manager.

Além disso, se você modificar a senha diretamente no aplicativo, por exemplo, no vRealize Operations Manager, deverá executar a sincronização de inventário do produto no vRealize Suite Lifecycle Manager para que as senhas modificadas sejam sincronizadas com o vRealize Suite Lifecycle Manager novamente. Essa ação solicita que você forneça as senhas modificadas durante uma sincronização de inventário.

Você pode sincronizar os inventários para cada produto e para todos os produtos em todos os ambientes.

- Em vez de navegar em cada produto para sincronizar os inventários, você pode clicar nas reticências horizontais no cartão do produto e clicar em **Disparar Sincronização de Inventário**.
- Se houver vários ambientes e vários produtos em um ambiente, você poderá clicar na guia **Disparar sincronização de inventário** na página de Ambiente. Isso dispara a sincronização de inventário de todos os produtos em todos os ambientes.
- Você pode clicar na guia **Exibir detalhes** do produto e, em seguida, clicar em **Disparar sincronização de inventário**. Isso dispara a sincronização de inventário apenas para o produto necessário.

## Referências do Produto

A partir do vRealize Suite Lifecycle Manager 8.1, os detalhes do produto têm uma nova guia vertical chamada **Referências de Produtos**, listando todas as integrações entre produtos. Por exemplo, se o produto A estiver integrado ao produto B, ou vice-versa, a página **Exibir Detalhes** dos produtos A e B terá uma entrada na tabela **Referências de Produtos**, apontando uma referência entre eles.

Para o vRealize Suite Lifecycle Manager, a tabela mostra apenas referências do Provedor de Autenticação do VMware Identity Manager. Se um produto, como o vRealize Automation, estiver integrado ao VMware Identity Manager do ambiente global e o estiver usando como provedor de autenticação, tanto o vRealize Automation e o VMware Identity Manager do ambiente global terão uma referência vinculando-os uns aos outros em suas tabelas **Exibir Detalhes > Referências de Produtos**.

As entradas de Referência de Produtos são criadas quando você cria um ambiente e durante uma sincronização de inventário. Se o produto esperado não aparecer na tabela Referência de Produtos do ambiente global do VMware Identity Manager, valide se a Sincronização de Inventário para o produto relacionado está selecionada e foi concluída com êxito.

No caso do VMware Identity Manager de ambiente global, as Referências de Produtos são usadas durante a execução das seguintes operações de dia 2:

- Operação de atualização ou substituição de certificado. Uma alteração no certificado do VMware Identity Manager requer a redefinição da confiança no certificado do VMware Identity Manager em todos os produtos ou serviços atualmente integrados a ele. Ao atualizar o certificado, você tem a opção de selecionar todos os produtos atualmente referenciados para aceitar a redefinição da confiança.
- Como ativar a locação. Depois que a locação está ativada, o VMware Identity Manager só pode ser acessado por meio de FQDNs de tenants. Todos os produtos ou serviços já existentes atualmente integrados ao VMware Identity Manager devem passar por um novo registro do VMware Identity Manager em relação ao seu FQDN de alias de tenant primário. Ao habilitar a locação, você tem a opção de escolher todos os produtos atualmente referenciados para aceitar o novo registro.

Com o recurso Gerenciar Ambientes na UI do vRealize Suite Lifecycle Manager, um inventário completo sobre cada produto é listado.

As Referências de Produtos, uma vez encontradas, serão usadas posteriormente nas operações de dia 2 para garantir que uma operação de ciclo de vida executada em um produto não interrompa a integração atual com outro produto vinculado e referenciado.

## Alterar sua senha para os produtos vRealize

Você pode alterar a senha dos produtos vRealize instalados. Há diferentes tipos de opções de alteração de senha disponíveis na página Detalhes do produto.

Para alterar a senha, no ambiente de cartão do produto, clique em **Exibir detalhes > Alterar senha**.

A tabela a seguir mostra a opção diferente de alteração de senha disponível na página de detalhes do produto.

Tipo de alteração de senha	Nome do produto vRealize
Alteração da senha do administrador	<ul style="list-style-type: none"> <li>■ vRealize Automation</li> <li>■ vRealize Operations Manager</li> <li>■ vRealize Network Insight</li> <li>■ vRealize Log Insight</li> <li>■ VMware Identity Manager</li> </ul>
Alteração da senha raiz	<ul style="list-style-type: none"> <li>■ vRealize Automation</li> <li>■ vRealize Operations Manager</li> <li>■ vRealize Business for Cloud</li> <li>■ vRealize Log Insight</li> <li>■ VMware Identity Manager</li> </ul>
Alteração de senha de suporte	<ul style="list-style-type: none"> <li>■ vRealize Network Insight</li> </ul>
Alteração de senha do usuário do Console	<ul style="list-style-type: none"> <li>■ vRealize Network Insight</li> </ul>
Alteração de senha do usuário SSH	VMware Identity Manager

## Excluir um produto de um ambiente

Você pode excluir uma instância de produto de um ambiente do Lifecycle Manager.

Você pode excluir uma implantação de produto de um vCenter Server. O Lifecycle Manager pode excluir a Integração do produto em um determinado ambiente para o produto selecionado, se isso for feito dentro de Lifecycle Manager durante a implantação dos produtos.

No caso de um ambiente no qual os produtos são importados, o Lifecycle Manager não coleta informações sobre uma integração de produto existente nos produtos. Portanto, você pode remover manualmente a integração do produto ao excluir os produtos.

### Pré-requisitos

Confirme que existe um produto em um ambiente.

### Procedimentos

- 1 Na página inicial do Ambiente, selecione qualquer instância do produto e clique com o botão direito do mouse nas reticências verticais.
- 2 Clique em **Excluir produto**.

**Observação** Quando houver produtos integrados internamente a um produto, verifique as integrações antes de excluir o produto. No entanto, o Lifecycle Manager não pode remover as integrações externas nos produtos.

- 3 Para excluir todas as VMs associadas do vCenter Server para o produto selecionado, marque a caixa de seleção **Excluir as VMs associadas**.

- 4 Se você quiser excluir máquinas do Windows, marque a caixa de seleção **Excluir máquinas Windows associadas** e clique em **Excluir**.

Antes de excluir as VMs associadas do vCenter Server, na janela **Excluir produto**, revise a lista de VMs e clique em **Confirmar exclusão**.

#### Resultados

O produto do conjunto selecionado e suas VMs associadas de um ambiente serão excluídos.

### Substituir certificados de produtos vRealize Suite Lifecycle Manager

Você pode substituir seus certificados existentes para produtos no vRealize Suite Lifecycle Manager.

Para substituir um certificado de VAMI/VA do vRealize Suite Lifecycle Manager, consulte [Substituir certificado para o vRealize Suite Lifecycle Manager](#). Para redefinir a confiança do Identity Manager, consulte [Operações do Dia 2 com outros produtos no vRealize Suite Lifecycle Manager](#).

#### Pré-requisitos

Verifique se um produto possui um certificado existente. Você pode criar ou importar um certificado no Locker. Para obter informações sobre como criar certificados, consulte [Configurar certificado no Locker](#).

#### Procedimentos

- 1 Na página Ambiente, selecione um cartão de produto e clique nas reticências verticais.
- 2 Clique em **Substituir Certificado**.
- 3 Em **Certificado Atual**, clique em **Avançar**.
- 4 Selecione um certificado no menu suspenso e clique em **Avançar**.
- 5 Selecione um certificado, analise o resumo do certificado e clique em **Avançar**.
- 6 Para substituir um certificado do VMware Identity Manager, você deve confiar novamente nos produtos que já estão configurados. Selecione a instância do produto aqui e clique em **Avançar**.

Por padrão, todos os produtos são listados no assistente Redefinir Confiança no Certificado do Produto.

7 (Opcional) Marque a caixa de seleção **Aceitar Snapshot**.

**Observação** Essa opção permite que você faça snapshots de produtos que não possuem a reversão de certificado incorporada. Você pode usar essa opção para reverter o snapshot em caso de falha ao substituir um certificado. E isso somente é aplicável ao vRealize Business for Cloud, ao VMware Identity Manager e ao vRealize Network Insight.

Se a solicitação de substituição de certificado tiver falhado e você tiver selecionado para tirar um snapshot, será possível definir o sinalizador revertToSnapshot como “true” e, em seguida, enviar a solicitação com falha para reverter a operação.

- 8 Para validar as informações do certificado, clique em **EXECUTAR PRÉ-VERIFICAÇÃO** e clique em **Concluir**.
- 9 Clique em **Aceitar** e **Enviar**.

## Adicionar licenças para os produtos do vRealize Suite

Você pode configurar e substituir alterações de licença nos vRealize Automation por meio da UI do vRealize Suite Lifecycle Manager da sua empresa, onde poderá acessar os detalhes do produto no cartão do ambiente.

### Pré-requisitos

- Verifique se existe a instância do vRealize Automation em vRealize Suite Lifecycle Manager.
- Certifique-se de que você adicionou uma licença no Locker. Para obter mais informações sobre como adicionar licenças, consulte [Configurar a licença no Locker](#).

### Procedimentos

- 1 Faça login na UI do vRealize Suite Lifecycle Manager.
- 2 Selecione a guia Ambientes e clique em **Exibir detalhes** para um cartão da vRealize do produto.
- 3 Selecione o ícone de opções do produto (...) e clique em **Adicionar Licença** a partir da suspensa. Você pode visualizar a lista de licenças atuais.
- 4 Clique em **Avançar**.
- 5 Selecione uma nova licença na lista suspensa e verifique os detalhes da licença.
- 6 (Opcional) Na vRealize Automation 8.0 e versões posteriores, vRealize Operations Manager e vRealize Log Insight, você poderá excluir as licenças mais antigas após selecionar uma nova licença. Selecione as licenças a ser removidas em **Encerrar licenças**.

**Observação** Essa opção se aplica ao vRealize Suite Lifecycle Manager 8.4.1 e versões posteriores.

**7 Clique em Concluir.**

As solicitações de Licença podem ser rastreadas na guia vRealize Suite Lifecycle Manager Solicitações .

**Próximo passo**

Para obter mais informações sobre como configurar a licença, consulte [Configurar licenças no Locker](#).

## Configurar o monitoramento de integridade da pilha de gerenciamento do vRealize Suite

Quando o vRealize Operations Manager faz parte do ambiente, você pode recuperar e exibir o status de integridade dos produtos do vRealize Suite em vRealize Suite Lifecycle Manager.

As informações de integridade no vRealize Suite Lifecycle Manager estão disponíveis somente para produtos compatíveis com o vRealize Suite Lifecycle Manager: vRealize Automation, vRealize Operations Manager, vRealize Log Insight e vRealize Business for Cloud.

**Pré-requisitos**

"Se quiser que o status de integridade apareça no seu cartão de ambiente, certifique-se de que o VMware vRealize Operations Manager esteja presente no mesmo cartão de ambiente, juntamente com os outros produtos do vRealize Suite." Para obter informações sobre como adicionar em um ambiente existente, consulte [Adicionar um produto a um ambiente de nuvem privada existente](#). Para obter informações sobre como criar um ambiente, consulte [Capítulo 3 Criar um ambiente no vRealize Suite Lifecycle Manager](#).

- [Status de integridade no vRealize Suite Lifecycle Manager](#)  
O vRealize Suite Lifecycle Manager exibe a integridade do ambiente de nuvem privada para o ambiente como um todo e no nível do produto individual.
- [Exibir o dashboard da Visão Geral da Integridade do SDDC no VMware vRealize Operations Manager](#)  
Com o vRealize Suite Lifecycle Manager, você pode exibir o status de integridade detalhado no vRealize Operations Manager.
- [Ativar ou desativar a verificação de integridade de produtos no vRealize Suite Lifecycle Manager](#)

**Procedimentos**

- 1 Instale o SDDC Management Pack no vRealize Operations Manager. Você pode instalar o SDDC Management Pack a partir do Marketplace no vRealize Suite Lifecycle Manager ou fora do vRealize Suite Lifecycle Manager.

- 2 Configure instâncias de adaptadores para vRealize Log Insight, vRealize Business for Cloud e vRealize Automation no vRealize Operations Manager.  
Para obter mais informações sobre como configurar adaptadores no vRealize Operations Manager, consulte [e](#).
- 3 Verifique se o dashboard SDDC Health Overview do vRealize Operations Manager exibe o status de integridade do vRealize Operations Manager e de outros produtos do vRealize Suite.
- 4 Depois que o status de integridade é exibido no dashboard SDDC Health Overview, o vRealize Suite Lifecycle Manager executa o status de integridade agendado.

---

#### **Observação**

- Se você tiver uma instância do vRealize Automation 7.x no ambiente, poderá instalar o agente de Gerenciamento de Operações de Endpoint 7.x em todos os nós em aplicativos do vRealize Automation e em qualquer novo nó adicionado ao cluster do vRealize Automation mais tarde.
  - Isso não é necessário para o vRealize Operations Manager que usa o VMware SDDC Management Pack 8.x.
- 

#### **Resultados**

O vRealize Suite Lifecycle Manager exibe o status de integridade do SDDC Management Pack e recupera as informações de status de integridade de uma instância do vRealize Operations Manager em um determinado ambiente de nuvem privada. O status de integridade se aplica apenas aos produtos do vRealize Suite configurados na instância de destino do vRealize Operations Manager no ambiente de nuvem privada. Você não deve configurar produtos adicionais do vRealize Suite de outros ambientes de nuvem privada na mesma instância do vRealize Operations Manager.

## **Status de integridade no vRealize Suite Lifecycle Manager**

O vRealize Suite Lifecycle Manager exibe a integridade do ambiente de nuvem privada para o ambiente como um todo e no nível do produto individual.

### **Status de integridade por cor**

Para ativar ou desativar a integridade no nível do ambiente, clique nas reticências verticais no cartão do ambiente. A tabela a seguir apresenta um guia codificado por cores para ajudá-lo a determinar o status de integridade do seu ambiente de nuvem privada.

Cor	Status
Cinza	Um status cinza indica um dos seguintes cenários: <ul style="list-style-type: none"> <li>■ O vRealize Operations Manager não faz parte do seu ambiente de nuvem privada.</li> <li>■ O vRealize Operations Manager não está configurado com o pacote de gerenciamento de solução de integridade do VMware SDDC Manager.</li> <li>■ Erro ao determinar a integridade do ambiente de nuvem privada.</li> <li>■ As informações de integridade ainda não estão disponíveis.</li> </ul>
Verde	O vRealize Operations Manager está relatando a integridade como verde, de acordo com suas políticas, para todos os produtos configurados.
Amarelo	O vRealize Operations Manager está relatando a integridade como Amarelo, de acordo com suas políticas, para pelo menos um produto configurado.
Vermelho	O vRealize Operations Manager está relatando a integridade como Laranja ou Vermelho, de acordo com suas políticas, para pelo menos um produto configurado.

O status de integridade do vRealize Suite Lifecycle Manager continua a exibir essas cores, mesmo quando você só configura parcialmente os produtos do vRealize Suite no vRealize Operations Manager. vRealize Suite Lifecycle Manager não tenta determinar o status de integridade dos produtos do vRealize Suite que não estão configurados no ambiente de nuvem privada.

## Exibir o dashboard da Visão Geral da Integridade do SDDC no VMware vRealize Operations Manager

Com o vRealize Suite Lifecycle Manager, você pode exibir o status de integridade detalhado no vRealize Operations Manager.

### Pré-requisitos

Verifique se você tem credenciais válidas do VMware vRealize Operations Manager ou o VMware Identity Manager configurado.

**Observação** Para o gerenciamento SDDC Pacote 4.0, não há necessidade de instalar agentes de Endpoint para o vRealize Automation 7.4 e o nó IaaS.

### Procedimentos

- 1 No vRealize Suite Lifecycle Manager, clique no status de integridade do ambiente de nuvem privada para abrir o Dashboard da visão geral de integridade do SDDC para o ambiente no VMware vRealize Operations Manager.
- 2 No vRealize Suite Lifecycle Manager, clique no status de integridade de um produto individual para abrir a página de resumo desse produto no VMware vRealize Operations Manager. Para obter mais informações, consulte o *VMware Marketplace*.

## Ativar ou desativar a verificação de integridade de produtos no vRealize Suite Lifecycle Manager

Você pode ativar a opção de verificação de integridade para verificar a integridade de um ambiente existente. Você pode usar essa opção em um cenário quando quiser avaliar o ambiente do vRealize Suite Lifecycle Manager que está instalado com o vRealize Operations Management Suite junto com o SDDC MP. Essa verificação de integridade só está disponível na instância do vRealize Operations Manager com um pacote de Gerenciamento do SDDC para monitorar a integridade de todo o sistema.

Esta opção primeiro verifica se há um ambiente a ser executado em primeiro lugar. Quando as verificações de integridade são executadas, é verificado se há uma solução de gerenciamento de integridade do SDDC disponível e, em seguida, verifica o último status da solução de integridade. Uma verificação de integridade é executada periodicamente em um intervalo agendado. Quando quiser evitar o uso de recursos em ambientes de desenvolvimento ou de produção, talvez queira desativar a verificação de integridade.

Quando a verificação de integridade está desativada, a integridade do ambiente não é mais avaliada. Uma mensagem é exibida no cartão do ambiente, sugerindo que o usuário ative a verificação de integridade para monitorar a integridade do ambiente. Quando uma verificação de integridade for executada, você poderá ver o status atual do ambiente. Se o status estiver OK e os dados forem buscados, você poderá visualizar uma mensagem no cartão como Integridade OK.

## Como adicionar e gerenciar conteúdo do Marketplace

Você pode usar o vRealize Suite Lifecycle Manager para adicionar e gerenciar conteúdo do Marketplace.

O Marketplace contém plug-ins de conteúdo para o vRealize Orchestrator, incluindo blueprints e OVAs do vRealize Automation, pacotes de gerenciamento do vRealize Operations Manager e pacotes de conteúdo do vRealize Log Insight, que você pode baixar e implantar em seus ambientes do vRealize Suite.

O **VMware Marketplace** exibe os detalhes do conteúdo dos produtos vRealize Suite disponíveis. A guia **Disponível** fornece a opção Sincronizar, se você estiver sincronizando o Marketplace pela primeira vez.

## Encontrar e baixar conteúdo do Marketplace

Você pode usar o vRealize Suite Lifecycle Manager para pesquisar e baixar conteúdo do Marketplace.

O vRealize Suite Lifecycle Manager 8.1 é compatível com a instalação OVA do vRealize Automation 7.6. Cada OVA está em GBs no Marketplace. Se você quiser baixar mais OVAs do Marketplace, aumente o tamanho da pasta de dados para evitar o alerta de Disco cheio. Os OVAs no Marketplace têm tamanho grande de arquivo. Se for baixar vários OVAs e, para evitar alerta de armazenamento em disco, aumente o armazenamento na página de configurações do sistema.

## Pré-requisitos

Verifique se foi executada uma sincronização inicial do Marketplace para carregar o conteúdo do Marketplace. Consulte [#unique\\_148](#).

## Procedimentos

- 1 Clique em **VMware Marketplace** e clique na guia **Todos**.

O vRealize Suite Lifecycle Manager exibe todo o conteúdo disponível para o vRealize Suite no Marketplace.

- 2 (Opcional) Para filtrar a lista de conteúdos disponíveis por termos de pesquisa, digite termos de pesquisa na caixa de texto **Pesquisar**.
- 3 (Opcional) Para filtrar a lista de conteúdos disponíveis por produto, editor ou tecnologia, clique em **Filtrar** e selecione os filtros apropriados.
- 4 Clique em **Exibir detalhes** para saber mais sobre o conteúdo que pode ser baixado, incluindo quais produtos e versões são compatíveis, avaliações dos usuários para o conteúdo e uma lista de conteúdo relacionado.
- 5 Clique em **Download** para baixar o conteúdo para o vRealize Suite Lifecycle Manager.

## Resultados

O conteúdo baixado aparece na guia **Download** da página do **Marketplace**.

## Próximo passo

Instale o conteúdo baixado. Consulte [Instalar conteúdo baixado do Marketplace](#).

## Exibir e atualizar conteúdo baixado do Marketplace

Você pode exibir detalhes sobre o conteúdo anteriormente baixado do Marketplace, incluindo o número da versão e a data da última atualização.

## Procedimentos

- 1 Clique em **Marketplace** e clique na guia **Disponível**.

O vRealize Suite Lifecycle Manager exibe todo o conteúdo baixado para o vRealize Suite Lifecycle Manager do Marketplace.

- 2 Se houver uma atualização disponível para o conteúdo, você poderá baixar uma versão mais recente do conteúdo.
  - a Passe o mouse sobre o ícone de notificação no canto superior esquerdo do bloco de conteúdo para verificar se há uma atualização disponível.

Se não houver notificações para o conteúdo, o ícone de notificação não aparecerá.

Se houver uma versão mais recente do conteúdo disponível, o vRealize Suite Lifecycle Manager exibirá a mensagem Novas atualizações da versão estão disponíveis para o aplicativo.
  - b Clique nos três pontos no canto superior direito do bloco de conteúdo e selecione **Atualizar**.
  - c Para baixar, selecione uma versão e clique em **Continuar**.

Se você estiver atualizando um blueprint do vRealize Automation, um plug-in do vRealize Orchestrator ou um pacote de conteúdo do vRealize Log Insight ou estiver atualizando um pacote de gerenciamento do VMware vRealize Operations Manager com uma versão mais recente, o conteúdo anterior será substituído por conteúdo atualizado. Se você tentar atualizar um pacote de gerenciamento do VMware vRealize Operations Manager com a mesma versão já instalada, ocorrerá falha na atualização.
- 3 Clique em **Exibir Detalhes** para exibir informações sobre o conteúdo, incluindo o conteúdo relacionado e a data da última modificação do conteúdo.

## Instalar um conteúdo baixado do Marketplace

Você pode instalar o conteúdo baixado do Marketplace.

### Pré-requisitos

- Baixe do Marketplace o conteúdo a ser instalado. Consulte [Encontrar e baixar conteúdo do Marketplace](#).
- Verifique se o ambiente que está sendo instalado tem o direito correspondente ao direito compatível com o conteúdo.

### Procedimentos

- 1 Clique em **Marketplace** e clique na guia **Disponível**.

O vRealize Suite Lifecycle Manager exibe todo o conteúdo baixado do Marketplace para o vRealize Suite Lifecycle Manager.

- 2 Clique nos três pontos no canto superior direito do bloco para instalar o conteúdo e clique em **Instalar**.

- 3 Selecione o centro de dados e o ambiente para instalar o conteúdo, se estiver instalando um blueprint ou OVA em um vRealize Automation e clique em **Avançar**.

O vRealize Automation e o conteúdo do vRealize Operations Management Suite têm tag com direitos de licença.

- 4 Depois de selecionar um centro de dados e um ambiente, selecione o tenant no qual o conteúdo precisa ser instalado e clique em **Enviar**.

#### Próximo passo

Você pode monitorar o progresso da instalação na página de **Solicitações**.

## Excluir conteúdo baixado do Marketplace

Você pode excluir o conteúdo baixado do Marketplace. No entanto, isso não remove o conteúdo dos ambientes nos quais ele está instalado por meio do vRealize Suite Lifecycle Manager.

#### Procedimentos

- 1 Clique em **Marketplace** e, em seguida clique na guia **Download** .
- 2 Clique nos pontos verticais no canto superior direito do bloco para excluir e clique em **Excluir**.
- 3 Clique em **Sim**.

#### Resultados

O conteúdo é excluído do vRealize Suite Lifecycle Manager e não aparece mais no conteúdo baixado na página do **Marketplace**.

# Como gerenciar o ciclo de vida do conteúdo no vRealize Suite Lifecycle Manager

5

O gerenciamento do ciclo de vida do conteúdo no vRealize Suite Lifecycle Manager fornece uma maneira para os gerentes de liberação e os desenvolvedores de conteúdo gerenciarem o centro de dados definido por software (SDDC). Ele inclui captura de conteúdo, teste e liberação para vários ambientes e recursos de controle de origem por meio de diferentes endpoints de controle de origem que incluem o GitHub, o GitLab e o Bitbucket. Os desenvolvedores de conteúdo não têm permissão para definir uma política de liberação em endpoints. Somente os Gerentes de Liberação podem definir políticas.

Não há suporte para a migração de conteúdo ou versões de uma instância mais antiga do vRealize Suite Lifecycle Manager. A versão de conteúdo mais recente pode ter a origem controlada ou ser implantada em um endpoint antes da migração para o vRealize Suite Lifecycle Manager. Dessa forma, o mesmo conteúdo pode ser novamente capturado do endpoint na nova instância.

Há suporte para a migração de endpoints e configurações de conteúdo, incluindo:

- Todos os endpoints são migrados com tokens de usuário de controle de origem.
- Tags associadas aos endpoints são migradas para a nova instância.
- Configurações de stubs de pipeline são migradas.

---

**Observação** Quando o usuário administrador de nuvem recebe uma função de gerente de liberação ou de desenvolvedor de conteúdo, ele só pode exibir o aplicativo de gerenciamento de conteúdo no vRealize Suite Lifecycle Manager. Porém, ele não tem permissão para exibir outros aplicativos. Por outro lado, um gerente de liberação e um usuário desenvolvedor de conteúdo podem exibir o aplicativo de gerenciamento de conteúdo. Como solução alternativa, você pode realizar todas as operações de administrador de nuvem usando somente a função de administrador de nuvem, sem mapeamento de permissões ou funções adicionais.

---

É possível usar o gerenciamento do ciclo de vida de conteúdo para dispensar os processos manuais demorados e propensos a erros necessários para gerenciar o conteúdo definido por software. O conteúdo com suporte inclui entidades dos seguintes produtos:

Nome do produto.	Versão com suporte
vRealize Automation	7.2 e posterior
vRealize Orchestrator	7.x e posterior
VMware vSphere	6.0 e posterior

<b>Nome do produto.</b>	<b>Versão com suporte</b>
vRealize Operations Manager	6.6.1+ e posterior
Servidores de controle de origem	<ul style="list-style-type: none"> <li>■ GitHub Enterprise Server: 2.20.15, 2.19.21, 2.21.6 e 3.0 (não há suporte para o GitHub Cloud)</li> <li>■ GitLab: 12.2.12 (Enterprise Edition), 12.7 e 12.8</li> <li>■ Bitbucket Server 6.10 e 7.0</li> <li>■ Bitbucket Cloud: versão 2.0</li> </ul>

O gerenciamento do ciclo de vida do conteúdo no vRealize Suite Lifecycle Manager é semelhante ao gerenciamento do ciclo de vida do conteúdo com o vRealize Code Stream Management Pack for DevOps, com as seguintes diferenças.

- O gerenciamento do ciclo de vida do conteúdo é implantado como parte do vRealize Suite Lifecycle Manager em um único dispositivo. Ele tem uma nova interface de usuário e está fortemente integrado aos principais serviços do vRealize Suite Lifecycle Manager.
- Serviços de pipeline atualizados: capacidade avançada de gerenciar conteúdo para trabalhar com controle de origem e oferecer suporte a um caso de uso de vários desenvolvedores.

Se houver dependências entre os pacotes de conteúdo capturados, todas essas dependências serão capturadas como objetos de primeira classe no vRealize Suite Lifecycle Manager. Cada versão do conteúdo mostra todas as suas dependências associadas. Por exemplo, se um Blueprint composto do vRealize Automation tiver uma dependência de Definição de Propriedade, haverá dois itens no catálogo de conteúdo, um para cada pacote de conteúdo. Com o controle de versão independente para cada pacote de conteúdo, você pode editar, capturar e liberar dependências de maneira independente e, portanto, o conteúdo nunca fica obsoleto. O vRealize Automation permite definir vários conjuntos de valores nomeados dentro dos tipos de perfil de componente Tamanho e Imagem. Você pode adicionar um ou mais dos conjuntos de valores a componentes de máquina em um blueprint. Não poderemos implantar ou liberar Perfis de Componente de Automação no vRealize Suite Lifecycle Manager em um endpoint de destino se o conjunto de valores correspondentes já existir nesse endpoint.

#### ■ [Como trabalhar com endpoints de conteúdo](#)

Um endpoint de conteúdo é um endpoint de infraestrutura no centro de dados definido por software (SDDC), como uma instância do vRealize Automation, que é alvo de captura, teste e liberação de conteúdo gerenciado.

#### ■ [Gerenciar conteúdo](#)

Conteúdo é um conjunto de arquivos que contém definições que representam serviços definidos por software.

#### ■ [Controle de origens de acesso](#)

Apenas um gerente de liberação pode adicionar um acesso de controle de origem, no qual o controle de origem pode ser o GitLab ou o Bitbucket. Com esse privilégio, um gerente de liberação pode selecionar o tipo GitLab, Bitbucket e inserir o nome do servidor GitLab. Você pode fornecer vários nomes de servidor e, em seguida, usar o token de acesso pessoal do GitLab e atribuí-lo ao servidor de controle de origem.

- [Como gerenciar endpoints de servidores de controle de origem](#)

Antes de você poder fazer o check-in ou o check-out do conteúdo, um vRealize Suite Lifecycle Manager deve adicionar um servidor de controle de origem GitLab ou Bitbucket ao sistema.

- [Como trabalhar com as configurações de conteúdo](#)

Você pode adicionar o endpoint do servidor de controle de origem, o editor vCenter, a extensibilidade do pipeline e as restrições do desenvolvedor em Configurações de Conteúdo.

- [Pipelines de Conteúdo](#)

A partir do vRealize Suite Lifecycle Manager 8.3, a página Pipelines de Conteúdo é reprojetada para exibir o status da captura de conteúdo, do teste e da liberação dos pipelines de conteúdo. É possível exibir todos os pipelines de conteúdo exibidos no estado concluído, em andamento ou com falha.

## Como trabalhar com endpoints de conteúdo

Um endpoint de conteúdo é um endpoint de infraestrutura no centro de dados definido por software (SDDC), como uma instância do vRealize Automation, que é alvo de captura, teste e liberação de conteúdo gerenciado.

Você adiciona um endpoint de conteúdo a um ambiente para capturar, testar, implementar ou verificar conteúdo definido por software na forma de pacote de conteúdo. Um pacote de conteúdo é um arquivo que contém definições para serviços definidos por software, como blueprints, modelos, fluxos de trabalho e assim por diante. Cada endpoint de conteúdo pode ser compatível com mais de um tipo de pacote de conteúdo. Por exemplo, um endpoint de conteúdo do vRealize Automation pode ser compatível com blueprints compostos e software.

Utilize os endpoints de conteúdo para executar as seguintes ações:

- Capture um ou mais pacotes de conteúdo.
- Teste um ou mais pacotes de conteúdo em um ambiente de preparação.
- Libere um ou mais pacotes de conteúdo testados em um ambiente de produção.

O Gerenciamento do ciclo de vida de conteúdo fornece as seguintes políticas para o vRealize Orchestrator, vRealize Automation, vRealize Automation Cloud, vCenter Server e endpoints de conteúdo do vRealize Operations.

**Tabela 5-1. Políticas para os produtos do vRealize Suite**

Política	Descrição
Permitir que o conteúdo seja capturado neste endpoint	Permite capturar conteúdo desse endpoint.
Permitir que testes de unidade sejam executados neste endpoint	Permite liberar conteúdo para o endpoint e executar fluxos de trabalho de teste no endpoint. Um vRealize Orchestrator marcado como endpoint de teste também atua como servidor de teste de unidade.

**Tabela 5-1. Políticas para os produtos do vRealize Suite (continuação)**

Política	Descrição
Permitir a liberação de pacotes de conteúdo para este endpoint	Permite que você libere conteúdo para o endpoint.
Somente conteúdo controlado pela origem	Permite que você libere somente conteúdo controlado pela origem para o endpoint.
Ativar revisão de código	Essa política se aplica somente aos endpoints de controle de origem. Permite uma revisão manual para os desenvolvedores. O gerenciamento de ciclo de vida de conteúdo do vRealize Suite Lifecycle Manager cria uma ramificação com alterações que exigem uma revisão de código. Um revisor de código aceita ou rejeita a solicitação de mesclagem na ramificação do respectivo controle de origem.
Ativar o suporte de modelo do vCenter	Solicita informações necessárias para a implantação de modelos. Essa opção está disponível apenas quando você marca um vCenter Server como endpoint de produção.

- **Adicionar um vRealize Orchestrator endpoint de conteúdo**

Um endpoint do vRealize Orchestrator é necessário para criar endpoints do vRealize Automation e capturar conteúdo.

- **Adicionar um endpoint de conteúdo do vRealize Automation**

Para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo, adicione um endpoint de conteúdo a um ambiente.

- **Adicionar um endpoint de nuvem do vRealize Automation**

O endpoint de vRealize Automation Cloud é introduzido para adicionar um endpoint de conteúdo a um ambiente.

- **Adicionar um endpoint de controle de origem**

Um endpoint de controle de origem representa um projeto (repositório) e um servidor de controle de origem.

- **Adicionar um endpoint de conteúdo do vCenter Server**

Adicione um endpoint de conteúdo a um ambiente para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo.

- **Adicionar um endpoint do vRealize Operations Manager**

Adicione um endpoint de conteúdo do vRealize Operations Manager para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo.

- **Excluir um endpoint de conteúdo**

Você pode excluir um endpoint de conteúdo existente.

- **Editar um endpoint de conteúdo**

Você pode editar as configurações de um endpoint de conteúdo existente.

## Adicionar um vRealize Orchestrator endpoint de conteúdo

Um endpoint do vRealize Orchestrator é necessário para criar endpoints do vRealize Automation e capturar conteúdo.

### Pré-requisitos

Se você estiver usando este endpoint do vRealize Orchestrator para testar a unidade, verifique se a instância do vRealize Orchestrator foi configurada como um servidor de teste da unidade.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em **Endpoints**, clique em **NOVO ENDPOINT**.
- 3 Clique em **vRealize Orchestrator**.

Para um conteúdo do Orchestrator, você pode capturar fluxos de trabalho, elementos de configuração e ações individualmente ou em uma pasta na qual eles residem.

---

**Observação** Se uma pasta for capturada, um nome de conteúdo temporário começando com [FOLDER] será exibido. Você pode iniciar um Pipeline de conteúdo para capturar todo o conteúdo, que é adicionado ao pacote do vRealize Orchestrator fornecido como entrada.

---

- 4 Digite as informações para o endpoint de conteúdo do vRealize Orchestrator.
  - a Na caixa de texto **Nome**, digite um nome exclusivo para o endpoint.
  - b Na caixa de texto **Tags**, digite as tags associadas ao endpoint.

O uso de tags permite implantar conteúdo em vários endpoints ao mesmo tempo. Ao implantar conteúdo, você pode selecionar uma tag em vez de nomes de endpoint de conteúdo individuais e o conteúdo é implantado em todos os endpoints que possuírem essa tag.

Para adicionar várias tags, pressione **Enter** depois de inserir cada tag.

- c No campo **FQDN/IP do Servidor**, digite o nome de servidor totalmente qualificado, o endereço IP ou o nome do host do servidor de endpoint de conteúdo.

Se a instância do vRealize Orchestrator não estiver incorporada no vRealize Automation, inclua o número da porta no FQDN/IP do servidor. Normalmente, o número da porta é 8281. O número da porta 8281 é necessário para as versões do vRealize Orchestrator 7.x. Para o vRealize Orchestrator 8.x e versões mais recentes, a porta não é necessária.

*vRO-Server-FQDN:Port*

- d Digite um nome de usuário e uma senha a serem usados para acessar esse endpoint de conteúdo.

- 5 Pressione **TESTAR CONEXÃO** para testar a conexão com o endpoint de conteúdo.

Se o teste de conexão falhar, verifique se as informações inseridas para o endpoint de conteúdo estão corretas e tente novamente.

## 6 Selecione Pacote vRO.

O pacote do vRealize Orchestrator pode ser capturado de um endpoint e está associado com o endpoint de conteúdo. Marque a versão como Produção pronta. A seleção de um pacote vRO é um recurso pós-implantação que importa o pacote assim que qualquer outro conteúdo tenha sido implantado, permitindo a manutenção de configurações localizadas ou regionais.

- Ignorar módulos ao listar conteúdo: uma lista separada por vírgula de ações ou módulos do vRealize Orchestrator que são excluídos ao listar um endpoint para reduzir o número. Com o Lifecycle Manager 8.0, qualquer módulo ou pasta com ou sem dependências pode ser excluído durante a captura ou listagem do conteúdo. No entanto, para o pacote do Orchestrator, esses módulos ou pastas não são ignorados. O Lifecycle Manager valida as dependências de conteúdo disponíveis no endpoint de origem durante a captura com dependências. Isso depende da política especificada nos endpoints.
- Ignorar fluxos de trabalho nessas pastas: uma lista separada por vírgula das pastas de fluxo de trabalho do vRealize Orchestrator que são excluídas ao listar de um endpoint para reduzir o número.
- Um nome de pacote do vRO não pode conter caracteres especiais e pode causar problemas quando você captura, libera ou faz check-in de um conteúdo. Se você tiver um nome de pacote vRO com um espaço entre o nome, o espaço será convertido em um sublinhado (\_) durante uma captura e falhará durante um teste e implantação.

## 7 Selecione as políticas apropriadas para o endpoint de conteúdo e clique em **Avançar**.

Para obter mais informações sobre as políticas, consulte a tabela de políticas fornecida em [Trabalhando com endpoints](#).

## 8 Verifique se os detalhes do endpoint de conteúdo estão corretos e clique em **Enviar**.

## Adicionar um endpoint de conteúdo do vRealize Automation

Para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo, adicione um endpoint de conteúdo a um ambiente.

### Pré-requisitos

Verifique se você adicionou pelo menos um endpoint do vRealize Automation.

---

**Observação** Se o vRealize Orchestrator estiver incorporado, não haverá necessidade de uma instância separada do endpoint do vRealize Orchestrator. A criação de endpoint do vRealize Orchestrator será necessária somente se você estiver usando um endpoint externo do vRealize Orchestrator para o vRealize Automation.

---

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em **Endpoints**, clique em **NOVO ENDPOINT**
- 3 Clique em **Automação**.

**4** Digite as informações do endpoint de conteúdo do vRealize Automation.

- a No campo **Nome** digite um nome exclusivo para o endpoint.

Pode ser um nome de servidor ou outro nome.

- b Selecione a versão do produto do endpoint no menu suspenso **Versão do Endpoint**.

- c No campo **Tags**, digite as tags associadas ao endpoint.

Com as tags, você pode implantar conteúdo em vários endpoints ao mesmo tempo. Ao implantar conteúdo, você pode selecionar uma tag em vez de nomes de endpoint de conteúdo individuais. O conteúdo será implantado em todos os endpoints que possuírem essa tag.

Para adicionar várias tags, pressione **Enter** depois de inserir cada tag.

- d No campo **FQDN/IP do Servidor**, digite o nome de servidor totalmente qualificado, o endereço IP ou o nome do host do servidor de endpoint de conteúdo.

Ao adicionar um endpoint para um determinado tenant, o FQDN baseado em tenant deve ser usado como um servidor. No entanto, para um domínio baseado em sistema, o FQDN do usuário sem um tenant deve ser usado.

Não há suporte para endereços IP durante a adição de endpoints do vRealize Automation 8.x.

- e Digite um nome de tenant, um nome de usuário e uma senha para usar para acessar este endpoint de conteúdo.

- f Selecione um endpoint externo ou incorporado do vRealize Orchestrator para ser associado no menu suspenso do **Endpoint do vRO Server**.

Ao selecionar uma conta de usuário para exportar ou importar conteúdo para o vRealize Suite Lifecycle Manager, verifique se a conta tem TODAS as funções selecionadas. A função **Consumidor de exportação segura** permite que o LCM exporte senhas que podem ser importadas para endpoints alternativos do vRA.

**5** Pressione **TESTAR CONEXÃO** para testar a conexão com o endpoint de conteúdo.

Se o teste de conexão falhar, verifique se as informações inseridas para o endpoint de conteúdo estão corretas e tente novamente.

**6** Clique em **Avançar**.

**7** Selecione as políticas apropriadas para o endpoint de conteúdo e clique em **Avançar**.

Para obter mais informações sobre as políticas, consulte a tabela de políticas fornecida em [Trabalhando com endpoints](#).

**8** Verifique se os detalhes do endpoint de conteúdo estão corretos e clique em **Enviar**.

## Adicionar um endpoint de nuvem do vRealize Automation

O endpoint de vRealize Automation Cloud é introduzido para adicionar um endpoint de conteúdo a um ambiente.

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em Endpoints, clique em **NOVO ENDPOINT**.
- 3 Selecione **vRealize Automation Cloud**.
- 4 Digite os detalhes do endpoint para o endpoint do vRealize Automation Cloud.
  - a No campo Nome, digite um nome exclusivo para o endpoint.
  - b No campo Tags, digite as tags associadas ao endpoint, para que você possa implantar conteúdo em vários endpoints ao mesmo tempo. Ao implementar conteúdo, você pode selecionar uma etiqueta em vez de nomes de endpoint de conteúdo individuais. O conteúdo implanta todos os endpoints com a tag selecionada. Quando quiser adicionar várias tags, pressione **Enter** depois de inserir cada etiqueta.
  - c Digite o token de atualização.
  - d No campo Endpoint do Servidor do vRO , selecione **vRO externo ou dispositivo de Extensibilidade de Nuvem do vRA**
  - e Para associar um Servidor do vRO, selecione endpoint do vRealize Orchestrator (vRO) no menu suspenso.
- 5 Para testar a conexão com o endpoint de conteúdo, clique em **TESTAR CONEXÃO**. Se o teste de conexão falhar, verifique se as informações inseridas para o endpoint de conteúdo estão corretas e, em seguida, tente novamente.
- 6 Clique em **Avançar**.
- 7 Em Configurações de Políticas, selecione as políticas do pacote vRealize Orchestrator adequada para o endpoint de conteúdo e clique em Próximo. Para obter mais informações sobre as políticas, consulte a tabela de políticas fornecida em [Trabalhando com endpoints](#).
- 8 Verifique se os detalhes do endpoint de conteúdo estão corretos e, em seguida, clique em **Enviar**.

### Pré-requisitos

- Crie um endpoint vRealize Orchestrator externo para o vRealize Automation.
- Gere um token de atualização de API. Para obter informações detalhadas sobre como gerar tokens de API, consulte os [VMware Cloud Services](#).

## Adicionar um endpoint de controle de origem

Um endpoint de controle de origem representa um projeto (repositório) e um servidor de controle de origem.

Você pode ter qualquer número de repositórios de controle de origem e ramificações adicionados ao vRealize Suite Lifecycle Manager. Adicionar uma ramificação de controle de origem permite fazer check-in e check-out do conteúdo do SDDC.

### Pré-requisitos

- Verifique se um administrador do vRealize Suite Lifecycle Manager adicionou um servidor de controle de origem do sistema em Configurações de conteúdo.
- Verifique se um desenvolvedor inseriu o token de acesso do GitLab para o servidor de controle de origem para que ele possa fazer check-in e check-out do conteúdo.

---

**Observação** Anteriormente, espaços de trabalho primários eram compatíveis com o Bitbucket Cloud. A partir do vRealize Suite Lifecycle Manager versão 8.6.1, vários espaços de trabalho também são compatíveis com o Bitbucket Cloud.

---

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em **Endpoints**, clique em **NOVO ENDPOINT**
- 3 Clique em **Controle de origem**.
- 4 Selecione o **Servidor de controle de origem** configurado (servidor do Bitbucket, nuvem do Bitbucket, GitLab ou GitHub).
- 5 Digite as informações para o endpoint de conteúdo do controle de origem.
  - a Na caixa de texto **Nome**, digite um nome exclusivo para o endpoint.
  - b Digite um nome de **Tag**.
  - c Digite o **Branch** e o **Nome do Re却itório** a serem usados para o endpoint de conteúdo no seguinte formato: para o GitLab, digite *group\_name/repository\_name*, para o servidor Bitbucket, digite *project\_name/repository\_name* e, para uma nuvem do Bitbucket, digite *repository\_name* se estiver usando o espaço de trabalho primário ou *workspace\_name/repository\_name* se você estiver usando vários espaços de trabalho.

---

**Observação** Na nuvem de bucket de bits, você só pode criar um repositório e usar o nome do repositório. O endpoint de controle de origem com um repositório deve ser inicializado com qualquer arquivo. A nuvem do GitLab e do bucket bits já tem um provisionamento para adicionar o arquivo, mas o servidor de bucket de bits não. Com o Lifecycle Manager 2.1, a instância de cluster e pesquisa elástica para história de vários desenvolvedores não é compatível com o servidor de bucket de bits.

---

- 6 Clique em **Testar conexão** e clique em **Avançar**.

- 7 Selecione as políticas apropriadas para esse endpoint de conteúdo e clique em **Avançar**.

Política	Descrição
Ativar revisão de código	Permite uma revisão manual entre os desenvolvedores. O gerenciamento do ciclo de vida do conteúdo do vRealize Suite Lifecycle Manager cria uma ramificação com as alterações que exigem uma revisão de código. Um revisor de código pode aceitar ou rejeitar a solicitação de mesclagem na ramificação.

- 8 Verifique se os detalhes do endpoint de conteúdo estão corretos e clique em **Enviar**.

## Adicionar um endpoint de conteúdo do vCenter Server

Adicione um endpoint de conteúdo a um ambiente para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo.

### Pré-requisitos

Verifique se você adicionou pelo menos um endpoint do vCenter no **Repositório de Modelos do vSphere > das Configurações de Conteúdo**.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em **Endpoints**, clique em **NOVO ENDPOINT**
- 3 Clique em **vCenter Server**.
- 4 Digite as informações para o endpoint de conteúdo do vCenter.
  - a Na caixa de texto **Nome**, digite um nome exclusivo para o endpoint.
  - b Na caixa de texto **Tags**, digite as tags associadas ao endpoint.

O uso de tags permite que você implemente um conteúdo em vários endpoints ao mesmo tempo. Ao implantar um conteúdo, você pode selecionar uma tag em vez de nomes de endpoint de conteúdo individuais e o conteúdo é implantado em todos os endpoints que possuírem essa tag. Para adicionar várias tags, pressione Enter depois de inserir cada tag.
- 5 Na caixa de texto FQDN/IP do Servidor, digite o nome do servidor totalmente qualificado, o endereço IP ou o nome do host do servidor de endpoint de conteúdo.
- 6 Para acessar o endpoint, digite o **nome de usuário** e a **senha**.
- 7 Clique em **Testar Conexão** e em **Avançar**.
- 8 Selecione as políticas apropriadas para o endpoint de conteúdo. Para obter mais informações sobre as políticas, consulte a tabela de políticas fornecida em [Trabalhando com endpoints](#).
- 9 Clique em **Avançar** e forneça os detalhes do vCenter Server.
- 10 Clique em **Avançar**.

**11** Para importar um centro de dados existente, clique em **Importar Centro de Dados LCM**.

As configurações do vCenter Server podem ser adicionadas a um centro de dados LCM, quando a coleta de dados do vCenter é concluída, este endpoint é visto ao importar do LCM e reduz o tempo para preencher o formulário, pois todas as propriedades foram coletadas. Exceto pelo caminho da pasta da Máquina Virtual que é fornecido no formato /Templates/ MyTemplates/ não é importado.

Depois que o endpoint é criado, ele valida se a configuração está correta. Ele pode se conectar através da API e se a configuração dos detalhes do assinante local estiver definida para apontar para o editor, conforme definido em Configurações de conteúdo/ Repositório de modelos do vSphere. Se houver um problema, o endpoint será desativado e um erro será exibido quando você cobrir o aviso.

## Adicionar um endpoint do vRealize Operations Manager

Adicione um endpoint de conteúdo do vRealize Operations Manager para capturar, testar, implantar ou fazer check-in de um pacote de conteúdo.

### Pré-requisitos

- Verifique se a conta de usuário SSH está configurada.
- Verifique se todas as instâncias do vRealize Operations Manager contêm os mesmos pacotes de gerenciamento instalados e as instâncias do adaptador necessárias configuradas.
- Os painéis configurados para fazer referência a objetos específicos, por exemplo, vCenter VM, Host ou Repositório de dados e não serão usados na liberação do endpoint até que sejam editados manualmente para atualizar a referência a um objeto específico.

---

**Observação** Alguns conteúdos podem não ser liberados entre versões diferentes do vRealize Operations Manager nas quais alguns tipos de conteúdo do 6.6 para o 6.7 podem falhar.

---

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em **Endpoints**, clique em **NOVO ENDPOINT**
- 3 Clique em **vRealize Operations**.
- 4 Digite as informações para o endpoint de conteúdo do vRealize Operations Manager.
  - a No campo **Nome** digite um nome exclusivo para o endpoint.
  - b Digite um nome de tag para que o endpoint possa usá-lo para teste ou captura.
  - c Digite o endereço do **FQDN/IP do Servidor**.
  - d Digite o **Nome de Usuário** e a **Senha**.

- e Digue o **Nome de Usuário SSH** e a **Senha SSH**.
  - f Clique em **Testar conexão** e, quando a conexão for estabelecida, clique em **Avançar**. Para obter mais informações sobre como criar um usuário SSH na instância do vRealize Operations Manager, consulte [Criar um usuário SSH no vRealize Operations Manager](#).
- 5 Em **Configurações de Política**, selecione as opções necessárias para capturar, testar ou marcar como produção. Para obter mais informações sobre as políticas, consulte a tabela de políticas fornecida em [Trabalhando com endpoints](#).
- 6 Verifique se os detalhes do endpoint de conteúdo estão corretos e clique em **Enviar**.

## Criar um usuário SSH no vRealize Operations Manager

Você pode criar um endpoint do vRealize Operations Manager no endpoint de Gerenciamento de conteúdo do vRealize Suite Lifecycle Manager .

- 1 Ao selecionar uma Raiz como usuário SSH no endpoint de conteúdo, crie um usuário no dispositivo do vRealize Operations Manager. O usuário deve ter um acesso SSH e pertencer à raiz do grupo de usuários e a um diretório home válido.
- 2 Faça login no dispositivo do vRealize Operations Manager como um usuário raiz e crie um usuário no dispositivo do vRealize Operations Manager usando o comando abaixo. `useradd sshuser`.
- 3 Configurar grupos de usuários para o usuário criado – `usermod -G root,wheel sshuser`
- 4 Configure o diretório home correto para o usuário:

```
mkdir /home/sshuser"
"chown sshuser /home/sshuser"
```

- 5 Defina a senha para o `passwd sshuser`
- 6 Ative a senha com recursos sudo.

```
Run command visudo

sshuser ALL = NOPASSWD: /usr/lib/vmware-vcopssuite/python/bin/python /usr/lib/vmware-vcops/
tools/opscli/ops-cli.py *
sshuser ALL = NOPASSWD: /bin/rm -rf /tmp/*
sshuser ALL = NOPASSWD: /bin/mv /tmp/*
```

**Observação** Use o OPS-CLI para a maioria dos conteúdos do vRealize Operations Manager para exportar ou importar uma captura de conteúdo ou versão no vRealize Suite Lifecycle Manager.

## Excluir um endpoint de conteúdo

Você pode excluir um endpoint de conteúdo existente.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.

- 2 Em **Endpoints**, clique nas reticências verticais à esquerda do endpoint e selecione **Excluir**.  
Você deve excluir manualmente o endpoint.
- 3 Clique em **OK**.

## Editar um endpoint de conteúdo

Você pode editar as configurações de um endpoint de conteúdo existente.

Todos os valores de endpoint de conteúdo podem ser editados separadamente do nome, que é usado em vários logs.

---

**Observação** Quando o vRealize Suite Lifecycle Manager implanta uma instância do vRA ou quando uma instância do vRA é importada para o vRealize Suite Lifecycle Manager, os serviços de gerenciamento de conteúdo importam os endpoints de conteúdo (por tenant) automaticamente por meio de um processo de coleta de dados. Por padrão, todas as políticas são desativadas, portanto você deve editar o endpoint e atribuir as políticas de conteúdo adequadas. Somente um determinado conjunto de usuários pode editar um endpoint de conteúdo, para obter mais informações sobre funções, consulte [Ações de conteúdo](#).

---

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em **Endpoints**, clique nas reticências verticais à esquerda do endpoint e selecione **Editar**.
- 3 Edite os detalhes do endpoint que deseja alterar e clique em **Avançar**.
- 4 Edite as configurações das políticas de endpoint que deseja alterar e clique em **Avançar**.
- 5 Verifique se os detalhes do endpoint de conteúdo estão corretos e clique em **Enviar**.

## Gerenciar conteúdo

Conteúdo é um conjunto de arquivos que contém definições que representam serviços definidos por software.

Depois de adicionar um endpoint de conteúdo para um ou mais ambientes, você pode gerenciar o conteúdo definido por software que cada um desses ambientes contém. É possível usar o vRealize Suite Lifecycle Manager para realizar as seguintes operações no conteúdo:

- Capturar conteúdo de um endpoint
- Implantar para teste e executar testes de unidade
- Fazer check-in do conteúdo
- Liberar conteúdo para produção

Por exemplo, um arquivo YAML para um blueprint do vRealize Automation ou um arquivo XML para um fluxo de trabalho do vRealize Orchestrator. O conteúdo é vinculado de modo que, quando você capturar um blueprint do vRealize Automation, todas as dependências também sejam exibidas no catálogo de conteúdo, e cada uma delas pode ter suas próprias versões. O vRealize Suite Lifecycle Manager exibe as informações de dependências em cada versão do conteúdo. Caracteres / não podem ser usados no nome para Métricas de Tipo de Recurso de Topologia ou Texto. Se eles forem usados, a exportação falhará.

O vRealize Suite Lifecycle Manager não oferece suporte a uma máquina do Azure no gerenciamento de conteúdo para testes e liberação de conteúdo. O blueprint de XaaS "Máquina Azure" é fornecido por padrão com o vRealize Automation. No entanto, não há suporte para a transferência do blueprint de XaaS entre ambientes vRealize Automation.

- [Adicionar conteúdo](#)

Você pode adicionar conteúdo de um endpoint de conteúdo existente.

- [Excluir diversos conteúdos](#)

Com o vRealize Suite Lifecycle Manager 8.0, você pode excluir vários itens e versões de conteúdo. O recurso de exclusão múltipla pode excluir todas as versões relacionadas ao item de conteúdo selecionado.

- [Trabalhar com conteúdo capturado](#)

Você pode capturar uma nova versão de um pacote de conteúdo existente.

- [Ações de conteúdo](#)

Depois de capturar um conteúdo, você pode executar e visualizar a atividade de um conteúdo.

- [Tipos de conteúdo disponíveis para os produtos](#)

Os pacotes de conteúdo disponíveis para cada endpoint são exibidos nas tabelas a seguir.

- [Como pesquisar conteúdo](#)

Você pode pesquisar um conteúdo existente com base em determinadas entradas definidas na interface do usuário.

- [Conteúdo do teste](#)

Você pode testar o conteúdo para garantir que esteja pronto para liberação.

- [Controle de origem com o gerenciamento do ciclo de vida de conteúdo vRealize Suite Lifecycle Manager](#)

O gerenciamento do ciclo de vida de conteúdo do vRealize Suite Lifecycle Manager integra-se nativamente a um endpoint de ramificação GitLab e Bitbucket definido para fornecer controle de origem para o conteúdo.

- [Implementar um pacote de conteúdo](#)

Implemente um pacote de conteúdo quando estiver pronto para um ambiente de produção.

- [Pacote de vários lançamentos de conteúdo](#)

O gerenciamento de conteúdo do vRealize Suite Lifecycle Manager 8.0 permite o lançamento em massa de conteúdo abrangendo diferentes tipos em que o vSphere, o vRealize Operations Manager ou o vRealize Automation são implantados em uma solicitação. Ele fornece uma opção avançada de filtro no tipo de conteúdo, que é estabelecida a partir de um endpoint de conteúdo específico.

- [Excluir um pacote de conteúdo](#)

Você pode excluir um pacote de conteúdo de todos os endpoints quando o pacote de conteúdo não for mais necessário.

- [Problemas de conteúdo que podem ser encontrados](#)

Pode haver problemas de conteúdo que podem ser encontrados durante qualquer operação de conteúdo.

## Adicionar conteúdo

Você pode adicionar conteúdo de um endpoint de conteúdo existente.

### Pré-requisitos

Verifique se você adicionou um endpoint de conteúdo.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em **Conteúdo**, clique em **ADICIONAR CONTEÚDO**.  
Se uma versão já tiver sido capturada, um conteúdo poderá ser adicionado com o botão **Adicionar conteúdo** ou com uma captura em linha.
- 3 Selecione testar ou implantar o pacote de conteúdo, além de capturar esse pacote, e clique em **CONTINUAR**.
- 4 Digite os detalhes de captura no pacote de conteúdo.
  - a No menu suspenso **Selecionar Endpoint de Captura**, você pode selecionar um ou vários tipos de conteúdo para capturar o conteúdo.
  - b Digite um nome de tag e selecione **Incluir todas as dependências** para capturar as dependências associadas ao conteúdo.

Você pode procurar conteúdo por tag na IU/API.

- c Digue o **Nome do Pacote vRO**. Todos os espaços no nome são substituídos por um caractere de sublinhado \_ e um nome do pacote vRO.

O Nome do Pacote vRO é aplicável apenas para vRealize Orchestrator ou conteúdo do vRealize Automation que tenha algumas dependências do vRealize Orchestrator. O campo é usado para gerenciar conteúdo do vRealize Orchestrator de uma maneira eficiente. Se você fornecer qualquer novo nome, todos os conteúdo do vRealize Orchestrator serão mesclados em um pacote. Se você selecionar um nome existente no menu suspenso, uma nova versão do pacote será criada e mescla todo o conteúdo da versão do vRealize Orchestrator. Se já existir uma versão do pacote desse endpoint, a nova versão terá conteúdo antigo na versão anterior com novo conteúdo. Isso ajuda você a trabalhar de forma incremental no conteúdo do vRealize Orchestrator.

Se o pacote vRealize Orchestrator não for capturado antes de um determinado endpoint de conteúdo, cria-se uma nova versão, mas o conteúdo pode não ser igual à versão anterior. Implemente o pacote adicionado do vRealize Orchestrator no endpoint de conteúdo do vRealize Orchestrator primeiro para anexar o conteúdo. Se você não inserir nenhum nome de pacote, o nome do pacote vRealize Orchestrator corresponde ao conteúdo que é capturado com um "-vro" adicionado como parte do nome. Todo o conteúdo descoberto e o conteúdo do vRealize Orchestrator, incluindo fluxos de trabalho individuais nos arquivos de conteúdo, aparecem no pacote do vRealize Orchestrator que é criado.

- d Se o conteúdo estiver pronto para produção, selecione **Marcar esta versão como pronta para produção**.
- e Digue uma descrição para esta versão de conteúdo no campo **Comentários**.
- f Clique em **Avançar**.

---

**Observação** Quando você lista o conteúdo pela primeira vez para um endpoint, a IU recupera o conteúdo do endpoint. No entanto, depois de capturado, o conteúdo é armazenado em cache e uma atualização automática da lista de conteúdo é executada em segundo plano a cada 30 minutos. Você pode selecionar a opção **Obter conteúdo mais recente** para recuperar o conteúdo nesse período.

- 5 Digue os detalhes do teste para o endpoint de conteúdo.

Essa opção só será exibida se você optar por testar o pacote de conteúdo.

- a Seleccione um ou mais endpoints de conteúdo para especificar os ambientes nos quais os testes devem ser executados.
- b Seleccione **Implantar conteúdo** para implantar o conteúdo no endpoint antes de executar os testes.
- c Seleccione **Parar a implantação de teste na primeira falha** para interromper a implantação de teste quando encontrar um erro.
- d Seleccione **Executar testes da unidade** para executar os testes da unidade disponíveis no conteúdo.

- e Selecione **Parar os testes da unidade na primeira falha** para interromper os testes se algum teste da unidade falhar.
  - f Selecione um servidor para executar testes de unidade no menu suspenso **Selecionar um servidor de teste da unidade**.  
Você deve ter um pacote de teste do vRealize Orchestrator para usar um servidor de teste da unidade.
  - g Clique em **Avançar**.
- 6 Digite os detalhes de check-in do pacote de conteúdo.  
Essa opção só será exibida se você optar por verificar o pacote de conteúdo.
- a Selecione um ou mais endpoints de conteúdo no menu suspenso **Selecionar liberação de endpoints** para especificar os ambientes de produção em que o sistema libera o conteúdo.
- 7 Clique em **ENVIAR**.

Se você selecionou uma única captura de conteúdo, poderá visualizar um único pipeline de conteúdo. Se você tiver selecionado várias capturas de conteúdo, poderá ver os pipelines de captura individuais acionados para cada um dos conteúdos.

## Excluir diversos conteúdos

Com o vRealize Suite Lifecycle Manager 8.0, você pode excluir vários itens e versões de conteúdo. O recurso de exclusão múltipla pode excluir todas as versões relacionadas ao item de conteúdo selecionado.

### Pré-requisitos

Verifique se existe um item de conteúdo já disponível na lista de conteúdo.

### Procedimentos

- 1 No dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em Conteúdo, selecione o item de conteúdo na caixa de seleção.
- 3 Clique em **Ações** e selecione **Excluir**.

Quando o item de conteúdo é excluído, as versões do conteúdo associadas também são excluídas. Se houver mais de um item de conteúdo, selecione todos e clique em Excluir. Você pode executar a operação de exclusão múltipla para até 15 itens de conteúdo.

## Trabalhar com conteúdo capturado

Você pode capturar uma nova versão de um pacote de conteúdo existente.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.

- 2 Em **Conteúdo**, clique no nome do pacote de conteúdo a ser capturado e clique em **CAPTURAR**.
- 3 No menu suspenso **Selecionar Capturar endpoint**, selecione o endpoint de conteúdo a ser capturado.
- 4 Selecione **Incluir todas as dependências** para capturar as dependências associadas ao conteúdo.
- 5 Se o conteúdo estiver pronto para produção, selecione **Marcar esta versão como pronta para produção**.
- 6 Digite uma descrição para esta versão de conteúdo no campo **Comentários** e clique em **CAPTURAR**.

## Ações de conteúdo

Depois de capturar um conteúdo, você pode executar e visualizar a atividade de um conteúdo.

### Implementação de conteúdo

Configurações de conteúdo	Função	Comportamento esperado
A versão do conteúdo está pronta para a produção	Gerenciador de liberação	Você pode exibir apenas endpoints de produção.
A versão do conteúdo está pronta para a produção	Desenvolvedor	Você pode testar endpoints que têm as políticas de teste definidas e não pode incluir as políticas de produção.
A versão do conteúdo NÃO está marcada como pronta para a produção	Gerenciador de liberação Desenvolvedor	Você pode visualizar os endpoints de teste que têm as políticas de teste definidas.
A versão do conteúdo NÃO está marcada como SourceControlled	Gerenciador de liberação Desenvolvedor	Você pode visualizar os endpoints de conteúdo que não têm as políticas de Controle de Origem definidas no endpoint de conteúdo.
A versão do conteúdo está marcada como SourceControlled	Gerenciador de liberação Desenvolvedor	Todos os endpoints de conteúdo são exibidos com base nas outras condições nesta tabela.

### Como gerenciar tags

As tags podem ser gerenciadas em uma determinada versão para navegar por conteúdo dentro da UI. As tags podem ser úteis como um mecanismo de agrupamento quando o recurso futuro de liberar todo o conteúdo por tag tiver suporte.

### Tipos de conteúdo disponíveis para os produtos

Os pacotes de conteúdo disponíveis para cada endpoint são exibidos nas tabelas a seguir.

## Tipos de conteúdo

**Tabela 5-2. Endpoint de conteúdo do vSphere**

Tipo de conteúdo	Versões de suporte do produto	Descrição
vSphere-CustomSpecification	vSphere vCenter 6.0 ou superior	Captura as configurações do sistema operacional convidado salvas em uma especificação que você pode aplicar ao clonar máquinas virtuais ou implantar dos modelos.
vSphere-Template	vSphere vCenter 6.0 ou superior	Captura o modelo para implantar máquinas virtuais no inventário do vCenter Server.

**Tabela 5-3. Endpoint de conteúdo do vRealize Automation 8.x**

Tipo de conteúdo	Versões compatíveis do vRealize Suite Lifecycle Manager	Descrição
Automation-CloudTemplate (versão vRealize Automation 8.2. Para o vRealize Automation versão 8.1 e anteriores, o tipo de conteúdo era conhecido como Automation-CompositeBlueprint)	vRealize Suite Lifecycle Manager 8.1 e versões posteriores.	Captura um blueprint composto do vRealize Automation para implantar máquinas virtuais gerenciadas pelo vRealize Automation.
Automation-PolicyDefinition (vRealize Automation 8.0 e versões posteriores. Antes do lançamento do vRealize Automation 8.0, o tipo de conteúdo era conhecido como Automation- PropertyDefinition)	vRealize Suite Lifecycle Manager 8.1 e versões posteriores.	Captura uma definição de propriedade do vRealize Automation para a especificação de propriedades personalizadas.
Automation-ResourceAction	vRealize Suite Lifecycle Manager 8.2 e versões posteriores.	Captura uma ação de recurso do vRealize Automation.
Automation-Subscription	vRealize Suite Lifecycle Manager 8.1 e versões posteriores.	Captura eventos de assinatura do vRealize Automation que são acionados usando o agente de eventos. Captura os eventos configurados e os fluxos de trabalho dependentes.
Automation-XaaSBlueprint	vRealize Suite Lifecycle Manager 8.1 e versões posteriores.	Captura blueprints XaaS do vRealize Automation.
Automation-CustomResource (no vRealize Suite Lifecycle Manager 8.2, o tipo de conteúdo é conhecido como Automation-Resource Type)	vRealize Suite Lifecycle Manager 8.2 e versões posteriores.	Captura o tipo de recurso do vRealize Automation
Automation-ABXAction	vRealize Suite Lifecycle Manager 8.3 e versões posteriores.	Captura, testa e libera ABXActions do vRealize Automation.
Automation-PropertyGroup	vRealize Suite Lifecycle Manager 8.4 e versões posteriores.	Captura um grupo de propriedades do vRealize Automation para agrupar propriedades personalizadas.

**Tabela 5-4. Endpoint na nuvem do vRealize Automation**

<b>Tipo de conteúdo</b>	<b>Versões compatíveis do vRealize Suite Lifecycle Manager</b>	<b>Descrição</b>
Automation-CloudTemplate	vRealize Suite Lifecycle Manager 8.3.	Captura um blueprint composto do vRealize Automation para implantar máquinas virtuais gerenciadas pelo vRealize Automation.
Automation-PolicyDefinition	vRealize Suite Lifecycle Manager 8.3.	Captura uma definição de propriedade do vRealize Automation para a especificação de propriedades personalizadas.
Automation-ResourceAction	vRealize Suite Lifecycle Manager 8.3.	Captura uma ação de recurso do vRealize Automation.
Automation-Subscription	vRealize Suite Lifecycle Manager 8.3.	Captura eventos de assinatura do vRealize Automation que são acionados usando o agente de eventos. Captura os eventos configurados e os fluxos de trabalho dependentes.
Automation-XaaSBlueprint	vRealize Suite Lifecycle Manager 8.3.	Captura blueprints XaaS do vRealize Automation.
Automation-CustomResource	vRealize Suite Lifecycle Manager 8.3.	Captura o tipo de recurso do vRealize Automation
Automation-ABXAction	vRealize Suite Lifecycle Manager 8.3.	Captura, testa e libera ABXActions do vRealize Automation.
Automation-PropertyGroup	vRealize Suite Lifecycle Manager 8.4.	Captura um grupo de propriedades do vRealize Automation para agrupar propriedades personalizadas.

**Observação** A convenção de nomenclatura para o tipo de conteúdo do vRealize Automation 8.x pode mudar para a versão 8.3 do vRealize Suite Lifecycle Manager.

**Tabela 5-5. Endpoint de conteúdo do vRealize Automation 7.x**

<b>Tipo de conteúdo</b>	<b>Versões compatíveis do vRealize Suite Lifecycle Manager</b>	<b>Descrição</b>
Automation-CompositeBlueprint	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura um blueprint composto do vRealize Automation para implantar máquinas virtuais gerenciadas pelo vRealize Automation.
Automation- Componentprofile	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura um perfil de componente do vRealize Automation.
Automation- PropertyDefinition	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura uma definição de propriedade do vRealize Automation para a especificação de propriedades personalizadas.

**Tabela 5-5. Endpoint de conteúdo do vRealize Automation 7.x (continuação)**

<b>Tipo de conteúdo</b>	<b>Versões compatíveis do vRealize Suite Lifecycle Manager</b>	<b>Descrição</b>
Automation-ResourceAction	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura uma ação de recurso do vRealize Automation.
Automation-Software	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura uma ação de recurso do vRealize Automation.
Automation-Subscription	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura as configurações dos componentes do software vRealize Automation que controlam como o middleware ou os aplicativos são instalados, configurados e desinstalados.
Automation-CustomForm	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura o formulário do cliente do vRealize Automation.
Automation-ResourceType	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura tipos de recursos do vRealize Automation.
Automation-ResourceMap	vRealize Suite Lifecycle Manager 2.1 e versões posteriores.	Captura mapas de recursos do vRealize Automation.

**Tabela 5-6. Endpoint de conteúdo do vRealize Operations Manager**

<b>Tipo de conteúdo</b>	<b>Versões de suporte do produto</b>	<b>Descrição</b>
Alerta de operações	vRealize Operations Manager 6.6.1 ou superior	Captura alertas do vRealize Operations contendo definições de sintomas e recomendações que são usadas para avaliar condições e gerar alertas.
Operations-Dashboard	vRealize Operations Manager 6.6.1 ou superior	Captura os dados do dashboard de alertas do vRealize Operations usados para determinar a natureza e o período de tempo dos problemas existentes e potenciais.
Operations-Report	vRealize Operations Manager 6.6.1 ou superior	Captura modelos de relatório do vRealize Operations
Operations-SuperMetric	vRealize Operations Manager 6.6.1 ou superior	Integra a definição de dados de supermétricas do vRealize Operations que é usada para rastrear combinações de métricas. Após liberar as supermétricas, atribuir um ou mais tipos de objeto e ativá-las nas políticas ainda é necessário. Todos os tipos de pacote do vRealize Operations também oferecem suporte às supermétricas, o que significa que os painéis, alertas, visualizações e configurações de métricas apontam automaticamente para a supermédia correta no momento da liberação.
Operations- TextWidgetContent	vRealize Operations Manager 6.6.1 ou superior	Lê o texto de uma página da Web ou arquivo de texto. Você especifica a URL da página da Web ou o nome do arquivo de texto ao configurar o widget de Texto.

**Tabela 5-6. Endpoint de conteúdo do vRealize Operations Manager (continuação)**

<b>Tipo de conteúdo</b>	<b>Versões de suporte do produto</b>	<b>Descrição</b>
Operations- TopoWidgetConfig	vRealize Operations Manager 6.6.1 ou superior	Captura a estrutura da topografia em torno de um recurso específico, incluindo os recursos principais e herdeiros.
Operations-View	vRealize Operations Manager 6.6.1 ou superior	Captura visualizações do vRealize Operations que ajudam a interpretar métricas, propriedades e políticas de vários objetos monitorados.
Operations- ResourceKindMetricConfig	vRealize Operations Manager 6.6.1 ou superior	Captura as configurações de métricas do vRealize Operations para adaptadores e tipos de objetos específicos, para que os widgets compatíveis sejam preenchidos com base nas métricas configuradas e no tipo de objeto selecionado.
Operations-Symptoms	vRealize Operations Manager 6.6.1 ou superior	Captura os sintomas de operação.

**Tabela 5-7. Endpoint de conteúdo do vRealize Orchestrator**

<b>Tipo de conteúdo</b>	<b>Versões de suporte do produto</b>	<b>Descrição</b>
Orchestrator-Action	vRealize Orchestrator versão 7.0 ou superior	Captura uma ação do vRealize Orchestrator.
Orchestrator- ConfigurationElement	vRealize Orchestrator versão 7.0 ou superior	Captura um elemento de configuração do vRealize Orchestrator.
Orchestrator- Package	vRealize Orchestrator versão 7.0 ou superior	Captura um pacote do vRealize Orchestrator.
Orchestrator- RestHost	vRealize Orchestrator versão 7.6+	Captura um host REST do vRealize Orchestrator.
Orchestrator- RestOperation	vRealize Orchestrator versão 7.6+	Captura uma operação REST do vRealize Orchestrator.
Orchestrator- Workflow	vRealize Orchestrator versão 7.0 ou superior	Captura um fluxo de trabalho do vRealize Orchestrator.

**Observação** Certifique-se de que o Orchestrator-RestHost esteja disponível no vRealize Orchestrator de destino antes de capturar ou implantar o Orchestrator-RestOperation.

## Como pesquisar conteúdo

Você pode pesquisar um conteúdo existente com base em determinadas entradas definidas na interface do usuário.

- Os arquivos de dependência e dependências de conteúdo podem ser vistos ao clicar na versão e observar a guia DEPENDÊNCIAS .
- Clicando em cada arquivo, você pode baixá-lo do repositório de conteúdo do vRealize Suite Lifecycle Manager.

## Conteúdo do teste

Você pode testar o conteúdo para garantir que esteja pronto para liberação.

### Pré-requisitos

Verifique se o pacote de conteúdo foi adicionado ao vRealize Suite Lifecycle Manager.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de Conteúdo**.
- 2 Em **Conteúdo**, clique no nome do pacote de conteúdo a ser capturado.
- 3 Clique nos três pontos horizontais à direita da versão para testar e selecione **Testar**.
- 4 Selecione um ou mais endpoints de conteúdo para especificar os ambientes nos quais executar os testes.
- 5 Selecione **Implantar conteúdo** para implantar o conteúdo no endpoint antes de executar os testes.
- 6 Selecione **Parar a implementação de teste na primeira falha** para interromper a implantação de teste assim que um erro for encontrado.
- 7 Selecione **Executar testes da unidade** para executar os testes da unidade disponíveis no conteúdo.
- 8 Selecione **Parar os testes da unidade na primeira falha** para interromper os testes se algum teste da unidade falhar.
- 9 Selecione **Incluir todas as dependências** para incluir todas as dependências associadas ao pacote de conteúdo nos testes.
- 10 Selecione **Liberar as dependências mais recentes** para liberar as versões mais recentes das dependências associadas ao pacote de conteúdo.
- 11 Selecione um servidor para executar testes de unidade no menu suspenso de **Selecionar um servidor de teste de unidade** e clique em **PROCEED**.

### Executar testes de unidade

Ao criar um endpoint de conteúdo, você pode selecionar a política **supportTest** para permitir que o sistema execute testes de unidade após implantar um conteúdo no ambiente de teste.

Existem dois servidores aqui:

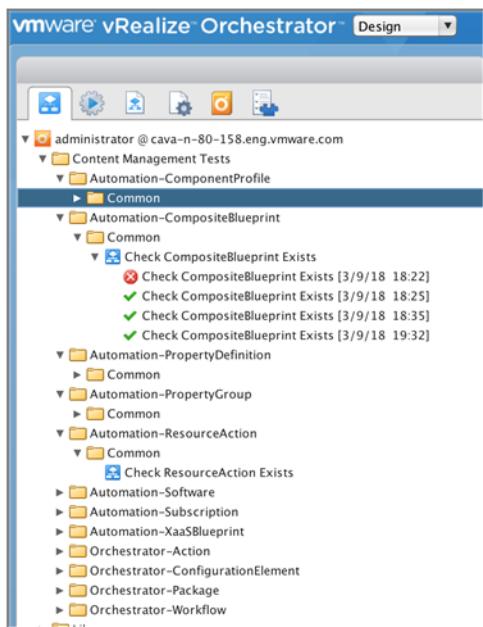
- Servidor de testes de unidade
- Endpoint de teste

O servidor é um ambiente de preparo no qual é possível implantar conteúdo e executar testes de unidade em relação ao conteúdo implantado no ambiente.

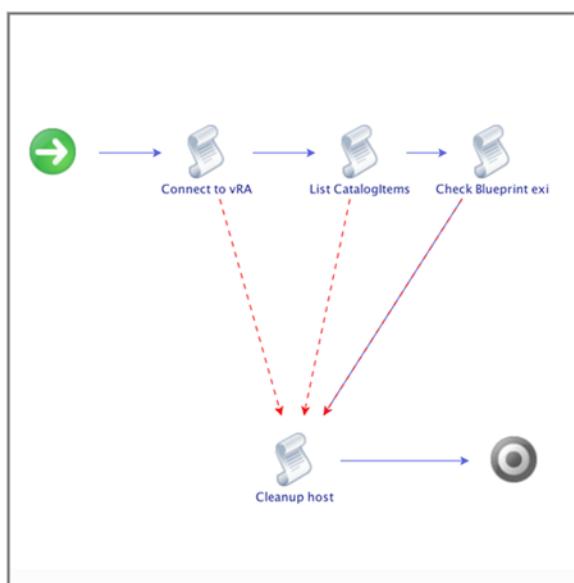
## Servidor de testes de unidade

O servidor de testes é um servidor vRO no qual é possível executar testes de unidade em um conteúdo implantado em um endpoint de teste. Sempre que você define um endpoint de orquestrador como um endpoint de teste, ele testa o pacote do vRealize Orchestrator e é implantado automaticamente nesse endpoint, permitindo testes de unidade ou integração. Existem alguns testes básicos já presentes no pacote, e você pode estender os testes no servidor de testes de unidade também.

Opções de menu para o servidor de testes de unidade



Fluxo de testes de unidade de amostra



## Testes comuns

Todos os testes na pasta PackageType Common são executados.

Se você acessar o servidor de testes de unidade (vRO), em **Testes de Gerenciamento de Conteúdo**, poderá exibir pastas separadas para todos os tipos de conteúdo. Para cada pasta de tipo de conteúdo, há uma pasta **comum** presente na qual é possível ver todos os fluxos de trabalho comuns que são executados para um determinado tipo de conteúdo.

### Testes específicos de pacotes

Testes específicos também podem ser executados por nome de conteúdo. Por exemplo, se um conteúdo de Automation-XaaS Blueprint chamado “Adicionar usuário do AD” solicitar um teste de unidade chamado “Adicionar usuário do AD - Teste 1”, que pode se conectar a um determinado endpoint de conteúdo e executar o Blueprint de XaaS e aguardar para ver se ele foi bem-sucedido. O formato dos testes é:

<content name - test name> e na pasta <Content-Type>.

Sempre que você seleciona o servidor de unidade durante o teste do conteúdo, os novos testes de unidade também são executados com base no tipo de conteúdo em relação ao conteúdo implantado em um endpoint de teste.

A lista a seguir indica a funcionalidade geral dos testes de unidade:

- Fluxos de trabalho de testes de unidade comuns podem ser gravados na pasta **comum** por tipo de conteúdo
- O fluxo de trabalho de testes de unidade para um determinado conteúdo pode ser gravado em <Content Type> e nomeado como <Content name> - <Tests name>.
- Se houver uma falha no teste, este exibirá um erro em um fluxo de trabalho.
- Verifica as entradas disponíveis para testar um fluxo de trabalho

### Fluxos de trabalho de amostra

Você pode consultar os fluxos de trabalho de unidades existentes disponíveis no vRealize Orchestrator (política definida para teste). Navegue até uma pasta comum no vRealize Orchestrator, **Fluxos de Trabalho > Testes de Gerenciamento de Conteúdo > Tipo de Conteúdo > Comum**.

Propriedades de entrada disponíveis para um fluxo de trabalho de testes de unidade fornecido pela plataforma.

Nome da propriedade	Descrição
versão	Versão do conteúdo que está sendo testado.
testEndpointLink	O link do endpoint de conteúdo no repositório.
tenant	O tenant com o qual uma conexão está sendo estabelecida.
packageVersionLink	O link da versão para o repositório.
packageType	Tipo de Conteúdo. Automation-CompositeBlueprint.
packageName	Nome do conteúdo

Nome da propriedade	Descrição
packageId	Identificador exclusivo de conteúdo no repositório.
endpointUser	O nome de usuário do endpoint que está sendo testado.
endpointServer	O nome de servidor do endpoint que está sendo testado.
endpointPassword	A senha (SecureString) do endpoint que está sendo testado.

## Controle de origem com o gerenciamento do ciclo de vida de conteúdo vRealize Suite Lifecycle Manager

O gerenciamento do ciclo de vida de conteúdo do vRealize Suite Lifecycle Manager integra-se nativamente a um endpoint de ramificação GitLab e Bitbucket definido para fornecer controle de origem para o conteúdo.

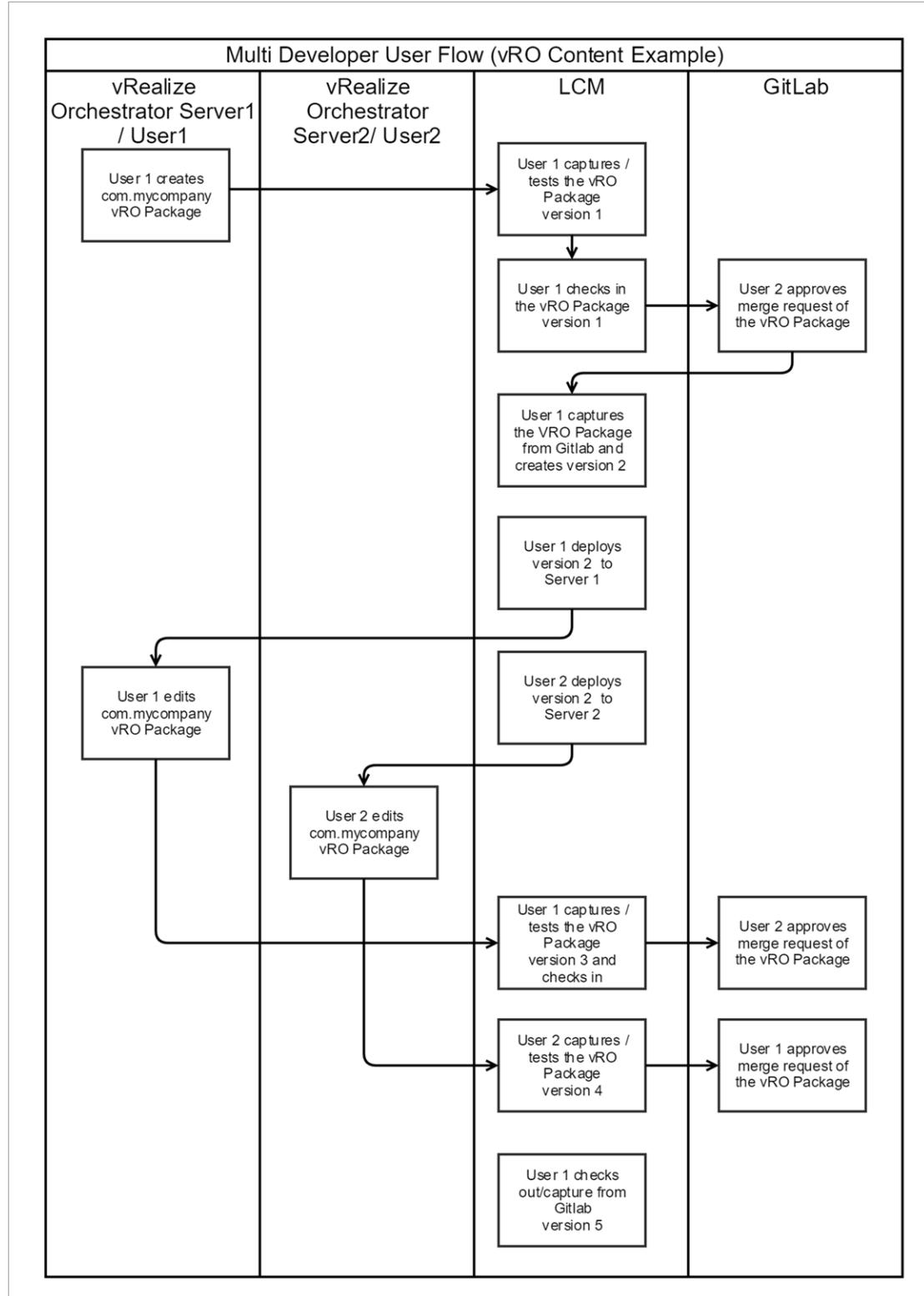
Você pode armazenar conteúdo no repositório controlado pela versão vRealize Suite Lifecycle Manager e em uma ramificação GitLab ou Bitbucket. Isso permite que os desenvolvedores trabalhem juntos para fazer check-in e check-out do conteúdo e para codificar as alterações de revisão antes da implantação em ambientes de teste ou de produção.

O vRealize Suite Lifecycle Manager armazena todos os hashes de confirmação do controle de origem para fins de check-in, para que o estado correto do conteúdo seja conhecido. Isso permite o suporte a vários desenvolvedores, o que reduz o risco de substituir o conteúdo, e reduz o número de conflitos de mesclagem que podem ocorrer.

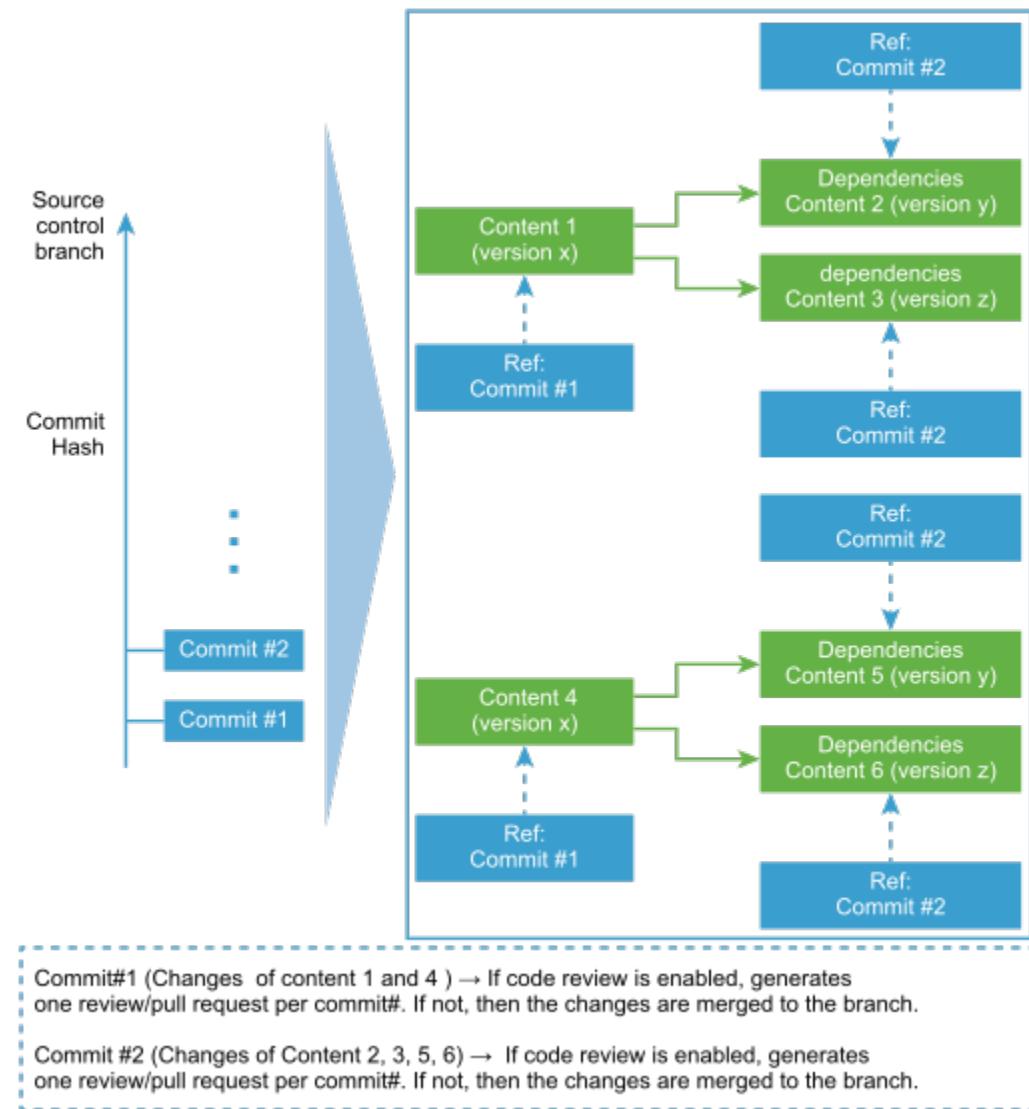
Para usar o controle de origem no vRealize Suite Lifecycle Manager, você deve atender aos seguintes pré-requisitos:

- Verifique se você tem um servidor GitLab ou Bitbucket. Se você não tiver um servidor GitLab existente, é possível usar o contêiner de docker grátis do Gitlab-CE.
- Verifique se pelo menos um usuário do vRealize Suite Lifecycle Manager tem acesso ao GitLab ou Bitbucket.
- Crie uma ramificação no GitLab e aplique as permissões necessárias no GitLab para que outros desenvolvedores façam check-in e check-out do conteúdo na ramificação.
- O usuário do GitLab deve criar um token de acesso no GitLab e armazenar o token na instância do GitLab em vRealize Suite Lifecycle Manager **Configurações de conteúdo**.

Essa é uma prática recomendada sempre que o conteúdo é verificado no controle de origem e a nova versão tiver que ser verificada e implantada em um endpoint de conteúdo. Isso salva as alterações mais recentes de outros desenvolvedores (troca de base efetiva do conteúdo) e também se comunica com os serviços de conteúdo do vRealize Suite Lifecycle Manager nos quais o Hash de confirmação GIT é implantado para o conteúdo por endpoint. Porém, quando você estiver capturando conteúdo do servidor GitLab, o check-out funcionará se você estiver usando a versão 11.6.5 do GitLab ou anterior. Ocorrerá falha na verificação se você estiver usando uma versão do GitLab superior à 11.6.5.



## Conteúdo referente a vários hashes de confirmação



## Fazer check-in do conteúdo em um endpoint de controle de origem

Você pode fazer check-in do conteúdo capturado anteriormente para um endpoint de controle de origem.

### Pré-requisitos

Verifique se você adicionou um endpoint de controle de origem ao vRealize Suite Lifecycle Manager. Consulte [Controle de origem com o gerenciamento do ciclo de vida de conteúdo vRealize Suite Lifecycle Manager](#) para obter os requisitos do controle de origem.

---

**Observação** Suportamos um check-in de conteúdo único, com um máximo de 1.000 arquivos de cada vez.

---

## Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em **Conteúdo**, clique no nome do pacote de conteúdo a ser capturado.
- 3 Clique no nome do pacote de conteúdo a ser testado.
- 4 Clique nos três pontos verticais à direita da versão para fazer check-in e selecione **Check-in**.
- 5 Selecione um endpoint de conteúdo para fazer o check-in do pacote de conteúdo.
- 6 Selecione **Incluir todas as dependências** para incluir todas as dependências associadas ao pacote de conteúdo no check-in.
- 7 Adicione um comentário descritivo no campo **Comentário** e clique em **CHECK-IN**.

**Observação** É obrigatório adicionar um comentário de check-in.

Ao verificar um pacote do vRO, existe um recurso opcional para fazer a mesclagem com um pacote vRO já existente constante no controle de origem. Isso garante que todos os arquivos capturados sejam verificados no caminho do pacote selecionado (mesclado por último). Se você não vir o pacote, **Selecione o tipo de pacote do Orchestrator > do endpoint de controle de origem** atualize o cache e faça check-in para exibir o pacote vRO no qual ele precisa ser mesclado. Você possui os novos recursos a seguir adicionados ao fazer o check-in de um pacote do Orchestrator:

- Você pode fazer a mesclagem de um pacote do orchestrator personalizado de um endpoint com uma versão superior do pacote no LCM.
- A capacidade de fazer a mesclagem de um pacote do Orchestrator personalizado diretamente a um pacote superior no GitLab.
- Você pode liberar um subconjunto de conteúdos de um pacote do Orchestrator durante a implantação em um endpoint.
- Como parte do gerenciamento de dependências, é possível remover a dependência de uma versão de conteúdo.

Para um check-in de conteúdo do vRealize Automation, você pode fazer a mesclagem diretamente no GitLab. Você pode fazer check-out sem dependência ou fazer check-out com dependência, onde é possível realizar o seguinte:

- Você pode remover a dependência do pacote da versão mais recente. Por exemplo, se você executou um check-in de conteúdo do vRealize Automation com dependência e ativou a opção para fazer a mesclagem do pacote do Orchestrator dependente para um pacote superior diretamente no GitLab. Quando você faz check-out do mesmo conteúdo de Automação com dependência de um controle de origem.

## Resultados

Se uma revisão de código estiver desativada na ramificação do controle de origem, o conteúdo será mesclado automaticamente.

## Próximo passo

Se uma revisão de código estiver ativada na ramificação do controle de origem, você ou outro revisor de código deverá verificar manualmente o conteúdo no GitLab depois da conclusão da revisão do código. Depois de verificar o conteúdo no GitLab, capture a versão mais recente do conteúdo do servidor de controle de origem no vRealize Suite Lifecycle Manager.

Se você continuar desenvolvendo no endpoint de conteúdo, capture a versão mais recente do conteúdo no controle de origem e implemente-a no endpoint de conteúdo de desenvolvimento. Isso atualiza o endpoint de conteúdo para que o conteúdo seja sincronizado com o controle de origem e os check-ins subsequentes sejam válidos.

Você pode visualizar o status de check-in no [Log de Atividades](#).

## Fazer check-out de conteúdo de um endpoint de controle de origem

Depois de fazer o check-in de um conteúdo em um endpoint de controle de origem, você pode check-out do conteúdo e implementá-lo em um endpoint de conteúdo. Quando o check-out do conteúdo for verificado do controle de origem, o conteúdo será marcado com o código hash do Git para referência.

### Pré-requisitos

Verifique se foi feito o check-in do conteúdo no endpoint de controle de origem. Consulte [Fazer check-in de conteúdo para um endpoint de controle de origem](#).

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
  - 2 Em **Conteúdo**, clique em **ADICIONAR CONTEÚDO**.
- 
- Observação** Você também pode fazer check-out do conteúdo em linha.
- 3 Escolha se deseja testar ou implantar o pacote de conteúdo, além de capturá-lo, e clique em **CONTINUAR**.
  - 4 Digite os detalhes de captura no pacote de conteúdo.
    - a No menu suspenso **Selecionar endpoint de captura**, selecione o endpoint de controle de origem para capturar o conteúdo.
    - b Selecione **Obter conteúdo mais recente** para recuperar as dependências de conteúdo mais recentes em vez das dependências com as quais o conteúdo foi inicialmente capturado.
    - c Selecione o tipo de conteúdo e o conteúdo a ser capturado.
    - d Selecione **Incluir todas as dependências** para capturar as dependências associadas ao conteúdo.

As dependências são armazenadas no vRealize Suite Lifecycle Manager, não no endpoint de controle de origem.

- e Se o conteúdo estiver pronto para produção, selecione **Marcar esta versão como pronta para produção**.
  - f Digite uma descrição para esta versão de conteúdo no campo **Comentários**.
  - g Clique em **Avançar**.
- 5 Digite os detalhes do teste para o endpoint de conteúdo.
- Essa opção será exibida somente se você selecionou testar o pacote de conteúdo.
- a Selecione um ou mais endpoints de conteúdo para especificar os ambientes nos quais executar os testes.
  - b Selecione **Implantar conteúdo** para implantar o conteúdo no endpoint antes de executar os testes.
  - c Selecione **Parar a implantação de teste na primeira falha** para interromper a implantação de teste assim que encontrar um erro.
  - d Selecione **Executar testes da unidade** para executar os testes da unidade disponíveis no conteúdo.
  - e Selecione **Parar os testes da unidade na primeira falha** para interromper os testes se algum teste da unidade falhar.
  - f Selecione um servidor para executar testes de unidade no menu suspenso **Selecionar um servidor de teste da unidade**.
- Você deve ter um pacote de teste do vRealize Orchestrator importado para usar um servidor de teste da unidade.
- g Clique em **Avançar**.
- 6 Digite os detalhes de implantação no pacote de conteúdo.
- Essa opção será exibida somente se você optar por testar o pacote de conteúdo.
- a Selecione um ou mais endpoints de conteúdo no menu suspenso **Selecionar Liberação de Endpoints** para especificar os ambientes de produção em que o sistema libera o conteúdo.
  - b Selecione **Parar implantação de liberação na primeira falha** para interromper a implantação assim que o sistema encontrar uma falha.
  - c Digite um comentário que explique por que o conteúdo está sendo liberado no campo **Publicar comentário** pois a redação de comentários é obrigatória.
- 7 Clique em **ENVIAR**.

## Resultados

O vRealize Suite Lifecycle Manager captura o conteúdo do endpoint de controle de origem e cria uma nova versão do conteúdo no catálogo de conteúdo. Esta versão está marcada como **Controle de Origem Ativado**, que informa ao vRealize Suite Lifecycle Manager o estado do conteúdo durante a implementação em um endpoint de conteúdo, de forma que o conteúdo seja verificado em relação ao momento certo.

## Próximo passo

Se você estiver usando o controle de origem e tiver vários endpoints de conteúdo de captura, apenas a implementação de conteúdo do catálogo de conteúdo será marcada como **Controle de origem ativado**. Isso comunica o estado do conteúdo ao implantar em um endpoint de conteúdo para que o conteúdo seja verificado em relação ao momento certo.

## Implementar um pacote de conteúdo

Implemente um pacote de conteúdo quando estiver pronto para um ambiente de produção.

### Pré-requisitos

- Verifique se o ambiente de produção foi adicionado como um endpoint de conteúdo.
- Verifique se o conteúdo está pronto para um ambiente de produção.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Clique em **Conteúdo** e no nome do pacote de conteúdo a ser implantado.
- 3 Clique em **IMPLANTAR** para a versão a ser implantada.
- 4 Selecione um ou mais endpoints de conteúdo no menu suspenso **Selecionar liberação de endpoints** para especificar os ambientes de produção em que o sistema libera o conteúdo.
- 5 Selecione **Parar a implantação de versão na primeira falha** para interromper uma implantação quando o sistema encontrar uma falha.
- 6 Selecione **Incluir todas as dependências** para implantar todas as dependências associadas ao pacote de conteúdo.
- 7 Selecione **Liberar as dependências mais recentes** para liberar as versões mais recentes das dependências associadas ao pacote de conteúdo.
- 8 Digite um comentário que explica por que o conteúdo está sendo liberado no campo **Comentário da liberação** e clique em **PROSSEGUIR**.

## Pacote de vários lançamentos de conteúdo

O gerenciamento de conteúdo do vRealize Suite Lifecycle Manager 8.0 permite o lançamento em massa de conteúdo abrangendo diferentes tipos em que o vSphere, o vRealize Operations Manager e o vRealize Automation são implantados em uma solicitação. Ele fornece uma opção

avançada de filtro no tipo de conteúdo, que é estabelecida a partir de um endpoint de conteúdo específico.

Vários conteúdos são selecionados como parte de uma solicitação de vários lançamentos. A falha em implantar um dos conteúdos selecionados não reverterá os conteúdos implantados que fazem parte dessa solicitação.

## Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Em **Conteúdo**, selecione **Lista de itens de conteúdo**.
- 3 Expanda a árvore **Filtro aplicado**.
- 4 Na seção Filtro de conteúdo, você pode filtrar por uma única tag ou várias tags, Tipo, Endpoint e Política para chegar a um subconjunto do conteúdo que deseja exibir e implantar.

Tipo de filtro	Descrição
Filtros de conteúdo	Esta seção lista os filtros de conteúdo. <ul style="list-style-type: none"> <li>■ Produção pronta</li> <li>■ Conteúdo de desenvolvimento</li> <li>■ Testado</li> <li>■ Origem controlada</li> <li>■ Dependências capturadas</li> </ul>
Tipos de conteúdo	Esta seção lista a categoria de conteúdo com base no tipo de conteúdo.
Endpoints de conteúdo	Esta seção lista todos os endpoints de conteúdo associados.

- 5 Depois de selecionar um filtro de conteúdo, você pode adicionar uma etiqueta e clicar em **Aplicar**.

Uma tag é associada quando um conteúdo é criado. Um filtro baseado em tags é útil quando você deseja pesquisar. No entanto, ainda é possível adicionar a tag mesmo depois de criar o conteúdo. Você também pode gerenciar tags em massa para todo o conteúdo e versões mais antigas.

- 6 Para salvar seus filtros, clique em **Salvar**.

Os desenvolvedores podem apenas visualizar seus filtros e os gerentes de lançamento podem visualizar todos os outros filtros RM. Os filtros salvos podem ser editados ou excluídos.

Após definir os filtros de conteúdo, a exibição de conteúdo padrão muda para **Lista de versões de conteúdo**. Ao fornecer um filtro, você pode localizar uma versão específica do conteúdo, por exemplo, Conteúdo Pronto para Produção com uma tag específica e de um conjunto específico de tipos de conteúdo. Por exemplo, exibir apenas modelos do vSphere, painéis do vRealize Operations Manager e blueprints do vRealize Automation.

- 7 Para implantar o conteúdo em um endpoint de versão, siga o assistente.

**8** Clique em **Ações** e selecione **Check-in**.

**Observação** Com o Lifecycle Manager 8,0, você pode fazer check-in de vários conteúdos depois de filtrar e selecionar conteúdo. Quando você estiver realizando uma captura múltipla, teste e liberação, verifique se todas as capturas foram bem-sucedidas porque, se uma das capturas de conteúdo falhar, todo o pipeline de conteúdo será marcado como com falha. Com base na falha de pipeline de captura múltipla, você não pode passar para a próxima etapa de teste e liberação de um pipeline.

**9** Para fazer check-in de vários conteúdos.

- a Seleccione um **Repositório de endpoint**.
- b se quiser capturar todas as dependências, selecione **Incluir todas as dependências** e faça a mesclagem do pacote vRO, se necessário.
- c Clique em **Check-in**.

**10** Selecione um endpoint apropriado para cada tipo de conteúdo que será exibido.

**Observação** Os endpoints do Orchestrator são assumidos pela instância de automação primário. Se houver endpoints autônomos do Orchestrator configurados, você também poderá implantá-los.

## Excluir um pacote de conteúdo

Você pode excluir um pacote de conteúdo de todos os endpoints quando o pacote de conteúdo não for mais necessário.

Esta operação não poderá ser desfeita.

### Pré-requisitos

- Verifique se um ou mais endpoints de conteúdo foram adicionados.
- Verifique se o pacote de conteúdo está presente na implantação.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Clique em **Conteúdo** e, em seguida, clique no nome do pacote de conteúdo a ser excluído.
- 3 Clique nos três pontos horizontais à direita da versão e selecione **Excluir**.
- 4 Clique em **OK**.

Para que as alterações sejam exibidas na UI, atualize a página.

## Problemas de conteúdo que podem ser encontrados

Pode haver problemas de conteúdo que podem ser encontrados durante qualquer operação de conteúdo.

- Ao transferir uma especificação de personalização entre servidores vCenter, os campos de senha não podem ser descriptografados pelo destino. Isso faz com que as implantações que dependem de especificações personalizadas com senhas falhem. Você pode inserir manualmente o valor correto no campo Senha do administrador após a especificação de personalização ser implantada pelo Lifecycle Manager pipeline.
- Quando uma definição de sintoma é configurada com REGEX ou NOT\_REGEX, a importação falha ao usar as APIs do vRealize Operations Manager com o seguinte erro. **Erro ao liberar a mensagem Operations-Symptom= "Solicitação inválida... violações de #1 encontradas.", "validationFailures": [{"failureMessage": "Campo de Condição de Evento de Mensagem 'operador' deve ser EQ ou CONTAINS"}**. Se um sintoma usar REGEX, o conteúdo precisará ser importado manualmente por meio da UI do Lifecycle Manager.
- A liberação de conteúdo de diferentes versões do vRealize Operations Manager pode falhar. Por exemplo, o conteúdo da 6.6 para a 6.7 alguns tipos de conteúdo podem falhar.
- Uma execução de pipeline com um grande número de capturas ou check-ins poderá falhar se o número de execuções for maior que o suportado pelo tipo de endpoint. Por exemplo, a nuvem bitbucket pode suportar 1.000 acessos por hora ao repositório.

## Controle de origens de acesso

Apenas um gerente de liberação pode adicionar um acesso de controle de origem, no qual o controle de origem pode ser o GitLab ou o Bitbucket. Com esse privilégio, um gerente de liberação pode selecionar o tipo GitLab, Bitbucket e inserir o nome do servidor GitLab. Você pode fornecer vários nomes de servidor e, em seguida, usar o token de acesso pessoal do GitLab e atribuí-lo ao servidor de controle de origem.

Ao habilitar o controle de origem de acesso, você pode adicionar um endpoint para um controle de origem. Para obter informações sobre como adicionar um controle de origem, consulte [Adicionar um endpoint do servidor de controle de origem](#). O gerente de liberação pode adicionar um servidor de controle de origem. Porém, qualquer desenvolvedor conectado ao vRealize Suite Lifecycle Manager precisa associar seu token ao servidor para acessar o servidor de controle de origem.

## Como gerenciar endpoints de servidores de controle de origem

Antes de você poder fazer o check-in ou o check-out do conteúdo, um vRealize Suite Lifecycle Manager deve adicionar um servidor de controle de origem GitLab ou Bitbucket ao sistema.

- [Adicionar um endpoint do servidor de controle de origem](#)

Para adicionar um servidor de controle de origem ao sistema, adicione um endpoint do servidor de controle de origem.

- [Excluir um endpoint do servidor de controle de origem](#)

Você pode excluir um endpoint do servidor de controle de origem que não está mais em uso.

### Adicionar um endpoint do servidor de controle de origem

Para adicionar um servidor de controle de origem ao sistema, adicione um endpoint do servidor de controle de origem.

Quando você desativa a opção de editor de arquivos, a API do bitbucket (PUT/POST) não funciona para um administrador ou desenvolvedor. Não inclua a propriedade abaixo (feature.file.editor) nos arquivos de propriedade ou, se ela for incluída, certifique-se de que a propriedade seja definida como verdadeira.

Localização:

```
<base_directory>\Atlassian\ApplicationData\Bitbucket\shared\bitbucket.properties
```

Propriedades: feature.file.editor=true

#### Pré-requisitos

- Verifique se você tem uma instância Bitbucket, GitHub ou GitLab com suporte para esta versão do vRealize Suite Lifecycle Manager. Para obter mais informações sobre as versões suportadas do Bitbucket, GitHub ou GitLab, consulte [Gerenciamento do ciclo de vida do conteúdo](#).
- Faça login no GitHub, GitLab ou Bitbucket e gere um token de acesso para o usuário com todos os escopos ativados. Copie e salve este token de uso único do GitHub, GitLab ou Bitbucket.
- Faça login no GitHub, GitLab ou Bitbucket e verifique se você tem grupo, projeto e ramificação criados no GitHub, GitLab ou Bitbucket antes de adicioná-lo como um endpoint de controle de origem.

#### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Clique em **Configurações de Conteúdo**.

- 3 Na guia **Acesso ao controle de origem**, clique em **ADICIONAR SERVIDOR DE CONTROLE DE ORIGEM**.
- 4 Selecione o **Tipo de Controle de Origem**.

---

**Observação** Agora, com o vRealize Suite Lifecycle Manager 8.0, você pode selecionar Servidor do Bitbucket ou Nuvem do Bitbucket.

---

- 5 Digite o endereço IP ou o nome de domínio completo do servidor e clique em **ENVIAR**.

Por padrão, o vRealize Suite Lifecycle Manager usa o esquema `https` para quaisquer APIs de controle de origem. Se você não tiver ativado o `https` na instância do GitLab, especifique o endereço `http://<endereço IP>:<porta>` no servidor de controle de origem, na página de configurações de conteúdo, para alterar o esquema. Quando você cria o endpoint de controle de origem, o repositório deve ser especificado no formato `<GroupName>/<ProjectName>`. Sempre que vários desenvolvedores estiverem trabalhando no repositório de buckets de bits, o desempenho é lento na versão corporativa do bucket de bits. Portanto, você pode usar pelo menos 4 máquinas vCPU de bucket de bits.

- 6 Clique no ícone de lápis do servidor de controle de origem.
- 7 Digite o token de acesso do servidor GitLab ou Bitbucket na caixa de texto **CHAVE DE ACESSO** e clique em **ENVIAR**.
  - a Para uma instância do GitHub, você pode optar por inserir a credencial da instância do GitHub fornecendo o nome de usuário e a senha ou inserir o token de acesso.
  - b Clique em **ENVIAR**.

Um token de acesso é uma identidade exclusiva para um usuário realizar o check-in ou o check-out para rastrear o GitLab ou a API do GitHub. Para criar um token de acesso para o GitLab ou o GitHub, acesse a URL do servidor do GitLab ou GitHub. Por exemplo, `gitlab.exemplo.com` ou `github.com`. Para o servidor e para a nuvem do Bitbucket, navegue até `bitbucket.org` e Senhas do aplicativo para criar uma senha com todas as permissões.

## Excluir um endpoint do servidor de controle de origem

Você pode excluir um endpoint do servidor de controle de origem que não está mais em uso.

### Pré-requisitos

Verifique se o endpoint do servidor de controle de origem não está sendo usado por nenhum endpoint de conteúdo.

### Procedimentos

- 1 No Dashboard Meus Serviços, clique em **Gerenciamento de conteúdo**.
- 2 Clique em **Configurações de Conteúdo**.
- 3 Na guia **Acesso ao Controle de Origem**, clique no ícone de lixeira para o endpoint do servidor de controle de origem a ser excluído.

- 4 Clique em **OK**.

## Como trabalhar com as configurações de conteúdo

Você pode adicionar o endpoint do servidor de controle de origem, o editor vCenter, a extensibilidade do pipeline e as restrições do desenvolvedor em Configurações de Conteúdo.

### Acesso ao controle de origem

Para adicionar um endpoint de controle de origem, forneça um servidor para esse controle de origem do GitLab. Para obter mais informações, consulte [Adicionar um endpoint do servidor de controle de origem](#).

---

**Observação** Você pode adicionar vários nomes de servidor para um endpoint do servidor de controle de origem e somente o controle de origem do GitLab é compatível com essa versão.

---

### Repositório de modelos do vSphere

A partir do vRealize Suite Lifecycle Manager 1.3 e versões mais recentes, você pode capturar conteúdo do vSphere vCenter Server. O Repositório de modelos do vSphere é uma biblioteca de conteúdo em uma instância designada do vCenter que armazenará todos os modelos capturados nos quais eles podem ser gerenciados a partir do LCM. Uma prática ideal é ter esta instância do vCenter próxima do local em que os modelos normalmente seriam capturados, ou seja, um vCenter de desenvolvimento para a autoria de modelos. Você pode voltar para Endpoints e selecionar vCenter a ser adicionado como seu endpoint. Para obter mais informações, consulte [Adicionar um endpoint de conteúdo do vCenter Server](#). O modelo da Configuração da biblioteca de conteúdo é o seguinte:

- 1 Criar a Biblioteca de Conteúdo (Editor): o Repositório de modelos do vSphere aponta para uma biblioteca de conteúdo que está configurada para publicação. Para obter mais detalhes sobre como configurar uma Biblioteca de Conteúdo do editor, consulte [Documentação do vCenter](#).
- 2 Criar assinantes da biblioteca de conteúdo: cada vCenter Server que opta por um suporte de modelo requer a configuração de uma Biblioteca de Conteúdo, que assinará a Biblioteca Publicada configurada na Etapa 1. As seguintes configurações são necessárias:

Configuração	Descrição
Sincronização automática	Você pode ativar essa configuração para sincronização automática dos metadados do modelo.
URL de assinatura	Essa URL contém detalhes sobre o arquivo lib.json de editores. Isso estará disponível quando você criar um editor na Etapa 1.

Configuração	Descrição
Autenticação desativada	Desativado
Conteúdo da biblioteca	<ul style="list-style-type: none"> <li>■ Baixar todas as bibliotecas imediatamente: se você não selecionar essa opção, o vCenter baixará TODOS os modelos de máquinas virtuais.</li> <li>■ Baixar o conteúdo da biblioteca somente quando necessário: apenas os metadados são baixados (não os discos). O vRealize Suite Lifecycle Manager instrui sobre demanda e conforme solicitado para baixar os discos associados</li> </ul>

## Restrições do desenvolvedor

As tags de conteúdo são úteis por várias razões: para localizar conteúdo na UI, ou seja, quando você encontra todo o conteúdo com a tag "BugFix-Task-1" ou pode ser usada para lógica de negócios personalizada durante o pipeline de liberação.

Um exemplo disso pode ser uma lógica de negócios personalizada implementada por um gerenciador de liberação: não implante Conteúdo no Endpoint B, a menos que o Conteúdo tenha sido implantado no Endpoint B, primeiro isso exige a implementação de um pipeline/fluxo de trabalho personalizado. Se esta regra deve ser ignorada, por exemplo, para os Gerenciadores de Liberação enviarem o Conteúdo diretamente para o Endpoint B, uma tag pode ser aplicada ao conteúdo. Essa tag só deve ser adicionada por um Gerenciador de Liberação e não um Desenvolvedor.

## Configurar Stub de Pipeline

Os stubs do pipeline podem ser executados de forma síncrona ou assíncrona. Ao executar um stub de forma assíncrona, os outros estágios de pipeline são executados sem aguardar a conclusão da lógica personalizada. Por exemplo, uma Pré-captura configurada para ser executada de forma assíncrona executa em paralelo com o estágio Capturar. No entanto, a execução de um estágio de Pós-captura é disparada somente depois que o estágio de Captura é executado, mas pode ser feito para ser executado em paralelo com o próximo estágio agendado, como o pré-teste.

Para associar uma tag a um fluxo de trabalho do vRealize Orchestrator, o nome da tag personalizada global de fluxo de trabalho e valor podem ser editados manualmente para incluir o vRSLCM\_CUSTOM ou o fluxo de trabalho "/Biblioteca/Marcação/Tag" também pode ser usado para a marcação. Não há suporte para a migração de stubs pré e pós.

### Pré-requisitos

Certifique-se de que todos os endpoints do Orchestrator cujos fluxos de trabalho devem ser usados nos stubs de pré ou pós sejam adicionados ao vRealize Suite Lifecycle Manager e que os fluxos de trabalho que devem ser usados nos stubs sejam marcados com a tag vRSLCM\_CUSTOM como palavra-chave.

### Procedimentos

1 Na guia **Configurações de Conteúdo**, clique no ícone de lápis **Editar**.

Será exibido **Configurar Stub de Pipeline**.

- 2 A condição **Nome e Executar Pipeline** é exibida por padrão.
- 3 Selecione Executar em segundo plano se o stub tiver que ser executado de forma assíncrona.
- 4 Selecione o **Endpoint do Orchestrator** do menu suspenso.
- 5 Selecione um **Fluxo de trabalho do Orchestrator** e clique em **Enviar**.  
Somente os fluxos de trabalho com tags como vRSLCM\_CUSTOM são mostrados na lista.
- 6 Selecione a **Configuração do Parâmetro de entrada** e clique em **Enviar**.

## Mapear a configuração do proxy

O vRealize Suite Lifecycle Manager 8.1 introduziu um proxy para endpoints de gerenciamento de controle de origem. Esse recurso permite que endpoints do SCM canalizem todas as chamadas REST por meio de um servidor proxy que pode ser definido na página de configurações do vRealize Suite Lifecycle Manager e mapeado para o gerenciamento de conteúdo. O proxy pode ser habilitado para um servidor SCM, o que habilita automaticamente o proxy para todos os endpoints que usam esse servidor SCM.

A guia Mapeamento do Proxy exibe o status do proxy e os detalhes da configuração, como o nome do host e a porta do servidor proxy.

---

**Observação** Você pode usar as configurações de proxy apenas para os endpoints de controle de origem.

---

Você pode habilitar o proxy para uma instância do SCM selecionando-o na lista de servidores e clicando em **Atualizar**. Quando o proxy estiver ativado para qualquer um dos servidores SCM, o administrador não poderá removê-lo da página de configurações do vRealize Suite Lifecycle Manager. Para remover o proxy, desabilite o mapeamento do proxy para todos os servidores SCM e, em seguida, prossiga com a remoção do proxy da página de configurações do vRealize Suite Lifecycle Manager. É possível desativar o mapeamento do proxy para um servidor SCM selecionando-o novamente e clicando em **Atualizar**. O administrador pode confirmar que o proxy não é usado por nenhum dos servidores observando o status do Proxy do vRealize Suite Lifecycle Manager usado pelo Gerenciamento de Conteúdo.

Se você perceber que o proxy não está habilitado, navegue até **Locker > Proxy** e marque a caixa de seleção **Configurar Proxy**. Para obter mais informações, consulte [Definir as configurações de proxy](#). Apenas um Gerente de Liberação e o administrador têm privilégios para acessar o mapeamento do Proxy no vRealize Suite Lifecycle Manager.

## Configurações de pipelines de conteúdo

A partir do vRealize Suite Lifecycle Manager 8.0, apenas Pipelines de Conteúdo e Pipelines de Captura são compatíveis. Na seção Pipelines de Conteúdo, na guia Pipelines, o status das últimas 24 execuções de pipeline pode ser visto no cartão Content\_Pipeline. Cada uma das execuções de pipeline de conteúdo, quando selecionada, mostra os Pipelines de captura associados, se houver, no cartão do pipeline de captura. As representações de execução, o ponto colorido no cartão do pipeline, podem ser selecionadas para exibir uma análise detalhada das vários estágios da

execução selecionada. A execução do pipeline de conteúdo pode conter no máximo nove estágios na ordem de execução. No entanto, a execução real possui os estágios que são relevantes para a execução.

## Stubs de Pipeline

Os stubs de pipeline exibem o status de cada ação sempre que um conteúdo é capturado. O pipeline de conteúdo tem os seguintes tipos de status sempre que um conteúdo é executado.

- Pré-captura
- Captura
- Pós-captura
- Pré-teste
- Testar
- Pós-teste
- Pré-implantação/Check-in
- Implantação/Check-in
- Pós-implantação/Check-in

Nos últimos três estágios, o termo Check-in é usado quando o conteúdo é liberado para um endpoint de controle de origem, como o Git ou o BitBucket. Nos demais casos, o termo Implantação é usado. Por padrão, os estágios “pré” ou “pós” estão desabilitados e devem ser configurados antes de serem usados em uma execução. A configuração e vários modos de execução para os estágios “pré” ou “pós”, também chamados de pré-stubs ou pós-stubs, são abordados na seção de stubs de pipeline de configuração. O pipeline de captura sempre terá um único estágio, que é Captura. Os detalhes correspondentes da pré ou pós-captura podem ser exibidos no pipeline de conteúdo associado, também conhecido como pipeline principal.

A guia Execuções lista todas as execuções de pipeline de conteúdo e captura. A lista mostra o estado, o tempo decorrido, a execução e a hora da solicitação de cada uma das execuções. Essa lista pode ser filtrada pelo tipo de pipeline e pelo status da execução.

Cada pipeline consiste em vários estágios, cada um podendo ter várias tarefas. Tarefas podem ser paralelas ou sequenciais, com base na lógica de negócios personalizada. Depois de selecionar uma ação que você deseja executar em um conteúdo, uma captura de conteúdo pode listar vários tipos de status relacionados a tal ação. Cada uma das configurações de conteúdo está relacionada à exibição exibida na página Pipeline de conteúdo.

### Condições de execução do pipeline:

- 1 **EXECUTE\_ON\_SUCCESS**: o stub será executado apenas se o estágio correspondente for executado com êxito. Por exemplo, Pós-captura, se configurada para EXECUTE\_ON\_SUCCESS, será executada apenas se o estágio de Captura for Executado com êxito.

- 2 **EXECUTE\_ON\_FAILURE:** o stub será executado apenas se a execução do estágio correspondente falhar. Por exemplo, Pós-captura, se configurada para EXECUTE\_ON\_FAILURE, será executada apenas se a execução do estágio de Captura falhar.
- 3 **EXECUTE\_ON\_SUCCESS\_AND\_FAILURE:** o stub é executado independentemente de a execução do estágio correspondente ser aprovada ou reprovada. Por exemplo, Pós-captura, se configurada para EXECUTE\_ON\_SUCCESS\_AND\_FAILURE, será executado em ambos os casos, independentemente de a execução do estágio de Captura for aprovada ou reprovada.

## Parâmetros de entrada

Os pré-stubs ou pós-stubs oferecem suporte à lista de parâmetros mencionada, cujos valores podem ser transmitidos ao respectivo fluxo de trabalho do vRealize Orchestrator como entradas. O valor dessas entradas depende do conteúdo (capturado/testado/implantado) da execução do pipeline para a qual as pré-rotinas ou pós-rotinas são executadas. Atualmente, todos os parâmetros são do tipo “String”. Portanto, os parâmetros de entrada configurados para o fluxo de trabalho correspondente no vRealize Orchestrator devem ser necessariamente do tipo “String”. Uma incompatibilidade entre o tipo de parâmetro resulta em uma falha de execução do pipeline. Para obter mais informações sobre configuração, consulte [Configurar Stub de Pipeline](#).

Pipeline-Pós-Implantação	Pipeline-Pré-Implantação	Pipeline-Pós-Teste	Pipeline-Pré-Teste	Pipeline-Pós-Captura	Pipeline-Pré-Captura
■ contentName	■ contentName	■ contentEndp oint	■ contentName	■ contentName	■ contentName
■ contentEndp oint	■ contentEndp oint	■ ContentId	■ contentEndp oint	■ contentEndp oint	■ contentEndp oint
■ ContentId	■ ContentId	■ contentName	■ ContentId	■ ContentId	■ ContentId
■ contentType	■ contentType	■ contentType	■ contentType	■ contentType	■ contentType
■ ContentVersi onID	■ ContentVersi onID	■ ContentVersi onID	■ ContentVersi onID	■ ContentVersi onID	■ ContentVersi onID
■ requestid	■ requestid	■ requestid	■ requestid	■ requestid	■ requestid
■ requestnumb er	■ requestnumb er	■ requestnumb er	■ requestnumb er	■ requestnumb er	■ requestnumb er
■ status	■ requestedby	■ requestedby	■ requestedby	■ requestedby	■ requestedby
■ requestedby	■ useridentity	■ useridentity	■ useridentity	■ useridentity	■ useridentity
■ useridentity				■ status	

## Pipelines de Conteúdo

A partir do vRealize Suite Lifecycle Manager 8.3, a página Pipelines de Conteúdo é reprojetada para exibir o status da captura de conteúdo, do teste e da liberação dos pipelines de conteúdo. É possível exibir todos os pipelines de conteúdo exibidos no estado concluído, em andamento ou com falha.

---

**Observação** Se você não conseguir exibir a lista completa de pipelines, atualize a página Pipelines de Conteúdo já que a solicitação em fila leva tempo para exibir os dados atuais.

---

Ao selecionar um pipeline de conteúdo na lista de Pipelines de Conteúdo, é possível exibir a divisão detalhada dos vários estágios da execução selecionada. Cada pipeline de conteúdo exibe a seguinte lista:

Opções de Pipelines de Conteúdo	Descrição
Mensagem de status	Exibe o resumo do status do pipeline de conteúdo selecionado.
Executado por	Exibe os detalhes do usuário ao realizar a execução.
Última atualização	Exibe a data do pipeline de conteúdo selecionado.
Comentários	Exibe comentários adicionais inseridos pelo usuário.
Tipos de conteúdo	Exibe o tipo de conteúdo selecionado para a execução do pipeline.
Content_pipeline	É possível selecionar as opções de captura, teste ou implementação para um pipeline de conteúdo. Com base na sua seleção, é possível ver a divisão detalhada da execução selecionada, como a Exibição de Todos os Estágios, a Exibição do Estágio <i>content_pipeline</i> e o estágio <i>content_pipeline</i> .

# Como atualizar produtos do vRealize Suite Lifecycle Manager e vRealize Suite

Este tópico descreve como atualizar seus produtos do vRealize Suite e vRealize Suite Lifecycle Manager quando você tem uma versão mais antiga.

Quando você deseja atualizar de uma versão mais antiga do vRealize Suite Lifecycle Manager, há três etapas.

- Upgrade do vRealize Suite Lifecycle Manager
- Upgrade do VMware Identity Manager
- Upgrade do vRealize Automation 8.x

Quando você quiser atualizar seus produtos individuais após a instalação do vRealize Suite Lifecycle Manager 8.x ou versões anteriores.

- Todos os produtos compatíveis com o vRealize Suite Lifecycle Manager.

Este capítulo inclui os seguintes tópicos:

- Fazer upgrade do vRealize Suite Lifecycle Manager 8.x
- Atualizar o VMware Identity Manager
- Fazer upgrade do vRealize Automation 8.x com o vRealize Suite Lifecycle Manager
- Atualizar um produto do vRealize Suite

## Fazer upgrade do vRealize Suite Lifecycle Manager 8.x

Você pode verificar e instalar atualizações no dispositivo do vRealize Suite Lifecycle Manager.

O upgrade é compatível com vRealize Suite Lifecycle Manager 8.0 e versões posteriores. Você também pode atualizar o vRealize Suite Lifecycle Manager usando um arquivo ISO para instalar o upgrade. Latências foram validadas com 350 ms e largura de banda de 1,5 MB para uma implantação e upgrade de um pacote pequeno do vRealize Suite.

### Pré-requisitos

- Verifique se os requisitos do sistema são atendidos. Consulte [Requisitos do sistema](#).
- Tire um snapshot do dispositivo virtual do vRealize Suite Lifecycle Manager. Se você encontrar problemas durante o upgrade, poderá reverter para esse snapshot.

- Verifique se nenhuma tarefa crítica está em andamento no momento em vRealize Suite Lifecycle Manager. O processo de atualização é interrompido, começam os serviços do vRealize Suite Lifecycle Manager e o dispositivo virtual do vRealize Suite Lifecycle Manager é reinicializado, o que pode corromper as tarefas que estão em andamento.
- Se você estiver atualizando o vRealize Suite Lifecycle Manager por meio de uma URL de repositório ou CD-ROM, certifique-se de baixar o binário de upgrade do vRealize Suite Lifecycle Manager do portal My VMware com antecedência. O nome do arquivo deve ser `-VMware-vLCM-Appliance-8.X.X.XX-XXXXXXXX-updaterepo.iso`.

---

**Observação** Você não pode usar o arquivo ISO do instalador fácil para um upgrade do vRealize Suite Lifecycle Manager. Você deve usar o arquivo ISO de upgrade do vRealize Suite Lifecycle Manager.

---

## Procedimentos

- 1 No painel Meus serviços, clique em **Operações de ciclo de vida** e clique em **Configurações**.
- 2 Clique em **Upgrade do Sistema**.  
O vRealize Suite Lifecycle Manager exibe o nome, o número da versão e o fornecedor do dispositivo do vRealize Suite Lifecycle Manager atual .
- 3 Selecione o tipo de repositório para atualizações do vRealize Suite Lifecycle Manager.

Opção	Descrição
<b>Verificar on-line</b>	Você pode verificar se os upgrades estão disponíveis on-line. Para usar essa opção, o dispositivo virtual do vRealize Suite Lifecycle Manager deve ter acesso a <a href="http://vapp-updates.vmware.com">vapp-updates.vmware.com</a> .
<b>URL</b>	Insira a URL do repositório para atualizações. Para usar essa opção, extraia o ISO que contém os arquivos de upgrade para um repositório privado. Não use um repositório privado que exija autenticação para acesso aos arquivos.
<b>CD-ROM</b>	Você pode atualizar o dispositivo do vRealize Suite Lifecycle Manager a partir de um arquivo ISO que o dispositivo lê na unidade de CD-ROM virtual.

- 4 Clique em **VERIFICAR UPGRADE**.

Depois de alguns minutos, o vRealize Suite Lifecycle Manager exibe uma mensagem indicando se há atualizações disponíveis.

- 5 Selecione o Tipo de repositório e clique em **UPGRADE**.
  - a Quando o vRealize Suite Lifecycle Manager estiver conectado à Internet, você poderá baixar o binário "Arquivo de Repositório de Atualização do vRealize Suite Lifecycle Manager" do My VMware Portal.
  - b O ISO baixado deve ser anexado à unidade de CD-ROM virtual da VM do vRealize Suite Lifecycle Manager. Para isso, você pode carregar o ISO em uma biblioteca de conteúdo do vCenter Server que hospeda o vRealize Suite Lifecycle Manager ou pode carregar em um datastore que a VM do vRealize Suite Lifecycle Manager pode acessar. Após carregar, você deve anexar o ISO ao dispositivo de CD-ROM da VM do vRealize Suite Lifecycle Manager editando a configuração de hardware da VM no inventário do vCenter. Na UI do vRealize Suite Lifecycle Manager, selecione a opção de upgrade baseada em CD-ROM e prossiga.
- 6 Marque a caixa de seleção nos snapshots do produto em Pré-requisito e clique em **Avançar**.
- 7 Clique em **EXECUTAR PRÉ-VERIFICAÇÃO**. Quando a validação de pré-verificação estiver concluída, você pode baixar o relatório para exibir as verificações e o status de validação.
- 8 Clique em **Upgrade** após uma validação de pré-verificação bem-sucedida.
- 9 Depois de alguns minutos, faça login na UI do vRealize Suite Lifecycle Manager e verifique se há uma mensagem de upgrade bem-sucedido em **Configurações > Upgrade do Sistema**.  
Ao concluir o upgrade, o vRealize Suite Lifecycle Manager exibe a mensagem de conclusão do upgrade. Se você não vir essa mensagem, aguarde alguns minutos e atualize a UI.

## Supporte para versões adicionais do produto

Esta seção abrange informações sobre como ativar versões de produtos aplicáveis para os produtos do vRealize Suite enquanto você estiver atualizando o dispositivo do LCM. É possível adicionar suporte a Políticas adicionais, aprimorar as novas versões do produto e adicionar patches ao vRealize Suite Lifecycle Manager como e quando aplicável.

Com o recurso de versão de verificação, você pode verificar as versões mais recentes disponíveis do produto, mesmo sem conectividade com a Web. A tabela com as versões do produto de cada vRealize Suite está pré-preenchida onde os dados são buscados na origem VMware.

Se a versão do produto atualizada selecionada não funcionar, navegue até o arquivo do produto baixado com uma extensão de arquivo .pspakk. Carregue o arquivo e valide o mesmo usando o Chrome ou o Internet Explorer.

## Atualizar o VMware Identity Manager

Você poderá atualizar versões anteriores do VMware Identity Manager para a versão mais recente se estiver em conformidade com o fator forma compatível com o vRealize Suite Lifecycle Manager. Caso contrário, o upgrade deve ser realizado fora do vRealize Suite Lifecycle Manager. Após um upgrade, você pode reimpor o VMware Identity Manager disparando a sincronização de inventário no vRealize Suite Lifecycle Manager. Para obter mais informações, consulte a

documentação *Instalação do vRealize Automation com o vRealize Suite Lifecycle Manager Easy Installer para o vRealize Automation e o VMware Identity Manager*.

---

### Observação

- Se a solicitação de instalação, upgrade ou dimensionamento horizontal do VMware Identity Manager estiver no estado EM ANDAMENTO ou COM FALHA no vRealize Suite Lifecycle Manager, certifique-se de não corrigir o cluster.
  - Se o VMware Identity Manager for agrupado em cluster através do vRealize Suite Lifecycle Manager, recomenda-se usar a opção Ligar e Desligar para um cenário que envolve a desativação do cluster, como reiniciar e desligar.
  - O VMware Identity Manager versão 3.3.4 é compatível retroativamente com conectores do Windows de versões anteriores.
  - Ao implantar o VMware Identity Manager com o vRealize Suite Lifecycle Manager, não altere o nome do host do VMware Identity Manager. Para obter mais informações, consulte a documentação [VMware Identity Manager](#).
- 

### Pré-requisitos

- Em um ambiente agrupado em cluster, certifique-se de que o Status de integridade do cluster Postgres está íntegro, selecionando a opção Disparar integridade do cluster para seu produto na página Ambientes. Depois que sua solicitação for concluída, você poderá exibir as notificações do seu produto e verificar se o seu status está íntegro. Se o seu status não estiver íntegro, você poderá usar a opção Ligar para corrigir o cluster, antes de um upgrade. Para a versão 8.4, o botão Correção está disponível no cartão do seu produto na página Ambientes.
- Verifique se você tirou um snapshot dos nós do VMware Identity Manager.
- Verifique se você mapeou os binários do produto. Para obter mais informações, consulte [Configurar binários de produto](#).
- Para um upgrade do VMware Identity Manager agrupado em cluster, certifique-se de desativar todos os nós em espera no平衡ador de carga, para que o tráfego não seja roteado aos nós em espera, e ative-os novamente após a conclusão do upgrade.

### Procedimentos

- 1 Na página Operações de Ciclo de Vida, clique em **Gerenciar Ambiente**.
- 2 Navegue até a instância do **Ambiente Global**.
- 3 Clique em **Exibir Detalhes > Upgrade..**

- 4 Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>URL do repositório</b>	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do ciclo de vida.
<b>Repositório do vRealize Suite Lifecycle</b>	Após selecionar essa opção, você poderá inserir o caminho de upgrade disponível depois de mapear os binários através do vRealize Suite Lifecycle Manager.
	<b>Observação</b> Para o VMware Identity Manager versão 3.3.4, a única opção disponível é o <b>Repositório do vRealize Suite Lifecycle</b> . As outras opções, <b>URL do repositório</b> e <b>Repositório do VMware</b> não estão disponíveis.
<b>Repositório VMware</b>	Selecione essa opção e a versão. O upgrade é realizado usando a fonte on-line.

- 5 Clique em e execute a pré-verificação.

- 6 Clique em **Enviar**.

## Migrar o conector do Windows

Na migração de conectores, o conector do Windows para VMware Identity Manager é instalado em uma máquina Windows, fornecendo o arquivo de configuração que é gerado por um conector do Linux externo ou incorporado. Isso é compatível com o vRealize Suite Lifecycle Manager 8.2 Patch 1 e versões posteriores.

Depois que o conector do Linux externo ou incorporado for migrado, os diretórios de Autenticação Integrada do Windows (IWA) e LDAP no conector do Linux serão migrados para o Windows. No VMware Identity Manager versão 3.3.2 e versões anteriores, os diretórios ativos tinham suporte em conectores do Linux externos e incorporados e em conectores externos do Windows. A partir do VMware Identity Manager versão 3.3.3, os diretórios ativos do IWA apenas têm suporte em conectores externos do Windows.

### Pré-requisitos

Siga os requisitos abaixo.

- A versão do JRE com suporte está entre a atualização 8 181 e a atualização 8 251.
- A versão do .NET Framework com suporte é 4.6.0.
- As versões com suporte do Windows Server são 2012 R2, 2016 e 2019.
- Um sistema Windows exclusivo é necessário para a migração e deve estar conectado a um servidor de domínio.

### Procedimentos

- 1 Na página Operações de Ciclo de Vida, clique em Gerenciar Ambiente.
- 2 Navegue até a instância do Ambiente Global.

- 3 Clique em **Exibir Detalhes > Fazer Upgrade**.
- 4 Marque a caixa de seleção e prossiga com o upgrade.
- 5 Na guia Selecionar Versão, selecione o **Tipo de Repositório**, a **Versão do Produto** e a **URL do Repositório**.
- 6 Para especificar a migração de conectores, insira os detalhes do Conector do Windows de Destino na seção Migrar Conector do Linux para Conexão do Windows.

**Observação** Os detalhes do Conector de Origem para o tipo de conector incorporado são preenchidos a partir do VMware Identity Manager. Você deve inserir somente as senhas SSH do Conector do Linux para o Tipo de Conector Externo.

- a Insira o **FQDN do Windows** de destino e o **Usuário do Domínio do Windows**.
  - b Selecione a **Senha do Domínio do Windows**.
  - c Selecione **Windows VM Center**.
- 7 Clique em e, em seguida, em **EXECUTAR PRÉ-VERIFICAÇÃO**.  
Se as validações não forem bem-sucedidas e você quiser fazer alterações antes de retomar a operação de upgrade do VMware Identity Manager, clique em **SALVAR E SAIR**.
  - 8 Se as validações forem bem-sucedidas, clique em **Avançar**.
  - 9 Na página Resumo do Upgrade, você pode verificar os detalhes e clicar em **Enviar**.

## Fazer upgrade do vRealize Automation 8.x com o vRealize Suite Lifecycle Manager

Você pode fazer upgrade do vRealize Automation no vRealize Suite Lifecycle Manager

### Pré-requisitos

- Certifique-se de ter feito upgrade das versões anteriores do vRealize Suite Lifecycle Manager para as mais recentes. Para obter mais informações sobre o upgrade do vRealize Suite Lifecycle Manager, consulte [Fazer upgrade do vRealize Suite Lifecycle Manager 8.x](#).
- Certifique-se de ter feito upgrade da versão anterior do VMware Identity Manager para 3.3.2 ou posterior. Para obter mais informações sobre o upgrade do VMware Identity Manager, consulte [Atualizar o VMware Identity Manager](#).
- Verifique se você já instalou o vRealize Automation 8.0, 8.0.1, 8.1, 8.2 ou 8.3.
- Execute o mapeamento binário do ISO upgrade do vRealize Automation a partir do compartilhamento Local, myvmware ou NFS. Para obter mais informações sobre o mapeamento binário, consulte [Configurar binários de produto](#).
- Aumente a CPU, a memória e o armazenamento de acordo com os requisitos do sistema do vRealize Automation 8.4. Para obter mais informações, consulte os Requisitos de Hardware da [Arquitetura de Referência do vRealize Automation 8.4](#).

## Procedimentos

1 Na página Operações de Ciclo de Vida, clique em **Gerenciamento de Ambientes**.

2 Navegue até uma instância do vRealize Automation.

3 Clique em **Exibir Detalhes** e clique em **Upgrade**.

Um menu pop-up aparece para alertar você para realizar uma sincronização de inventário.

4 Clique em **Disparar sincronização de inventário** do produto antes de atualizar.

**Observação** Às vezes, pode haver um desvio ou uma alteração no ambiente externo do Lifecycle Manager e, para que o Lifecycle Manager esteja ciente do estado atual do sistema, o inventário precisa estar atualizado.

a Se o inventário do produto já estiver sincronizado e atualizado, clique em **Continuar Upgrade**.

5 Depois que o inventário for sincronizado, selecione a versão do vRealize Automation para 8.4.

6 Para selecionar o **Tipo de Repositório** você pode selecionar o **Repositório LCM do vRealize Suite** somente se tiver mapeado o mapa binário ISO ou se for possível selecionar a **URL do Repositório** com uma URL de Repositório de upgrade privada.

7 Se você selecionou a URL do Repositório, insira a URL não autenticada e, em seguida, clique em **Avançar**.

8 Clique em **Pré-Verificação**.

A pré-verificação valida os seguintes critérios:

- Se as versões do vRealize Automation de origem forem 8.0.0 ou 8.0.1, certifique-se de seguir as etapas fornecidas no artigo da KB [78325](#) antes de atualizar para restaurar as contas raiz expiradas.
- SSH ativado: verifica se o SSH para o usuário raiz está ativado.
- Verificação da versão: verifica se a versão de destino selecionada para o upgrade é compatível com a versão atual do vRealize Automation.
- Espaço em disco na partição de log de serviços, dados e raiz: verifica se a quantidade necessária de espaço livre em disco está disponível na partição de log de serviços, dados e raiz.
- Verificação de CPU e memória: verifica se a quantidade necessária é de 12 CPU e 42 GB de recursos de memória disponíveis em cada nó do vRealize Automation antes do upgrade.
- Verificação de existência da propriedade vCenter: verifica se os detalhes do vCenter estão presentes como parte de cada nó no inventário do Lifecycle Manager. Como um snapshot é tirado durante o processo de upgrade, é importante ter os detalhes corretos do vCenter no inventário do Lifecycle Manager.

- Verificação de recuperação de ID de referência de objeto gerenciado por VMs do vRealize Automation: verifica se o ID de referência do objeto gerenciado da VM pode ser recuperado dos detalhes disponíveis no inventário do Lifecycle Manager. Isso é necessário à medida que você realiza operações relacionadas ao snapshot nas VMs, encontrando a VM que usa o mesmo.

**9 Clique em Avançar e em Enviar.**

Você pode navegar até a página Detalhes da Solicitação para exibir o progresso do status de upgrade. Você pode ativar o recurso vários tenants para o vRealize Automation, consulte [Gerenciamento de tenants no vRealize Suite Lifecycle Manager](#).

## Funcionalidade de upgrade do vRealize Automation

Há três estágios no processo de upgrade do vRealize Automation no vRealize Suite Lifecycle Manager.

Estágios de upgrade	Descrição
Preparação para upgrade	A fase de preparação verifica se o sistema está em estado de integridade e encerra os serviços para garantir que todos os dados persistam.
Snapshot de todas as VMs para uma recuperação automática	Snapshots são tirados para recuperação mais rápida de falhas. O vRealize Suite Lifecycle Manager, em seguida, desliga as VMs, tira uma snapshot, liga e continua para a próxima fase.
Execução de upgrade.	Execute a atualização.

Em determinados cenários inesperados ou de falha, o fluxo de trabalho de upgrade do vRealize Suite Lifecycle Manager fornece pontos de decisão do usuário para concluir o upgrade com êxito ou reverter para o estágio anterior ao upgrade.

- O processo de upgrade começa com uma tarefa de verificação de status que verifica o estado atual de VA. Se o sistema já tiver uma solicitação de upgrade devido a uma tentativa de upgrade anterior, o vRealize Suite Lifecycle Manager fornecerá uma opção para limpar os estados mais antigos e iniciar um novo upgrade. É possível ver que há falha na tarefa de status com um parâmetro de repetição semelhante a "cancelAndStartAfresh". Definir este parâmetro de repetição para verdadeiro limpa os estados mais antigos e dispara novamente o upgrade.
- Se ocorrerem falhas inesperadas durante a fase de preparação, você poderá cancelar todo o processo de upgrade e iniciá-lo novamente. Se uma falha não puder ser corrigida ou se a falha inesperada for corrigida manualmente, você poderá prosseguir para a próxima fase no fluxo de trabalho de upgrade. O status seleciona “concluído” após a falha na preparação lhe fornecer dois parâmetros de nova tentativa que ajudam a decidir qual opção selecionar. Se você definir “cancelAndStartAfresh” como “true”, o processo de upgrade será cancelado e retornará o sistema ao estado anterior ao upgrade. Se você definir “proceedNext” como “true”, o fluxo de trabalho de upgrade do vRealize Suite Lifecycle Manager prosseguirá para o próximo estado com uma suposição de que você corrigiu o problema de preparação externamente.

- O fluxo de trabalho de upgrade consiste em operações de nível de VM, como reverter ou excluir um snapshot e Encerrar VM, Ligar e assim por diante. Se houve uma falha, essas operações incluem a opção **Ignorar** que pode ser usada se a opção REPETIR no vRealize Suite Lifecycle Manager não ajudar e quando você executa manualmente a mesma operação diretamente no vCenter Server.
- A fase final do upgrade pode ser bem-sucedida ou obter êxito com avisos ou um estado fatal.
  - O êxito com avisos indica que o upgrade foi concluído com êxito, mas um erro secundário foi detectado. Você pode verificar os erros e retificá-los. Você pode definir o parâmetro de repetição “succeedUpgradeRequest” como “true”, que será bem-sucedido e concluirá o fluxo de trabalho de upgrade do vRealize Suite Lifecycle Manager.
  - Se houver um erro fatal, você poderá decidir se deseja reverter o snapshot e repetir o upgrade ou cancelar todo o processo de upgrade. Você pode reverter e excluir o snapshot, cancelar a solicitação de upgrade atual e mover o sistema para um estado anterior ao início do upgrade.
    - Quanto a um erro fatal, é possível ver a tarefa de status após a falha de upgrade com parâmetros de repetição semelhantes a "revertSnapshotNRetryUpgrade" e "cancelUpgradeNRevertBack". Se você definir "revertSnapshotNRetryUpgrade" como "true", ele poderá reverter o snapshot e repetir o upgrade.

- Se você definir “cancelUpgradeNRevertBack” como “true”, é possível cancelar o processo de upgrade, o que pode reverter e excluir o snapshot, cancelar a solicitação de upgrade atual e mover o sistema para um estado anterior ao início do upgrade.

### **Observação**

- O fluxo de trabalho de upgrade do vRealize Suite Lifecycle Manager não é compatível com a remoção dos snapshots se houve um upgrade bem-sucedido. Mantenha os snapshots ou remova-os manualmente do vCenter Server, se necessário.
- Se você Cancelar o processo de upgrade após uma preparação posterior com falha ou fase de upgrade, o fluxo de trabalho do vRealize Suite Lifecycle Manager termina em um estado cancelado ao fazer a pós-limpeza da solicitação de upgrade no vRealize Automation. Isso indica que o fluxo de trabalho de upgrade do vRealize Suite Lifecycle Manager foi interrompido. Em tais situações, dispare novamente um upgrade das ações do produto na página **Ambiente do gerente**.
- Você pode ativar o recurso vários tenants para o vRealize Automation, consulte [Gerenciamento de tenants no vRealize Suite Lifecycle Manager](#).
- Se a atualização do vRealize Automation falhar, você deverá cancelar o upgrade ou reverter um snapshot e, em seguida, repetir o upgrade por meio do vRealize Suite Lifecycle Manager. Se você reverter o snapshot manualmente em um vCenter Server, o vRealize Automation entrará em um estado inconsistente.
- Quanto ao vRealize Automation, se você cancelar o upgrade ou reverter um snapshot e, em seguida, repetir o upgrade, certifique-se de criar um pacote de suporte que contenha os arquivos de log para análise e referência futuras.

## Atualizar um produto do vRealize Suite

Você pode usar o vRealize Suite Lifecycle Manager para atualizar as instalações de produtos do vRealize Suite.

Quando uma solicitação de implantação é salva no vRealize Suite Lifecycle Manager 1.1, e a mesma solicitação é retomada após a atualização do vRealize Suite Lifecycle Manager para 1.2, os itens da página de detalhes dos produtos do vRealize Automation 7.3 não são carregados. Para obter mais informações, consulte o artigo [KB 56369](#). Quando um upgrade do vRealize Suite Lifecycle Manager é disparado, a tela permanece no modo de Manutenção e a página **Início** nunca aparece. Após um upgrade, pode haver alguns erros no conteúdo do Marketplace. O conteúdo pode conter poucas solicitações que impeçam o serviço de iniciar. A UI do vRealize Suite Lifecycle Manager exibe uma mensagem no modo de manutenção e a página Início não é exibida. Nesse cenário, reinicie o servidor xenon. Se o problema ainda persistir, exclua a solicitação de erro e reinicie o xenon. Para fazer upgrade para o vRealize Automation 8.x, consulte [Fazer upgrade do vRealize Automation 8.x com o vRealize Suite Lifecycle Manager](#).

## Pré-requisitos

Verifique se o produto do vRealize Suite a ser atualizado faz parte de um ambiente de nuvem privada do vRealize Suite Lifecycle Manager e tire um snapshot do produto para o qual você pode reverter, caso algo dê errado com o upgrade . Consulte [Criação e configuração de um snapshot do produto](#).

Se você estiver atualizando o vRealize Automation 7.x, certifique-se de que os seguintes pré-requisitos adicionais sejam atendidos:

- O agente de gerenciamento do vRealize Automation e todos os nós do IaaS Windows estão em execução.
- O segundo membro no balanceador de carga do vRealize Automation está desativado.

Se você estiver atualizando o vRealize Automation 8.x, certifique-se de que os seguintes pré-requisitos adicionais sejam atendidos:

- O vRealize Suite Lifecycle Manager deve ser atualizado para a versão mais recente.
- O VMware Identity Manager deve ser atualizado para a versão 3.3.2 ou posterior.
- Os serviços do vRealize Automation devem estar em execução.

## Procedimentos

- 1 Clique em **Gerenciar Ambientes**.
- 2 Clique em **VIEW DETAILS** no ambiente que contém o produto a ser atualizado.
- 3 Clique no ícone de reticências (...) ao lado do nome do produto a ser atualizado e selecione **Upgrade** no menu suspenso.
- 4 Escolha uma versão do produto para a qual deseja atualizar.
- 5 Se estiver atualizando o vRealize Automation ou o vRealize Business for Cloud, escolha se vai fazer upgrade do repositório **Padrão**, do repositório do **vRealize Suite Lifecycle Manager** ou de uma URL do Repositório **inserida manualmente**.
- 6 Se estiver atualizando o vRealize Log Insight ou o vRealize Operations Manager, escolha se vai fazer upgrade do **Repositório do vRealize Suite Lifecycle Manager** ou de uma **URL de repositório** digitada manualmente e selecione a **Versão do produto**.
- 7 Clique em **Avançar**.

- 8 Em Snapshot há duas opções. Você pode selecionar **Obter snapshot do produto** e **Reter o snapshot obtido do produto**. Se **Obter snapshot do produto** for definido como verdade, o snapshot será obtido antes de um upgrade e poderá ser revertido ao estado inicial durante uma falha de upgrade, o snapshot será obtido com o prefixo LCM\_AUTOGENERATED. Se **Reter o snapshot obtido do produto** for definido como verdade, ele será retido e poderá ser revertido para a versão anterior após um upgrade bem-sucedido.

---

#### Observação

- A opção Snapshot não é compatível com o vRealize Automation versão 7.x.
  - Ao selecionar um snapshot, as VMs do produto são desligadas antes da obtenção do snapshot o que resulta em inatividade por um tempo especificado.
  - Se o upgrade falhar, agora você poderá reverter através da opção Revert snapshot. Isso só é aplicável a uma solicitação de upgrade ou de dimensionamento horizontal com falha. Se optar por obter um snapshot como uma opção e o upgrade falhar, a ação Revert snapshot dispara uma nova solicitação para reverter para o estado inicial. Selecione as reticências (...) na página Solicitações para a ação Revert snapshot.
- 9 Clique em **EXECUTAR PRÉ-VERIFICAÇÃO**. Após a pré-verificação bem-sucedida, você pode visualizar o Resumo do upgrade e, em seguida, clique em **Atualizações**.

Se você tiver atualizado um produto do vRealize Suite fora do vRealize Suite Lifecycle Manager, o vRealize Suite Lifecycle Manager não refletirá a versão mais recente do produto ou os dados mais recentes do produto atualizado. Em tais instâncias, você precisa excluir o produto do vRealize Suite (o produto que já está atualizado para a versão mais recente fora do vRealize Suite Lifecycle Manager) somente do vRealize Suite Lifecycle Manager e, em seguida, importar novamente o mesmo produto para que o vRealize Suite Lifecycle Manager obtenha o estado mais recente de determinado produto juntamente com sua versão mais recente.

#### Próximo passo

Você pode exibir o progresso do upgrade na guia **Solicitações**.

### Atualizar produtos já existentes usando o verificador de pré-atualização

Você pode acionar uma verificação de pré-validação na UI do produto antes de atualizar um produto existente dentro de um ambiente. Você pode avaliar os upgrades do produto e permitir a operação de upgrade mais tarde. Você também pode validar a matriz de compatibilidade do produto que deve ser validada.

Para obter mais informações sobre o upgrade de produtos do vRealize Suite, consulte [Atualizar um produto do vRealize Suite](#).

#### Pré-requisitos

Verifique se você já tem um produto do vRealize Suite no seu ambiente.

## Procedimentos

- Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Suite existente e selecione um upgrade.

As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com produtos que precisam ser atualizados.

- Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>Repositório VMware</b>	Quando você seleciona essa opção, as versões mais recentes dos produtos vRealize Suite são exibidas na tabela Matriz de Compatibilidade. Você só pode ver essa opção no vRealize Automation e vRealize Business for Cloud. Embora as informações da matriz de compatibilidade sejam preenchidas no nível do produto Suite, pode haver uma possibilidade de que as versões mais recentes possam não estar disponíveis no vRealize Suite Lifecycle Manager. Porém, com a opção <b>Verificar versão disponível</b> , é possível obter apenas o número da versão mais recente com o número da compilação associado.
<b>URL do repositório</b>	Ao selecionar essa opção, você poderá adicionar manualmente o local do arquivo de upgrade local no dispositivo virtual do vRealize Suite Lifecycle Manager.
<b>Repositório do vRealize Suite Lifecycle</b>	Ao selecionar essa opção, você poderá escolher o caminho de upgrade disponível após mapear os binários por meio do vRealize Suite Lifecycle Manager.

**Observação** Apenas o upgrade do vRealize Operations Manager consiste no recurso **Executar Avaliação**. A avaliação de execução verifica a preparação de upgrade do vRealize Operations Manager. Não é obrigatório que a avaliação de execução seja aprovada, você ainda pode continuar com o upgrade. As informações da matriz de compatibilidade são preenchidas de acordo com a versão selecionada do vRealize Operations Manager no menu suspenso Versão do produto .

- Clique em **Avançar** e em **Executar Pré-Verificação**.

Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação.

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, é possível selecionar a opção**Executar novamente a pré-verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

- Clique em **Avançar** e em **Enviar**.
- Se ocorrer uma falha no upgrade de componentes IaaS do vRealize Automation
  - Reverta todos os componentes de Infraestrutura de volta para o snapshot "snapshot de VA pós-atualização".
  - Reverta o banco de dados MS SQL de volta para o estado pré-atualizado.

- c Clique em **Repetir** a partir do vRealize Suite Lifecycle Manager e defina **Atualizar IaaS usando Cli** como **True**.
- d Clique em **Enviar**.

## Atualizar vRealize Operations Manager

Você pode disparar uma verificação de pré-validação na UI antes de atualizar o vRealize Operations Manager dentro de um ambiente. Você pode avaliar os upgrades do vRealize Operations Manager e permitir a operação de upgrade mais tarde. Você também pode validar a matriz de compatibilidade do produto que deve ser validada.

### Pré-requisitos

Verifique se há uma versão mais antiga ou existente da instância do vRealize Operations Manager nos Ambientes de Gerenciamento.

### Procedimentos

- 1 Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Operations Manager existente e selecione um **Upgrade**.

As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com o produto que deve ser atualizado.

- 2 Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>URL do repositório</b>	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local em um dispositivo virtual do Ciclo de vida.
<b>Repositório do vRealize Suite Lifecycle</b>	Ao selecionar essa opção, você poderá inserir o caminho de upgrade disponível após mapear os binários por meio do LCM.

- 3 Clique em **Avançar**.

- 4 Para executar o formato de arquivo e o **suporte da versão do LCM**, clique em **EXECUTAR PRÉ-VERIFICAÇÃO**.

Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação.

**Observação** Ao atualizar a instância do vRealize Operations Manager, você tem duas opções.

- Executar Pré-verificação: você deve executar para atualizar o vRealize Operations Manager.
- Executar a ferramenta de avaliação: você pode usar essa opção para executar uma ferramenta APUAT do vRealize Operations Manager .

O binário da ferramenta APUAT do vRealize Operations Manager é empacotado com uma compilação do vRealize Suite Lifecycle Manager e, quando o vRealize Suite Lifecycle Manager é implantado, ele está presente na localização VA do vRealize Suite Lifecycle Manager: /data/lcmcontents/, por padrão.

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, poderá selecionar a opção **Executar Novamente a Pré-Verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

Se a Senha do administrador do SO do vRealize Operations Manager expirar, ocorrerá falha na pré-verificação de upgrade do vRealize Operations Manager ao fazer check-in, mesmo se a conta de administrador estiver bloqueada ou não. Você pode alterar a senha do administrador do vRealize Operations Manager na UI vRealize Suite Lifecycle Manager e, em seguida, clicar em Pré-verificar no vRealize Operations Manager novamente. Você também pode alterar a senha de administrador do vRealize Operations Manager fora do vRealize Suite Lifecycle Manager diretamente no vRealize Operations Manager e, em seguida, executar uma sincronização de inventário para a instância do vRealize Operations Manager selecionada na UI do vRealize Suite Lifecycle Manager. Clique em **Executar Pré-Verificação de Upgrade** no vRealize Operations Manager novamente.

## Atualizar o vRealize Automation 7.x

Você pode disparar uma verificação de pré-validação na UI antes de atualizar o vRealize Automation dentro de um ambiente. Você pode avaliar os upgrades do vRealize Automation e permitir a operação de upgrade mais tarde. Você também pode validar a matriz de compatibilidade do produto que deve ser validada.

### Pré-requisitos

Verifique se há uma versão mais antiga ou já existente da instância do vRealize Automation nos Ambientes de Gerenciamento.

## Procedimentos

- 1 Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Automation existente e selecione um **Upgrade**.  
As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com produtos que precisam ser atualizados.
- 2 Marque a caixa de seleção **Snapshot de AAS após Upgrade de VA**.  
Se ocorrer falha de um componente IaaS após vRealize Automation, você poderá reverter para o snapshot de VA pós-atualização.
- 3 Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
URL do repositório	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do Lifecycle.
Repositório VMware	Quando você seleciona essa opção, as versões mais recentes dos produtos vRealize Suite são exibidas na tabela Matriz de Compatibilidade. Você só pode ver essa opção no vRealize Automation. Embora as informações da matriz de compatibilidade sejam preenchidas no nível do produto Suite, pode haver uma possibilidade de que as versões mais recentes possam não estar disponíveis no vRealize Suite Lifecycle Manager. Porém, com a opção <b>Verificar versão disponível</b> , é possível obter apenas o número da versão mais recente com o número da compilação associado.
Repositório do vRealize Suite Lifecycle	Ao selecionar essa opção, você poderá selecionar o caminho de upgrade disponível após mapear os binários por meio do LCM.

- 4 Clique em **EXECUTAR PRÉ-VERIFICAÇÃO** para executar.  
Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação.

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, é possível selecionar a opção**Executar novamente a pré-verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

- 5 Clique **Avançar** e leia o resumo antes de clicar em **Enviar**.

## Atualizar vRealize Network Insight

Você pode disparar uma verificação de pré-validação na UI antes de atualizar o vRealize Network Insight dentro de um ambiente. Você pode avaliar os upgrades do vRealize Network Insight e permitir a operação de upgrade mais tarde. Você também pode validar a matriz de compatibilidade do produto que deve ser validada.

## Procedimentos

- Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Network Insight existente e selecione um **Upgrade**.

As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com produtos que precisam ser atualizados.

- Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>URL do repositório</b>	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do Lifecycle.
<b>Repositório do vRealize Suite Lifecycle</b>	Ao selecionar essa opção, você poderá inserir o caminho de upgrade disponível após mapear os binários por meio do LCM.

- Clique em **Avançar**.

- Clique em **EXECUTAR PRÉ-VERIFICAÇÃO** para executar o formato do arquivo e o **suporte da versão do LCM**.

Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação. `

---

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, é possível selecionar a opção**Executar novamente a pré-verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

---

## Atualizar vRealize Log Insight

Você pode disparar uma verificação de pré-validação na UI antes de atualizar o vRealize Log Insight dentro de um ambiente. Você pode avaliar os upgrades do vRealize Log Insight e permitir a operação de upgrade mais tarde. Você também pode validar a matriz de compatibilidade do produto que deve ser validada.

### Pré-requisitos

Verifique se há uma versão mais antiga ou já existente da instância do vRealize Log Insight nos Ambientes de Gerenciamento.

### Procedimentos

- Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Log Insight já existente e selecione um **Upgrade**.

As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com produtos que precisam ser atualizados.

- 2** Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>URL do repositório</b>	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do Lifecycle.
<b>Repositório do vRealize Suite Lifecycle</b>	Ao selecionar essa opção, você poderá escolher o caminho de upgrade disponível após mapear os binários por meio do LCM.

- 3** Clique em **Avançar**.

- 4** Clique em **EXECUTAR PRÉ-VERIFICAÇÃO**.

Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação.

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, é possível selecionar a opção**Executar novamente a pré-verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

## Atualizar vRealize Business for Cloud

Você pode disparar uma verificação de pré-validação na UI antes de atualizar o vRealize Business for Cloud dentro de um ambiente.

### Procedimentos

- 1** Clique com o botão direito do mouse nas reticências verticais de um produto do vRealize Business for Cloud existente e selecione um **Upgrade**.

As informações da matriz de compatibilidade são carregadas com versões novas, compatíveis e incompatíveis com o produto que deve ser atualizado.

- 2** Na seção de detalhes do produto , você pode selecionar o seguinte tipo de repositório.

Opção	Descrição
<b>URL do repositório</b>	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do Lifecycle.
<b>Repositório do vRealize Suite Lifecycle</b>	Após selecionar essa opção, você poderá inserir o caminho de upgrade disponível após mapear os binários através do Lifecycle Manager.

- 3** Clique em **Avançar**.

- Clique em **EXECUTAR PRÉ-VERIFICAÇÃO** para executar o formato do arquivo e o **Suporte da versão do LCM**.

Depois que a validação de pré-verificação for concluída, você poderá baixar o relatório para exibir as verificações e o status de validação.

---

**Observação** Se você quiser executar a pré-verificação novamente depois de avaliar as discrepâncias, é possível selecionar a opção**Executar novamente a pré-verificação**. A pré-verificação também pode ser realizada usando o botão de alternância**Enviar**.

---

## Atualizar a configuração do vRealize Automation Salt Stack

Você pode disparar uma verificação de pré-validação da UI do produto antes de atualizar a configuração do vRealize Automation Salt Stack em um ambiente. Você pode avaliar os upgrades de configuração do vRealize Automation Salt Stack e permitir a operação de upgrade mais tarde.

### Pré-requisitos

---

**Observação** Se você tiver vários tenants, só poderá atualizar um tenant por vez.

---

Verifique se há uma versão mais antiga ou existente da instância de configuração do vRealize Automation Salt Stack nos ambientes de gerenciamento.

### Procedimentos

- Na página Ambientes, selecione Configuração do vRealize Automation Salt Stack e clique em **Upgrade**.
- Clique em **Continuar** para atualizar.
- Na seção Selecionar versão, é possível selecionar o seguinte tipo de repositório.

Opção	Descrição
Repositório LCM vRealize Suite	Ao selecionar essa opção, você poderá selecionar o caminho de upgrade disponível depois de mapear os binários através do vRealize Suite Lifecycle Manager.
URL do repositório	Quando você seleciona essa opção, é possível adicionar manualmente a localização do arquivo de upgrade local no dispositivo virtual do Lifecycle.

- Clique em **Avançar**.
- Na página Pré-verificação, você pode exibir o status de validação. Você pode clicar no botão **EXECUTAR PRÉ-VERIFICAÇÃO NOVAMENTE** para avaliar as discrepâncias.
- Clique em **Avançar** para exibir o resumo do upgrade.
- Clique em **Enviar**.

# Executar um plano de recuperação de desastres para o vRealize Suite Lifecycle Manager

Você pode realizar a recuperação de desastres executando um plano de recuperação no vRealize Suite Lifecycle Manager com re-IP usando o Site Recovery Manager.

## Procedimentos

- 1 Crie um plano de recuperação para a VM do vRealize Suite Lifecycle Manager e configure as etapas de recuperação desativando o re-IP manualmente e, em seguida, desabilitando a inicialização pós-recuperação.
- 2 Edite a configuração de hardware da VM do vRealize Suite Lifecycle Manager recuperada no inventário do vCenter e, em seguida, atribua a rede correta.
- 3 Ligue a VM do vRealize Suite Lifecycle Manager.
- 4 Acesse o console da VM do vRealize Suite Lifecycle Manager no inventário do vCenter como usuário `root`.
- 5 Execute os comandos a seguir no console da VM.
  - a `/opt/vmware/share/vami/vami_set_network <Network-Interface-Name> STATICV4+NONEV6 <New-IPv4> <SUBNETMASK> <DEFAULT-GATEWAY>`
  - b `/opt/vmware/share/vami/vami_set_dns <New-DNS-IP-OR-FQDN>`
  - c `/opt/vmware/share/vami/vami_set_hostname <New-Hostname>`
  - d Reinicialize.
- 6 Acesse a UI do vRealize Suite Lifecycle Manager com o novo IPv4 ou o novo FQDN e, em seguida, faça login. No Locker, selecione Certificados Iniciais e, em seguida, gere um novo certificado que inclua o FQDN do vRealize Suite Lifecycle Manager atualizado.
- 7 Na página Início de Operações de Ciclo de Vida, selecione Configurações e, em seguida, selecione Alterar Certificado para atualizar o certificado do vRealize Suite Lifecycle Manager gerado na etapa anterior.

- 8 Na página Início de Operações de Ciclo de Vida, selecione Configurações e, em seguida, selecione Provedor de Autenticação para executar **SINCRONIZAR** e **REPETIR REGISTRO**. Isso atualizará o novo FQDN do vRealize Suite Lifecycle Manager no catálogo do VMware Identity Manager.

---

**Observação** Execute esta etapa apenas se o VMware Identity Manager estiver ao alcance da rede da VM do vRealize Suite Lifecycle Manager recuperada.

---

- 9 Faça uma sincronização de inventário com os produtos gerenciados para garantir que o vRealize Suite Lifecycle Manager esteja funcional com as novas configurações de rede.

# Gerenciamento de licenças do vRealize Cloud no vRealize Suite Lifecycle Manager

Agora você pode centralizar o gerenciamento de suas licenças de assinatura do vRealize Cloud, juntamente com outras licenças no local pelo Locker do vRealize Suite Lifecycle Manager.

Para saber mais sobre o vRealize Cloud, você pode consultar [Criando ambientes no vRealize Cloud](#).

Este capítulo inclui os seguintes tópicos:

- Gerenciar licenças do vRealize Cloud no Locker
- Ativação de licenças de assinatura do vRealize Cloud Universal
- Operações do Dia 2 para o vRealize Cloud Universal
- Operações de Dia 2 para licenças do vRealize Cloud

## Gerenciar licenças do vRealize Cloud no Locker

O aplicativo Locker ajuda você a gerenciar licenças do vRealize Cloud para sua assinatura do vRealize Cloud e a coletar o uso diário de dados para os produtos e serviços de nuvem associados.

Ao comprar uma Assinatura do vRealize Cloud, você recebe acesso ao vRealize Cloud Subscription Manager, um novo serviço utilitário gratuito. Com o vRealize Cloud Subscription Manager, você pode adicionar endpoints e monitorar o uso de dados para seus serviços de Assinatura do vRealize Cloud. Você deve criar licenças do vRealize Cloud no nível do Locker no vRealize Suite Lifecycle Manager e, em seguida, conectar essas licenças ao vRealize Cloud Subscription Manager para monitorar o uso de dados na nuvem. Para obter mais informações sobre o vRealize Cloud Subscription Manager, consulte a [documentação do vRealize Cloud Subscription Manager](#).

### Pré-requisitos

Verifique se você se registrou no My VMware para acessar licenças.

### Procedimentos

- 1 Se você não tiver uma conta My VMware, navegue até o painel Operações de Ciclo de Vida e clique em **Configurações**.

- 2 Clique em **My VMware** e adicione uma conta do vRealize Cloud.
- 3 Depois que suas contas My VMware forem configuradas, as chaves de licença correspondentes serão sincronizadas.
- 4 No painel Operações de Ciclo de Vida, clique em **Locker**.
- 5 Clique no ícone **Licença**. As licenças do vRealize Cloud são criadas na conta My VMware e exibidas na tabela Licenças.
- 6 Para sincronizar novamente as licenças da conta My VMware, clique em **Recuperar Licenças**.
- 7 Se você já tiver produtos implantados, importe-os no vRealize Suite Lifecycle Manager e aplique as licenças do vRealize Cloud Universal a esses produtos capturados no Locker. Se não houver produtos existentes, você poderá usar as licenças do vRealize Cloud Universal presentes no Locker do vRealize Suite Lifecycle Manager para a implantação de produtos. Para obter mais informações, consulte o tópico *Configurar licenças no Locker*.
- 8 Se você já tiver baixado sua licença, poderá adicionar os detalhes dessa licença no Locker.
- 9 Para conectar uma licença à Assinatura do vRealize Cloud, selecione uma licença exibida na tabela Licença e clique com o botão direito do mouse nas reticências verticais.
  - a Clique em **Conectar Licença**.
  - b Em Token de API, gere um token de API da sua conta de usuário para a Assinatura do vRealize Cloud e clique em **Avançar**.
  - c Em Associar Chave de Licença, o vRealize Cloud Subscription Manager encontra uma correspondência correta para o token de API fornecido e lista os detalhes da organização.
  - d Em Frequência de Relatórios, você receberá uma confirmação de que está conectado ao vRealize Cloud Subscription Manager, e seu uso de dados será relatado ao vRealize Cloud Subscription Manager duas vezes por dia.
  - e Clique em **Concluir**.
- 10 Para desconectar uma licença no vRealize Suite Lifecycle Manager, clique com o botão direito do mouse nas reticências verticais e depois clique em **Desconectar Licença**.
- 11 Para acionar o uso da licença para um produto, selecione uma licença na tabela Licença e clique com o botão direito do mouse nas reticências verticais.
  - a Clique em **Sincronizar Uso**.
  - b Você pode baixar o relatório de sincronização de uso para exibir o uso de dados dos produtos.
- 12 Para exibir o relatório de consumo de dados, selecione uma licença e clique com o botão direito do mouse nas reticências verticais.
  - a Clique em **Gerar Relatório**.
  - b Para exibir uma representação gráfica do relatório, clique em **GERAR** na página Gerar Relatório.

- c Para baixar o relatório por um período máximo de 120 dias, clique em **BAIXAR**.

## Fazendo download do relatório de uso para licenças do vRealize Cloud

A partir do vRealize Suite Lifecycle Manager 8.4.1, duas novas opções estão disponíveis para as licenças do vRealize Cloud exibidas como o tipo de licença do vRealizeFlex na tabela de Licenças. Ao clicar com o botão direito do mouse nas reticências verticais, você pode visualizar o Relatório de uso e as opções de Chave de uso de atualização.

O Relatório de uso permite fazer o download e visualizar os relatórios de licença.

- **Fazer download de relatório:** a opção Geral permite baixar relatórios para fins de visualização, análise, armazenamento, documentação ou auditoria.

A opção vRealize Cloud Subscription Manager Billing permite fazer o download de um arquivo de dados de uso criptografado, que você carrega no vRealize Cloud Subscription Manager, e isso gera uma chave de uso. Para obter mais informações, consulte a documentação do [VMware vRealize Cloud Subscription Manager](#). Você pode usar essa chave de uso no vRealize Suite Lifecycle Manager para atualizar a opção de chave de uso do vRealize Assinatura Manager. Quando a chave de uso for atualizada, você poderá gerar o relatório de uso da licença para a última data carregada até a data atual.

- **Exibir uso:** essa guia exibe um gráfico com os detalhes de uso de uma determinada licença.

## Ativação de licenças de assinatura do vRealize Cloud Universal

Na página vRealize Cloud Universal, você deve ativar suas licenças de assinatura do vRealize Cloud Universal. Depois de ativar suas licenças, você pode executar as ações disponibilizadas pela licença.

### Procedimentos

- 1 Para ativar uma licença de assinatura, navegue até o dashboard **vRealize Cloud** e clique em **Cloud Universal**.
- 2 Clique em **Ativar licença de assinatura**.
- 3 Marque a caixa de seleção para confirmar se os vRealize Suite estão nos patches necessários para prosseguir.
- 4 Selecione o sinal de mais (+) para adicionar os detalhes da chave de licença e clique em **Validar**. Após a validação da chave de licença, clique em **ADICIONAR**. Clique em **Avançar**.

---

**Observação** A chave de licença deve ser uma assinatura do vRealize Cloud. Ao adicionar uma nova licença, você pode visualizar a chave de licença em Locker no vRealize Suite Lifecycle Manager.

- 5 Selecione o **Tipo de produto** e a **Versão**.

- 6** Digite o **FQDN/Endereço IP**.
- 7** Com base no produto selecionado, você pode escolher **Senha de administrador** ou **Senha raiz**.
- 8** Marque a caixa de seleção para remover todas as licenças perpétuas do produto selecionado, se necessário.
- 9** Clique em **Validar e adicionar**. Quando a validação estiver concluída, clique em **Avançar**.
- 10** Na página Detalhes da Conexão à Nuvem, há duas opções.
  - Enviar automaticamente o consumo de licença de assinatura do seu local para VMware Cloud: Esta caixa de seleção permite enviar assinaturas para o vRealize Suite Subscription Manager. Se você marcar essa caixa de seleção, digite os detalhes do **Token do API**.
  - Usar licenças de assinatura vRCU com licenças perpétuas: Se você marcar essa caixa de seleção, insira detalhes da sua **Conta MyVMware associada**.
  - Se marcar ambas as caixas de seleção, digite os detalhes da **Rede proxy**.
- 11** Clique em **Avançar**.
- 12** Você pode validar os detalhes na página Resumo e, em seguida, clicar em **Concluir**.

#### Próximo passo

Você pode acompanhar os detalhes da solicitação na guia Solicitações.

## Operações do Dia 2 para o vRealize Cloud Universal

Agora você pode realizar as operações de Dia 2 no vRealize Cloud Universal.

Operações de Dia 2	Função
Excluir	A opção Excluir remove a entrada selecionada da página Cloud Universal, mas não exclui o produto.
Atualizar senha	A opção Atualizar senha atualiza o inventário do vRealize Suite Lifecycle Manager.
Sincronização de inventário	A opção Sincronização de inventário ajuda a sincronizar com o produto e recuperar os detalhes da licença mais recente.
Adicionar/substituir licença	A opção Adicionar/substituir licença ajuda a selecionar uma nova licença e remover licenças existentes.

## Operações de Dia 2 para licenças do vRealize Cloud

Agora você pode realizar as operações de Dia 2 no vRealize Cloud Universal.

Operações de Dia 2	Função
Conectar licença à nuvem	<ol style="list-style-type: none"> <li>1 Conecte a licença de assinatura do vRealize Cloud a uma organização VMware.</li> <li>2 Adicione a chave de licença e o token de API correto.</li> <li>3 A chave de licença deve ser conectada à organização na qual a assinatura é resgatada.</li> </ol>
Desconectar licença para a nuvem	Desconecte a chave de licença da assinatura do vRealize Cloud.
Download do pacote de utilização	<ol style="list-style-type: none"> <li>1 Selecione a chave e a finalidade da licença.</li> <li>2 Clique em Download.</li> </ol>
Uso da sincronização	<ol style="list-style-type: none"> <li>1 Forneça a chave de licença e o uso de sincronização.</li> <li>2 Clique em Sincronizar Uso.</li> <li>3 Você pode visualizar o uso de sincronização de todos os produtos.</li> </ol>
Atualize a chave de licença	<ol style="list-style-type: none"> <li>1 Selecione a chave de licença na opção Download do pacote de uso.</li> <li>2 Selecione a finalidade.</li> <li>3 Clique em Download.</li> </ol>

# Solução de problemas com o vRealize Suite Lifecycle Manager

9

Os tópicos de solução de problemas do vRealize Suite Lifecycle Manager oferecem soluções para problemas que você pode ter ao instalar e gerenciar o vRealize Suite com o vRealize Suite Lifecycle Manager.

- Falha inesperada ao ligar a grande máquina virtual do vRealize Operations Manager devido às limitações de recursos  
Falha ao ligar grandes máquinas virtuais do vRealize Operations Manager devido a limitações dos recursos.
- Há falha na implantação do ambiente ou agrupamento em cluster do vRealize Log Insight e no Registro do VMware Identity Manager  
A implantação do ambiente falha durante a tarefa Adding vIDM user as vRLI Super Admin durante a execução do vRLI Clustering and vIDM Registration.
- Alterações no servidor DNS  
Se houver uma alteração no servidor DNS, você poderá atualizar as configurações DNS do dispositivo do vRealize Suite Lifecycle Manager.
- Detalhes de IP incorretos durante a implantação do vRealize Suite Lifecycle Manager  
Se você tiver fornecido um endereço IP incorreto ou se quiser atualizar um endereço IP existente durante a implantação do vRealize Suite Lifecycle Manager, siga as etapas fornecidas nesta seção.
- Os mapeamentos binários não estão preenchidos  
Mesmo que as solicitações para cada binário de produto sejam marcadas como concluídas, os mapeamentos binários não serão preenchidos.
- A captura de conteúdo falha com o campo seguro  
Um conteúdo do vRealize Automation com um campo seguro corrompe o campo no ambiente de destino após a implementação bem-sucedida.
- Reparar erros usando arquivos de log  
Os arquivos de log do vRealize Suite Lifecycle Manager estão presentes nos seguintes locais para resolver quaisquer problemas.
- Falha na captura do blueprint  
O blueprint capturado falha após a exclusão do grupo de propriedades.

- [Falha na implantação do perfil do componente](#)

Quando os perfis do componente são liberados para o vRealize Automation, os valores das caixas de texto "Clonar de" e "Clonar do smartphone" não são atribuídos automaticamente.

- [Atualizar o nome de host do vRealize Suite Lifecycle Manager](#)

Se você fornecer um nome de host incorreto ou se quiser alterar o nome de host do vRealize Suite Lifecycle Manager após a implantação, siga as etapas fornecidas nesta seção.

- [Recurso não encontrado no Gerenciamento de Diretórios](#)

O sistema mostra uma mensagem de erro no Gerenciamento de Diretórios.

- [A UI do vRealize Automation não exibe novas chaves de licença](#)

Quando você aplica uma licença a termo do vRealize Cloud Universal a uma instância do vRealize Automation 7.5 ou 7.6 a partir do vRealize Suite Lifecycle Manager, a solicitação é bem-sucedida na UI do vRealize Suite Lifecycle Manager, mas as chaves de licença do vRealize Cloud Universal recém-aplicadas não são visíveis na UI do vRealize Automation VAMI.

- [Falha na captura, teste ou liberação de conteúdo do vRealize Orchestrator](#)

Capturar, testar ou liberar o conteúdo do vRealize Orchestrator pode falhar devido a operações relacionadas ao banco de dados em vRealize Orchestrator.

- [Estado sem resposta de operações relacionadas a licenças no vRealize Automation 7.6](#)

Ao realizar operações relacionadas a licença no vRealize Automation 7.6, as tarefas correspondentes entram em um estado sem resposta e continuam a ser executadas por mais tempo do que o esperado.

- [Falha na importação ou sincronização de inventário de produto do vRealize Suite](#)

A sincronização de importação ou inventário de produto do vRealize Suite falha com uma mensagem de erro.

- [Falha nas operações do Dia 2 do VMware Identity Manager quando a senha raiz expira](#)

As operações do dia 2 do VMware Identity Manager como o upgrade ou a falha de atualização da senha raiz quando a senha raiz do VMware Identity Manager expirar.

- [Ativar rotação de log para logs de pgpool nos arquivos do Postgres agrupado em cluster do VMware Identity Manager](#)

Você pode ativar a rotação de log para logs de pgpool do postgres agrupado em cluster VMware Identity Manager instalados usando o vRealize Suite Lifecycle Manager.

- [Interrupção do cluster do VMware Identity Manager postgres devido à perda de IP delegado](#)

Solução de problemas de interrupção de cluster do VMware Identity Manager postgres implantado por meio do vRealize Suite Lifecycle Manager.

- [Falha na importação do vRealize Automation para o vRealize Suite Lifecycle Manager](#)

Ao importar o vRealize Automation para o vRealize Suite Lifecycle Manager, a importação falha com uma mensagem de erro.

- **O vRealize Suite Lifecycle Manager exibe a versão mais antiga após um upgrade**  
O vRealize Suite Lifecycle Manager exibe uma versão mais antiga após um upgrade bem-sucedido.
- **Licenças desconectadas como operação do Dia 2 na interface de usuário do Cloud Universal não estão listadas para reconexão**  
Se você desconectar uma licença conectada em vRealize Cloud > Cloud Universal > Ações de licença > Desconectar licença para Nuvem, talvez você não possa conectá-la em vRealize Cloud > Cloud Universal > Ações de licença > Conectar licença à nuvem

## Falha inesperada ao ligar a grande máquina virtual do vRealize Operations Manager devido às limitações de recursos

Falha ao ligar grandes máquinas virtuais do vRealize Operations Manager devido a limitações dos recursos.

### Problema

Ao implantar o vRealize Operations Manager no vRealize Suite Lifecycle Manager, selecionando o tamanho do nó como grande e se você tiver recursos de orçamento para uma máquina virtual de tamanho diferente, poderá ocorrer falha ao ligar a máquina virtual devido às limitações de recursos.

### Causa

O tamanho da implantação do vRealize Operations Manager definido no vRealize Suite Lifecycle Manager baseia-se no número de máquinas virtuais, itens de catálogo, provisões simultâneas e outras métricas de carga de trabalho para o ambiente do vRealize Operations Manager. O tamanho da máquina virtual não está relacionado ao tamanho da implantação.

### Solução

As máquinas virtuais do vRealize Operations Manager implantadas a partir do vRealize Suite Lifecycle Manager possuem um tamanho de máquina virtual grande (16 vCPU e 48 GB de RAM), se implantadas com tamanho grande, e exigem vCPU e RAM suficientes para ligar com êxito.

## Há falha na implantação do ambiente o agrupamento em cluster do vRealize Log Insight e no Registro do VMware Identity Manager

A implantação do ambiente falha durante a tarefa Adding vIDM user as vRLI Super Admin durante a execução do vRLI Clustering and vIDM Registration.

## Problema

Mesmo após a operação de implantação múltipla, a implantação do ambiente falha durante a tarefa Adding vIDM user as vRLI Super Admin durante a execução do vRLI Clustering and vIDM Registration.

A seguinte mensagem de erro é exibida nos logs:

```
{"errorMessage": "Unable to retrieve information about this user from VMware Identity Manager.", "errorCode": "RBAC_USERS_ERROR", "errorDetails": {"errorCode": "com.vmware.loginsight.api.errors.rbac.invalid_vidm_user"}}
```

## Solução

- 1 Adicione o usuário administrador do conjunto do VMware Identity Manager para o vRealize Log Insight usando a UI do vRealize Log Insight.  
Consulte [Criar uma nova conta de usuário no vRealize Log Insight](#).
- 2 Remova o usuário administrador de conjunto do VMware Identity Manager do vRealize Log Insight usando a UI do vRealize Log Insight.
- 3 Repetir a implantação do ambiente no vRealize Suite Lifecycle Manager.

## Alterações no servidor DNS

Se houver uma alteração no servidor DNS, você poderá atualizar as configurações DNS do dispositivo do vRealize Suite Lifecycle Manager.

### Causa

Quando um servidor DNS fornecido durante a implantação for alterado, siga estas etapas para atualizar as configurações de DNS do vRealize Suite Lifecycle Manager.

### Solução

- 1 Use SSH para o dispositivo do vRealize Suite Lifecycle Manager usando o usuário raiz.
- 2 Atualizar a configuração do DNS usando o comando:

```
/opt/vmware/share/vami/vami_set_dns
vami_set_dns [-d <domain>] [ -s <searchpath>] DNS_Server_1 [DNS_Server_2]
```

Por exemplo: /opt/vmware/share/vami/vami\_set\_dns -d sqa.local -s sqa.local 10.1.1.25

- 3 Feche o dispositivo virtual do vRealize Suite Lifecycle Manager.
- 4 Selecione o dispositivo virtual do vRealize Suite Lifecycle Manager do vCenter e selecione **Configurar**.
- 5 Ative as Opções vApp.

- 6 Em Propriedades, edite o seguinte comando:

```
vami.DNS.VMware_vRealize_Suite_Life_Cycle_Manager_Appliance
```

- 7 Ligue o dispositivo virtual do vRealize Suite Lifecycle Manager.  
8 Verifique a nova entrada DNS executando o status resolvectl, em seguida, verifique o servidor DNS.

## Detalhes de IP incorretos durante a implantação do vRealize Suite Lifecycle Manager

Se você tiver fornecido um endereço IP incorreto ou se quiser atualizar um endereço IP existente durante a implantação do vRealize Suite Lifecycle Manager, siga as etapas fornecidas nesta seção.

### Causa

Se você tiver fornecido um endereço IP incorreto durante a implantação do vRealize Suite Lifecycle Manager.

### Solução

- 1 Use SSH para o dispositivo do vRealize Suite Lifecycle Manager utilizando o usuário raiz.
- 2 Atualize o endereço IP usando o comando abaixo:

```
vami_set_network <interface> (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6) <ipv4_addr>
<netmask> <gatewayv4>Por exemplo: /opt/vmware/share/vami/vami_set_network eth0
STATICV4 192.168.1.150 255.255.255.0 192.168.1.1
```

## Os mapeamentos binários não estão preenchidos

Mesmo que as solicitações para cada binário de produto sejam marcadas como concluídas, os mapeamentos binários não serão preenchidos.

### Problema

Quando você navega de **Configurações > iniciais > dos binários do produto**, a solicitação correspondente é marcada como CONCLUÍDA na página de **Solicitações** mas os mapeamentos binários não são preenchidos.

### Causa

A soma de verificação para o binário do produto de destino não pode ser igual à publicada pela VMware.

### Solução

- ◆ Certifique-se de que os binários não estão corrompidos nem foram modificados e que a soma de verificação SHA256 é a mesma que a mencionada no portal MyVMware.

## A captura de conteúdo falha com o campo seguro

Um conteúdo do vRealize Automation com um campo seguro corrompe o campo no ambiente de destino após a implementação bem-sucedida.

### Causa

No vRealize Suite Lifecycle Manager 8.0, o campo seguro é capturado como criptografado do ambiente de origem e o valor não pode ser descriptografado quando implantado.

### Solução

- ◆ Após a implantação bem-sucedida, faça login no vRealize Automation de destino e atualize manualmente os campos seguros no conteúdo.

## Reparar erros usando arquivos de log

Os arquivos de log do vRealize Suite Lifecycle Manager estão presentes nos seguintes locais para resolver quaisquer problemas.

### Solução

- 1 Para o vRealize Suite Lifecycle Manager versão 1.1 ou anteriores, os logs de camada de serviço estão presentes no local `/opt/vmware/vlcm/logs/` e o formato do arquivo é `xenon.*.log`, o arquivo de log ativo é `xenon.0.log`. Para o vRealize Suite Lifecycle Manager versão 1.2 ou posterior, esse log está disponível em `/var/log/vlcm` e o nome do arquivo de log é `vrlcm-xserver.log`
- 2 Para o vRealize Suite Lifecycle Manager versão 1.1 ou anterior, os logs do mecanismo estão presentes no local `/var/log/vlcm/` e o nome do arquivo de log atual é `catalina.out`. Para o vRealize Suite Lifecycle Manager 1.2 ou posterior, esse log está disponível em `/var/log/vlcm` e o nome do arquivo de log é `vrlcm-server.log`

---

**Observação** Para fazer o upgrade da 1.0 ou 1.1–1.3, o log de camadas de serviço LCM antigos presentes no local `/opt/vmware/vlcm/logs/` está com o nome `console.log` e os novos logs da camada de serviço estão no formato de arquivo `xenon.*.log`.

---

## Falha na captura do blueprint

O blueprint capturado falha após a exclusão do grupo de propriedades.

### Problema

Quando um blueprint composto de vRealize Automation tem referências a quaisquer propriedades, como Definição de propriedades ou Grupos de propriedades, e se essas propriedades são excluídas do vRealize Automation então o Blueprint deve ser atualizado no vRealize Automation ou, caso isso não seja feito, a captura no Lifecycle Manager falhará.

## Solução

- 1 Editar o Blueprint.
- 2 Clique no ícone **Configuração** ao lado do nome do blueprint na parte superior.
- 3 Clique na guia **Propriedades** (selecione a guia **propriedades personalizadas** se alguma propriedade tiver sido adicionada anteriormente) e selecione OK.
- 4 Selecione cada um dos componentes no blueprint e selecione a guia **Propriedades**. (selecione a guia **propriedades personalizadas** se alguma propriedade tiver sido adicionada anteriormente).
- 5 Clique em **Salvar**.
- 6 Clique em **Concluir**.

## Falha na implantação do perfil do componente

Quando os perfis do componente são liberados para o vRealize Automation, os valores das caixas de texto "Clonar de" e "Clonar do smartphone" não são atribuídos automaticamente.

### Problema

Ao implantar um "Perfil de componente de imagem", o valor "Clonar de" do perfil de componente é removido. As caixas de texto "Clonar de" estão vazias no sistema de destino.

### Solução

- ◆ Você pode editar manualmente o perfil do componente e os respectivos valores pelo menu suspenso.

---

**Observação** Ao capturar e liberar um perfil de componente do vRealize Automation usando vRealize Suite Lifecycle Manager, o nome do perfil do componente deve começar com "ValueSet".

---

## Atualizar o nome de host do vRealize Suite Lifecycle Manager

Se você fornecer um nome de host incorreto ou se quiser alterar o nome de host do vRealize Suite Lifecycle Manager após a implantação, siga as etapas fornecidas nesta seção.

### Causa

Se você quiser atualizar o nome de host do vRealize Suite Lifecycle Manager.

### Solução

- 1 Use o Secure Shell (SSH) para acessar o dispositivo do vRealize Suite Lifecycle Manager usando os privilégios do usuário raiz .

- 2 Atualize o nome de host usando os seguintes comandos:

```
rm /opt/vmware/etc/vami/flags/vami_setnetwork  
/opt/vmware/share/vami/vami_set_hostname new-hostname
```

- 3 Reinicie o dispositivo do vRealize Suite Lifecycle Manager.
- 4 Atualize o certificado do vRealize Suite Lifecycle Manager em Configurações no vRealize Suite Lifecycle Manager.
- 5 Feche o dispositivo do vRealize Suite Lifecycle Manager.
- 6 Localize a máquina virtual no vCenter.
- 7 Selecione Configurar e, em seguida, selecione Opções do vApp.
- 8 Selecione `vami.hostname`, defina o valor e atualize o valor para o novo nome do host.
- 9 Ligue a máquina virtual e altere o nome do host usando o seguinte comando:  
`/opt/vmware/share/vami/vami_config_net`
- 10 Reinicialize o dispositivo do vRealize Suite Lifecycle Manager.

## Recurso não encontrado no Gerenciamento de Diretórios

O sistema mostra uma mensagem de erro no Gerenciamento de Diretórios.

### Problema

Quando você exibe ou edita o diretório no Gerenciamento de Diretórios, o sistema não pode recuperar as informações necessárias do VMware Identity Manager e exibe uma mensagem de erro.

### Causa

O diretório foi parcialmente criado ou a configuração do diretório está incompleta.

### Solução

- 1 Faça login no VMware Identity Manager. Verifique a configuração do diretório e confirme se ele está associado a um conector. Valide também a senha de vinculação.
- 2 Se a configuração do diretório estiver incompleta, você pode defini-la no VMware Identity Manager. Você também pode usar o vRealize Suite Lifecycle Manager para remover o diretório usando a funcionalidade de exclusão, fornecer detalhes de configuração corretos e depois adicionar novamente o diretório.

### Solução

---

**Observação** Qualquer função atribuída ao usuário do diretório no vRealize Lifecycle Manager deverá ser excluída e reatribuída depois que o diretório voltar a ser adicionado.

---

Essa opção é compatível com o vRealize Suite Lifecycle Manager 8.2 Patch 1 e versões mais recentes.

## A UI do vRealize Automation não exibe novas chaves de licença

Quando você aplica uma licença a termo do vRealize Cloud Universal a uma instância do vRealize Automation 7.5 ou 7.6 a partir do vRealize Suite Lifecycle Manager, a solicitação é bem-sucedida na UI do vRealize Suite Lifecycle Manager, mas as chaves de licença do vRealize Cloud Universal recém-aplicadas não são visíveis na UI do vRealize Automation VAMI.

### Problema

Quando uma chave de licença a termo é aplicada a uma instância do vRealize Automation 7.x com uma chave de licença perpétua, ocorre uma falha da tarefa no vRealize Automation. O vRealize Suite Lifecycle Manager não mostra essa falha e a solicitação correspondente é marcada como concluída. Esse problema ocorre somente quando o modo FIPS está ativado no vRealize Suite Lifecycle Manager.

### Causa

Essa é uma limitação conhecida no vRealize Suite Lifecycle Manager com o modo FIPS.

### Solução

Desative o modo FIPS antes de aplicar licenças do vRealize Cloud Universal a partir do vRealize Suite Lifecycle Manager para que os erros reais possam ser refletidos na UI de solicitação do vRealize Suite Lifecycle Manager.

## Falha na captura, teste ou liberação de conteúdo do vRealize Orchestrator

Capturar, testar ou liberar o conteúdo do vRealize Orchestrator pode falhar devido a operações relacionadas ao banco de dados em vRealize Orchestrator.

### Causa

Ao capturar, testar ou liberar conteúdo do vRealize Orchestrator, os elementos do vRealize Orchestrator podem falhar no endpoint ao criar o conteúdo.

### Solução

Inspecione os logs do vRealize Orchestrator e identifique o elemento que está causando a falha. Exclua o respectivo elemento do vRealize Orchestrator e tente novamente.

## Estado sem resposta de operações relacionadas a licenças no vRealize Automation 7.6

Ao realizar operações relacionadas a licença no vRealize Automation 7.6, as tarefas correspondentes entram em um estado sem resposta e continuam a ser executadas por mais tempo do que o esperado.

### Causa

Isso ocorre quando o FIPS está habilitado no vRealize Suite Lifecycle Manager.

### Solução

- 1 Desative o FIPS no vRealize Suite Lifecycle Manager em Operações de Ciclo de Vida > Início > Configurações > Conformidade com o Modo FIPS.
- 2 Cancele a solicitação em andamento na página Solicitações. Como alternativa, a solicitação pode ser excluída usando a API quando a opção de cancelar a solicitação não está disponível.
- 3 Acione a solicitação cancelada. Se for uma solicitação programada do sistema, ela será acionada automaticamente após um intervalo de tempo específico.

---

**Observação** O modo FIPS deve ser desabilitado no vRealize Suite Lifecycle Manager para evitar esse problema. Se o FIPS estiver ativado, o problema ocorrerá.

---

## Falha na importação ou sincronização de inventário de produto do vRealize Suite

A sincronização de importação ou inventário de produto do vRealize Suite falha com uma mensagem de erro.

### Causa

Quando o `keyUsage` não possui o atributo `digitalSignature` no certificado HTTPS do produto de destino, a sincronização de importação ou inventário do produto do vRealize Suite falha com uma mensagem de erro.

### Solução

Execute as seguintes etapas:

- 1 Clique no ícone do cadeado na barra de endereço de um navegador (Chrome, Edge ou Firefox) e, em seguida, clique em **Certificado**.
- 2 Clique em **Detalhes** e, em seguida, clique em **Uso de chave**.
- 3 Verifique se o atributo `digitalSignature` está presente no `keyUsage`. Se o atributo `digitalSignature` não estiver presente, substitua o certificado no produto de destino pelo certificado que tenha o atributo `digitalSignature` presente no `keyUsage`.

## Falha nas operações do Dia 2 do VMware Identity Manager quando a senha raiz expira

As operações do dia 2 do VMware Identity Manager como o upgrade ou a falha de atualização da senha raiz quando a senha raiz do VMware Identity Manager expirar.

### Solução

- 1 Faça login no console do dispositivo virtual do VMware Identity Manager no vCenter Server.
- 2 Atualize a senha raiz do dispositivo virtual do VMware Identity Manager.
- 3 Faça login no vRealize Suite Lifecycle Manager e execute a sincronização de inventário do VMware Identity Manager. Atualize a senha raiz do VMware Identity Manager ao tentar novamente uma solicitação de sincronização de inventário com falha.
- 4 Dispare as operações do Dia 2 do VMware Identity Manager.

### Solução

## Ativar rotação de log para logs de pgpool nos arquivos do Postgres agrupado em cluster do VMware Identity Manager

Você pode ativar a rotação de log para logs de pgpool do postgres agrupado em cluster VMware Identity Manager instalados usando o vRealize Suite Lifecycle Manager.

### Problema

O uso do disco combinado mostrado com `du -hsc /var/log/pgService/pgService*` está com mais de 50% da capacidade total de disco de `/dev/sda4` conforme indicado na saída do comando `df -h`.

### Solução

- 1 Ao executar o comando `find/etc/logrotate.d -iname pgservice.log`, se a resposta for `/etc/logrotate.d/pgservice.log`, execute os comandos a seguir:
  - a `touch /etc/cron.d/rotatePgServiceLogs`
  - b `echo "*/45 * * * root /usr/sbin/logrotate /etc/logrotate.d/pgservice.log" > /etc/cron.d/rotatePgServiceLogs`
  - c Para o VMware Identity Manager 3.3.2: `/etc/init.d/cron restart`  
Para o VMware Identity Manager 3.3.3 ou posterior: `systemctl restart crond`
- 2 Ao executar o comando `find /etc/logrotate.d -iname pgservice.log`, se não houver resposta, execute os comandos a seguir:
  - a `touch /etc/cron.d/rotatePgServiceLogs`

```
b touch /etc/logrotate.d/pgservice.log  
c echo "/var/log/pgService/pgService.log {  
    copytruncate  
    rotate 6  
    compress  
    missingok  
    size 50M  
}" > /etc/logrotate.d/pgservice.log  
d echo "*/45 * * * root /usr/sbin/logrotate /etc/logrotate.d/  
    pgservice.log" > /etc/cron.d/rotatePgServiceLogs  
e Para o VMware Identity Manager 3.3.2: /etc/init.d/cron restart  
Para o VMware Identity Manager 3.3.3 ou posterior: systemctl restart crond
```

## Interrupção do cluster do VMware Identity Manager postgres devido à perda de IP delegado

Solução de problemas de interrupção de cluster do VMware Identity Manager postgres implantado por meio do vRealize Suite Lifecycle Manager.

### Problema

O status de integridade do cluster do VMware Identity Manager é exibido como CRÍTICO na Notificação de integridade do vRealize Suite Lifecycle Manager devido à perda de rede no dispositivo do VMware Identity Manager.

### Causa

Perda de rede no nó primário do cluster postgres. Para o comando `/usr/local/bin/pcp_watchdog_info -p 9898 -h localhost -U pgpool`, ele solicitaria uma senha. Se o arquivo `/usr/local/etc/pgpool.pwd` estiver presente no nó do VMware Identity Manager, que contém a senha. Se a senha não estiver disponível, use a senha padrão `senha`.

Ajuda para parâmetros de comando:

`-h` : o host no qual o comando é executado é `localhost`.

`-p` : a porta na qual `pgpool` aceita conexões é `9898`.

`-U` : o usuário de verificação de atraso de replicação e verificação de integridade `pgpool` é `pgpool`.

Deve haver uma resposta esperada.

```
3 YES <Host1>:9999 Linux <Host1> <Host1>
```

```
<Host1>:9999 Linux <Host1> <Host1> 9999 9000 4 MASTER  
<Host2>:9999 Linux <Host2> <Host2> 9999 9000 7 STANDBY  
<Host3>:9999 Linux <Host3> <Host3> 9999 9000 7 STANDBY
```

Na resposta, deve haver um nó MESTRE e um nó 2 EM ESPERA presentes. Se qualquer um dos status do nó for DESLIGADO, INATIVO ou a execução do comando estiver errada, siga as etapas para resolver esse problema.

#### Solução

- 1 Traga normalmente os serviços referentes aos nós do VMware Identity Manager. Consulte a KB [78815](#) para ver as etapas necessárias.
- 2 Desligue os dispositivos do VMware Identity Manager no vCenter.
- 3 Ligue os nós do VMware Identity Manager por meio do vRealize Suite Lifecycle Manager.

## Falha na importação do vRealize Automation para o vRealize Suite Lifecycle Manager

Ao importar o vRealize Automation para o vRealize Suite Lifecycle Manager, a importação falha com uma mensagem de erro.

#### Problema

Se os detalhes do VMware Identity Manager não corresponderem ao vRealize Automation, ao importar o vRealize Automation para o vRealize Suite Lifecycle Manager, poderá receber a seguinte mensagem de erro.

Error Code: LCMVRAVACONFIG590026

vRealize Automation Import failed due to VMware Identity Manager details in vRealize Suite Lifecycle Manager not matching with the provided vRealize Automation. Please retry by providing vRealize Automation which has VMware Identity Manager details same as vRSLCM VMware Identity Manager details.

vRA vIDM details mismatch. vRA Import is supported only if vRSLCM vIDM is matched with vRA vIDM details.

#### Causa

O VMware Identity Manager importado para o vRealize Suite Lifecycle Manager não corresponde ao host do vRealize Automation que estava sendo importado.

#### Solução

- 1 Exclua o ambiente global do vRealize Suite Lifecycle Manager. Essa ação tem suporte na UI do vRealize Suite Lifecycle Manager versão 8.4.
- 2 Importe o VMware Identity Manager que está associado ao host do vRealize Automation.

- 3 Crie uma nova solicitação para importar o vRealize Automation.

## O vRealize Suite Lifecycle Manager exibe a versão mais antiga após um upgrade

O vRealize Suite Lifecycle Manager exibe uma versão mais antiga após um upgrade bem-sucedido.

### Problema

Quando você atualiza o vRealize Suite Lifecycle Manager da versão  $x$  para a versão  $y$  o vRealize Suite Lifecycle Manager pode exibir incorretamente a versão  $x$  após um upgrade bem-sucedido.

### Causa

Esse comportamento ocorre quando o VAMI, o componente que realiza a atualização, não consegue atualizar um arquivo de manifesto no vRealize Suite Lifecycle Manager após o upgrade da versão.

### Solução

Nenhuma ação necessária do usuário. Quando o VAMI não consegue atualizar a versão no arquivo de manifesto, ele agenda um trabalho que executa essa operação no próximo ciclo em 12 horas.

## Licenças desconectadas como operação do Dia 2 na interface de usuário do Cloud Universal não estão listadas para reconexão

Se você desconectar uma licença conectada em vRealize Cloud > Cloud Universal > Ações de licença > Desconectar licença para Nuvem, talvez você não possa conectá-la em vRealize Cloud > Cloud Universal > Ações de licença > Conectar licença à nuvem

### Problema

Se você selecionar vRealize Cloud > Cloud Universal > Ações de licença > Desconectar Licença para nuvem e, em seguida, desconectar uma licença conectada, você não poderá conectar a mesma licença em vRealize Cloud > Cloud Universal > Ações de licença > Conectar licença à nuvem, pois a chave de licença não é listada na interface do usuário.

### Solução

- 1 No dashboard Operações de ciclo de vida, navegue até **Locker** e selecione **Licenças**.
- 2 Selecione **Conectar licença** nas ações para a chave de licença que não está sendo exibida no Cloud Universal e siga as etapas fornecidas no assistente para conectar a chave de licença para nuvem.